Contents

12. ***Technology***

13. ***Telecommunications***

14. ***Defending yesterday: Key findings Main report***

15. ***Defending yesterday: Key findings Executive summary***

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

Aerospace & Defense

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents evolve in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global aerospace and defense (A&D) industry are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising, confidence is high, and detected incidents are down.

But while many A&D companies have raised the bar on security, their adversaries have done better.

Threats are constantly multiplying and evolving. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few A&D companies have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that companies identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

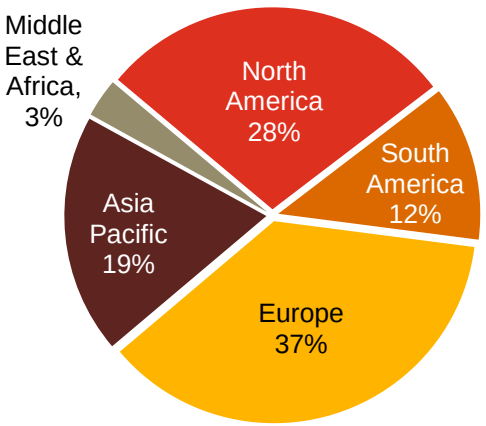
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

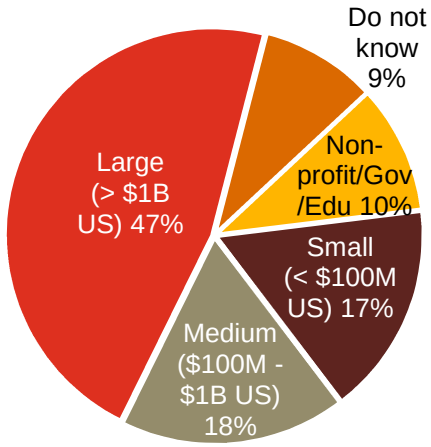
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 193 respondents from the aerospace and defense industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

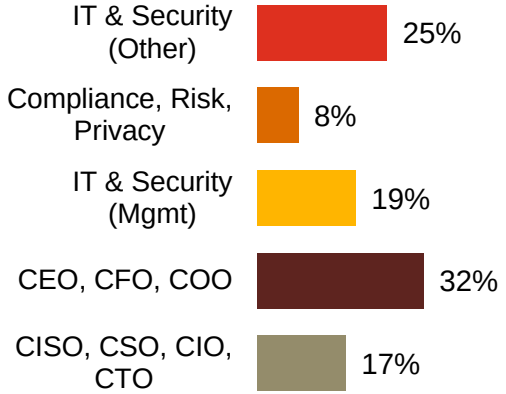
A&D respondents by region of employment



A&D respondents by company revenue size



A&D respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

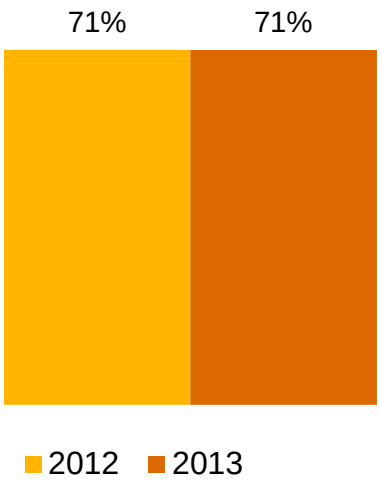
Section 2

Confidence in an era of advancing risks

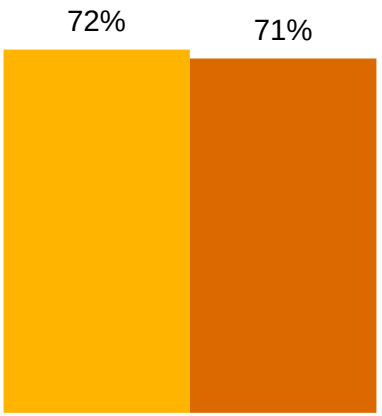
Confidence is high: 71% of A&D respondents believe their security activities are effective.

The same number of respondents report confidence in their partners' and suppliers' security programs.

Confidence in effectiveness of security activities



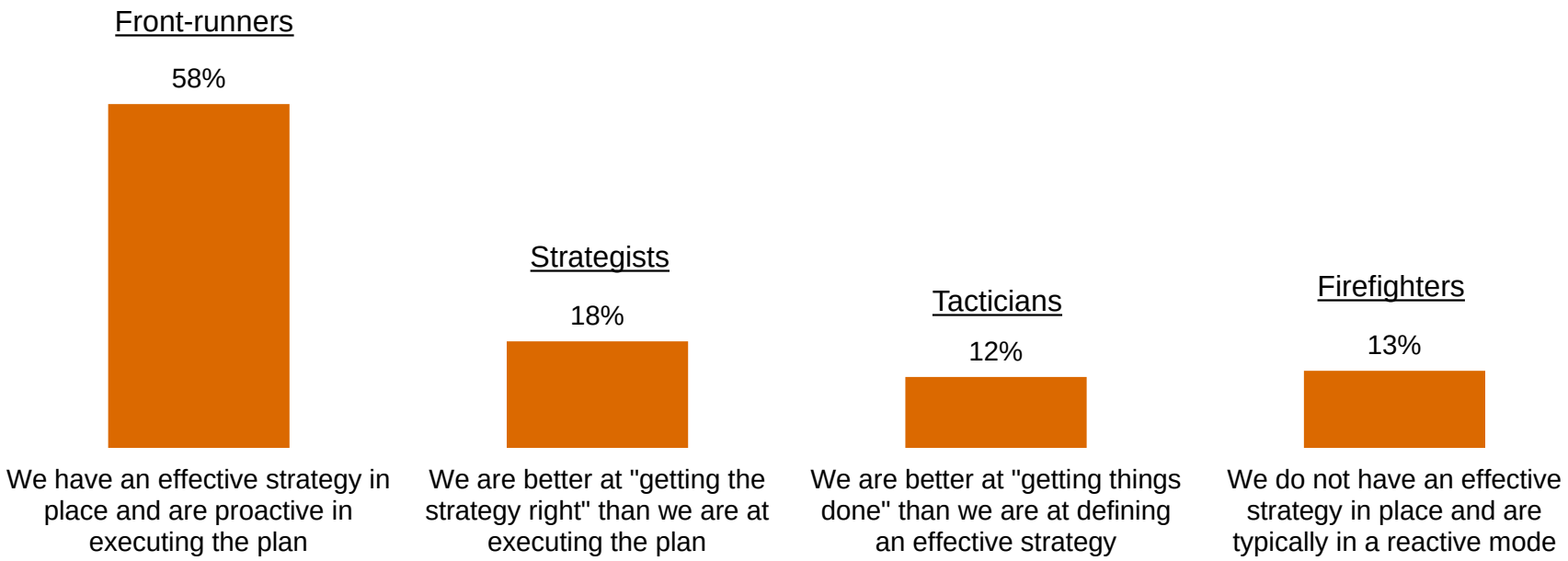
Confidence in effectiveness of partners'/suppliers' security activities



Question 39: "How confident are you that your organization's information security activities are effective?" Question 40: "How confident are you that your partners'/suppliers' information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.")

58% of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

The number of A&D respondents reporting they have an effective strategy in place and are proactive in executing the plan increased 16% over last year. About one in five (18%) say they are better at getting the strategy right than executing the plan.



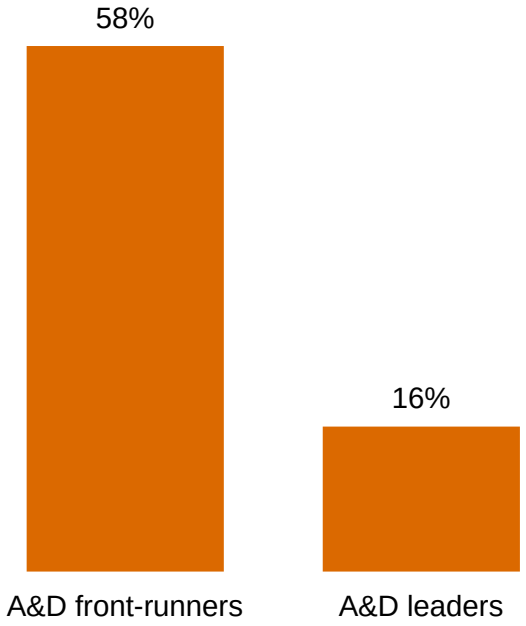
Question 27: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding.)

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured A&D respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

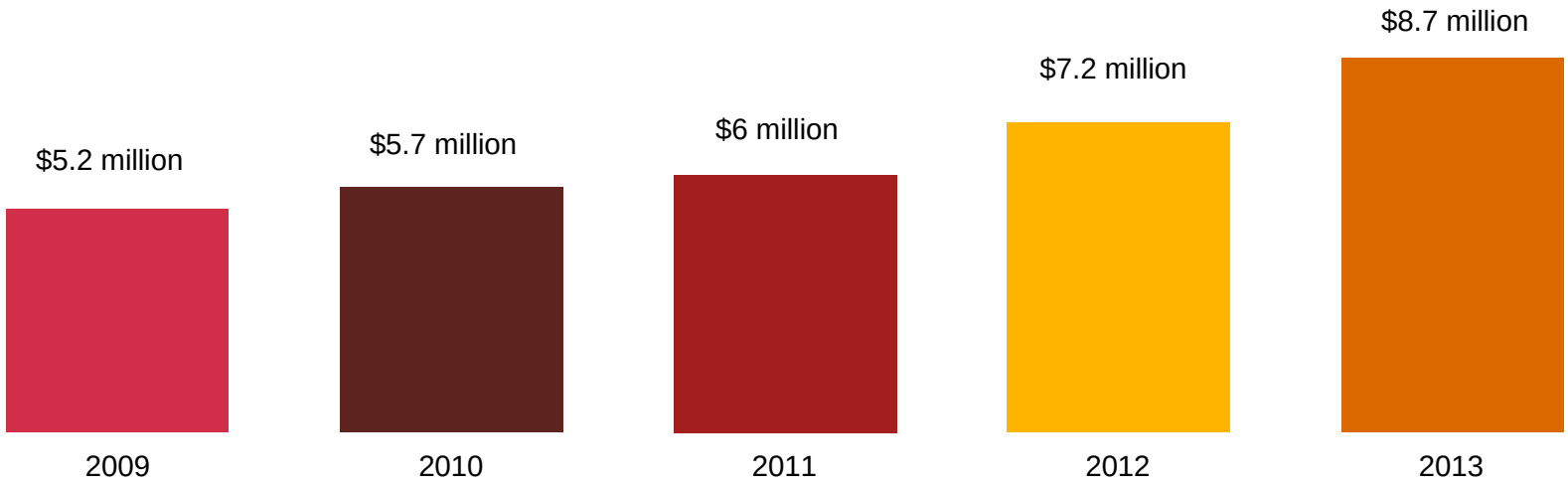


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

A&D security budgets have increased significantly.

Information security budgets average $8.7 million this year, a gain of 21% over 2012. This boost suggests that A&D companies understand that today's elevated threat landscape demands a greater investment in security.

Average information security budget

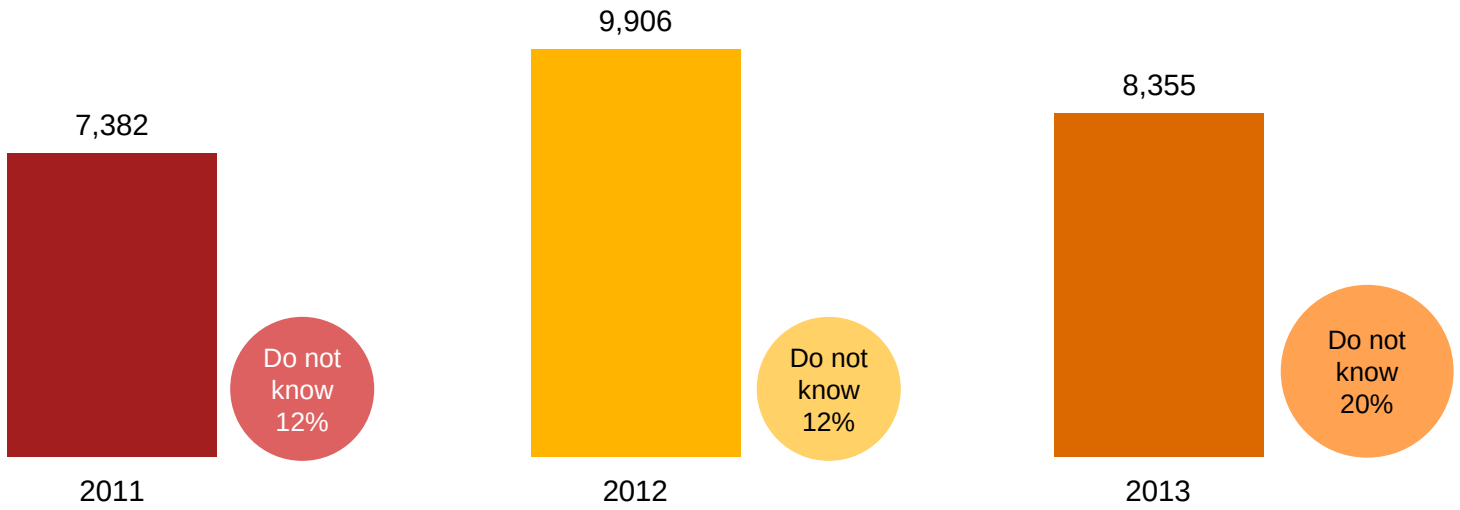


Question 8: "What is your organization's total information security budget for 2013?"

A&D respondents detected fewer security incidents this year, and financial losses are down substantially.*

A&D respondents detected 16% fewer security incidents in the past 12 months, perhaps an indication of the industry's implementation of sophisticated security tools. Average financial losses associated with security incidents dropped 32% over last year, which is surprising given the cost and complexity of responding to incidents.

Average number of security incidents in past 12 months



* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

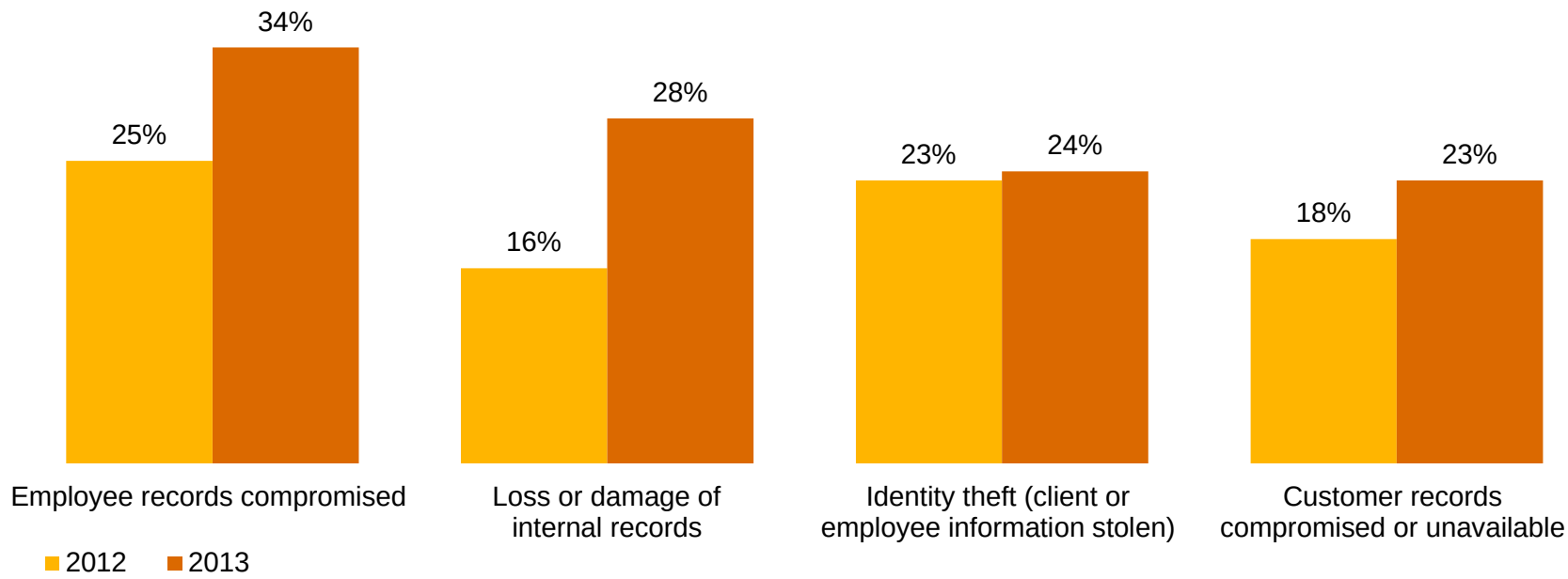
Section 3

Today's incidents, yesterday's strategies

A&D respondents report an increase in data loss as a result of security incidents.

Compromise of employee records remains the most cited impact, potentially jeopardizing an organization's most valuable relationship. Also significant: Loss or damage of internal records jumped 77% over 2012.

Impact of security incidents

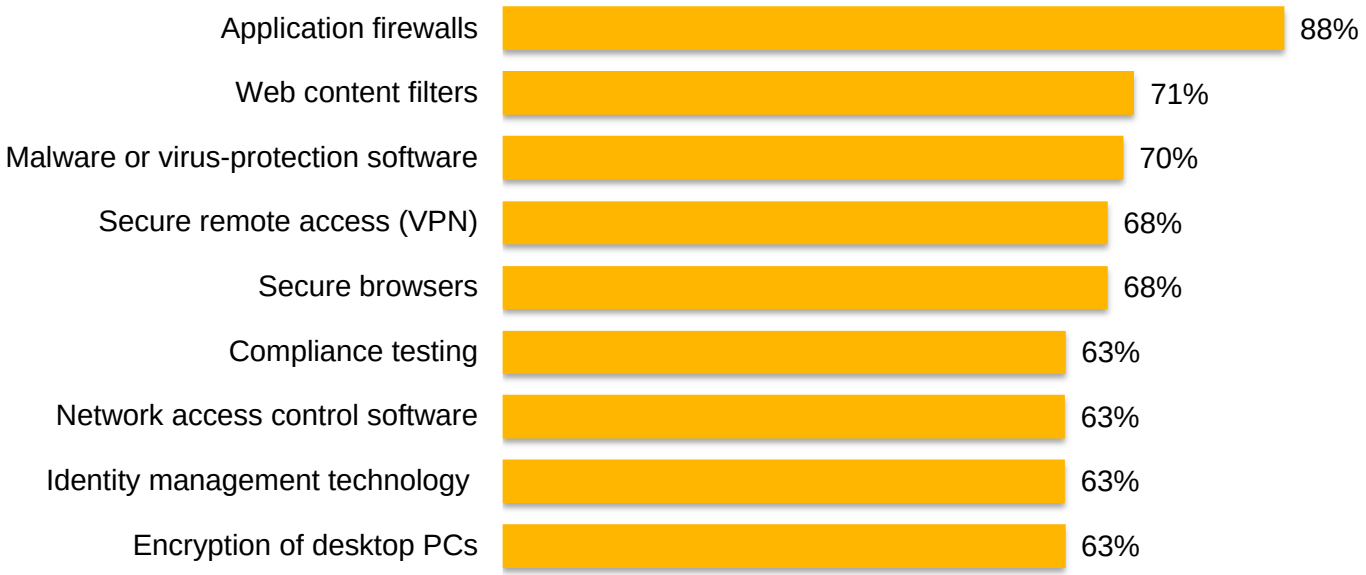


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

Information security safeguards and processes currently in place

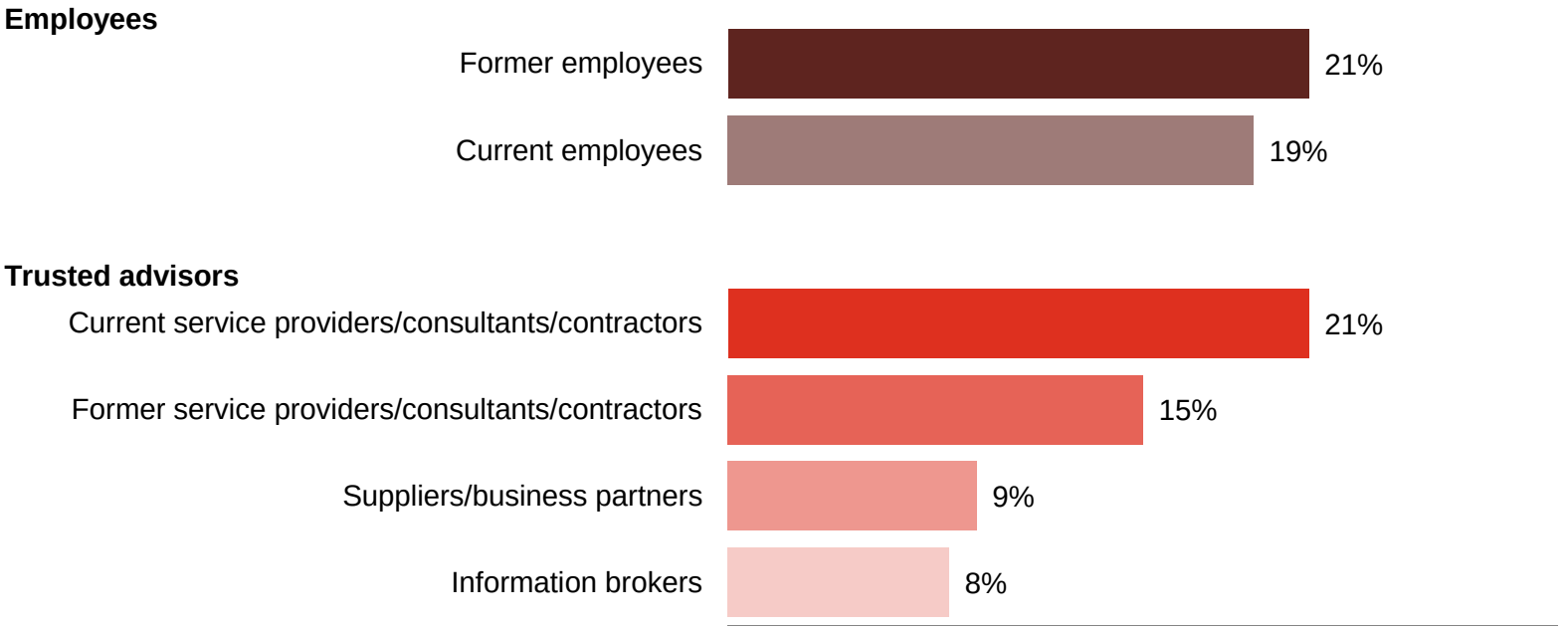


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most A&D respondents.

It's the people you know—current and former employees, as well as other insiders—who are most likely to perpetrate security incidents. Also noteworthy: Respondents say trusted advisors like service providers and contractors are responsible for one in five incidents.

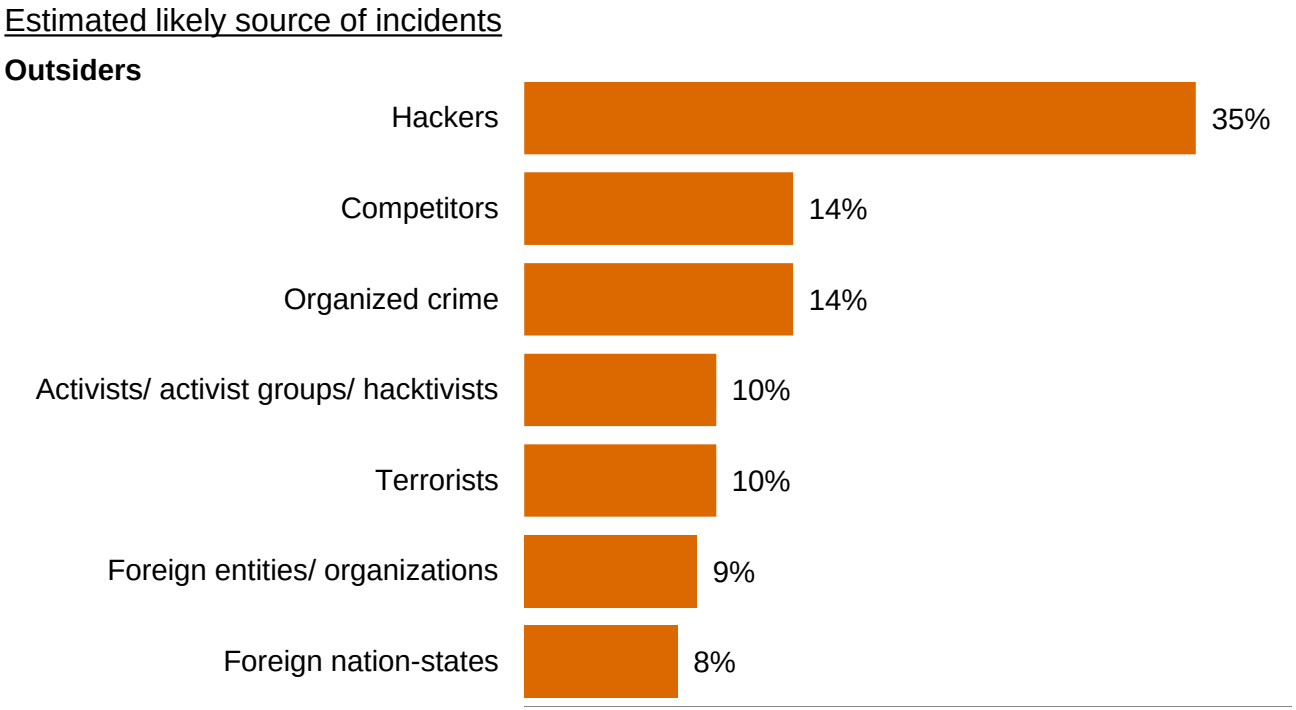
Estimated likely source of incidents



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, A&D companies are more likely to be hit by other outsiders.

Only 8% of respondents report security incidents perpetrated by foreign nation-states. Nontargeted attacks, such as hackers, represent a much more likely danger.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

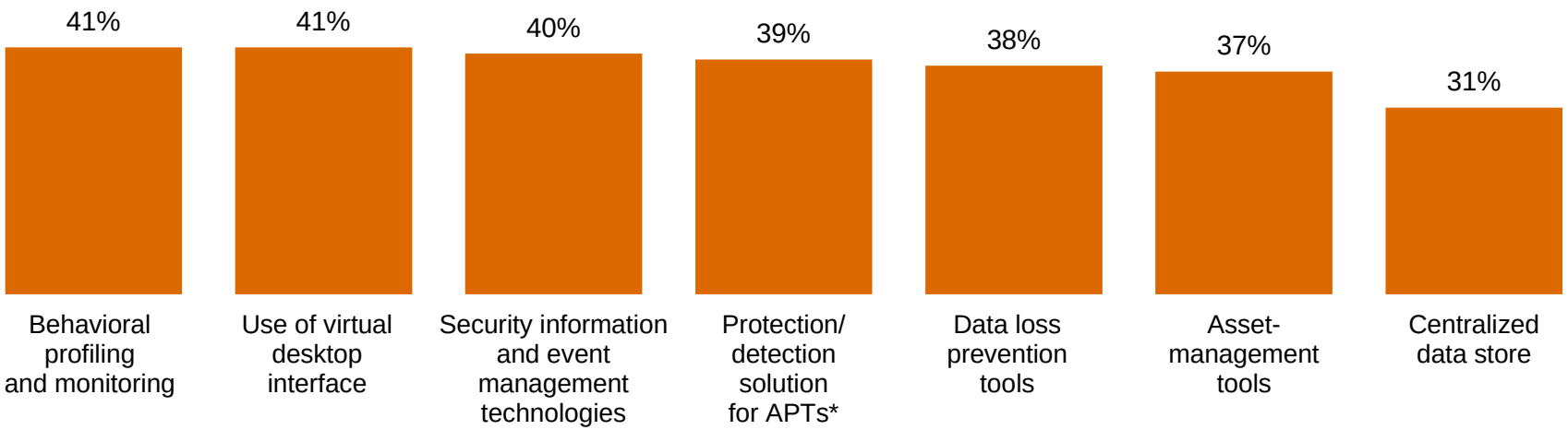
Section 4

A weak defense against adversaries

Many A&D companies have not implemented technologies and processes that can provide insight into today's risks.

Safeguards that monitor data and assets are less likely to be in place than traditional technologies. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place



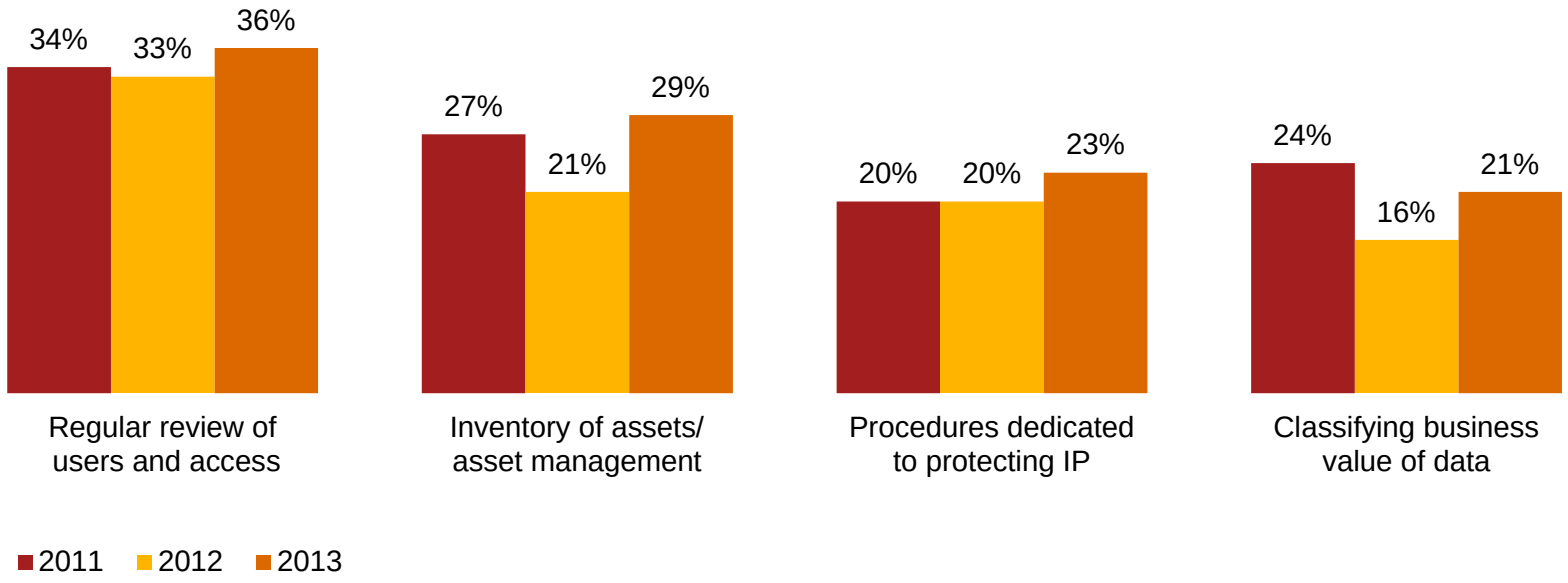
*Advanced persistent threats (APTs)

Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite potential consequences, many A&D companies do not adequately safeguard high-value information.

It is imperative that organizations identify, prioritize, and protect their "crown jewels." A&D respondents show progress in implementing basic policies to safeguard intellectual property (IP), but these levels remain low.

Have policies to help safeguard IP and trade secrets

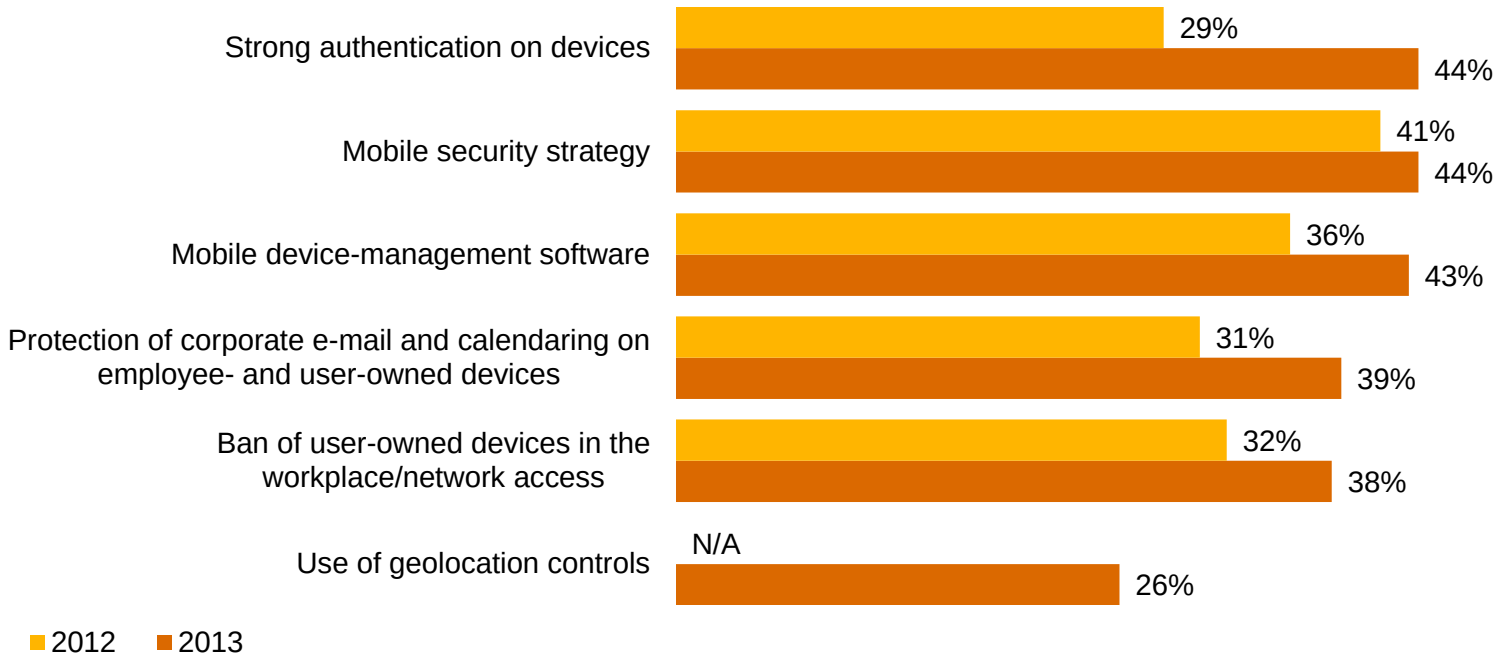


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. A&D companies' efforts to implement mobile security programs show solid gains over last year, but continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

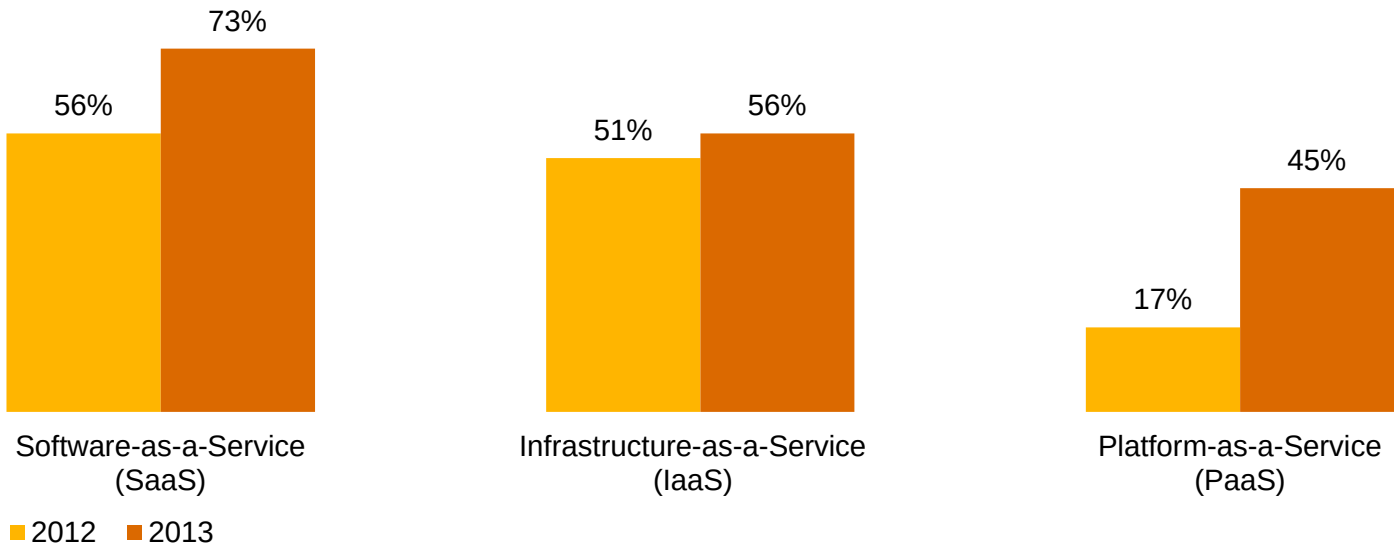


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Almost half of A&D respondents use cloud computing, but they often do not include cloud in their security policies.

While 49% of A&D respondents use cloud computing—and 66% report better information security as a result—only 22% include provisions for cloud in their security policy. SaaS remains dominant, but deployment of PaaS almost tripled over last year.

Type of cloud service used



Question 32: "Which of the following elements, if any, are included in your organization's security policy?" Question 42: "Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?" Question 42A: "What type of cloud service does your organization use?" Question 42C: "What impact has cloud computing had on your company's information security?" (Not all factors shown.)

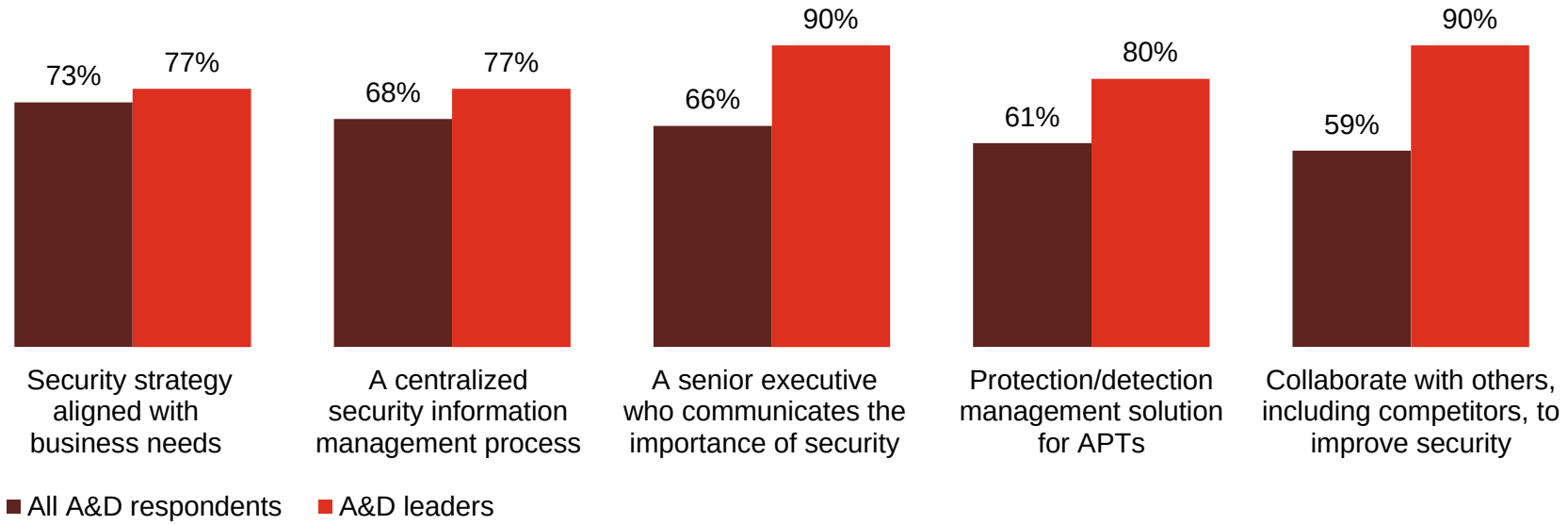
Section 5

Preparing for the threats of tomorrow

A&D leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT challenge.

Aligning security with business needs, improving communications, and collaborating with others show leaders, in particular, are rethinking the fundamentals of security.

Security policies and safeguards currently in place: All respondents vs. leaders



Question 14: “What process information security safeguards does your organization currently have in place?” Question 15: “What technology information security safeguards does your organization currently have in place?” (Not all factors shown.) Question 29: “Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?” Question 41: “Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?”

Many respondents have invested in technology safeguards to secure their ecosystems against today's evolving threats.

A&D leaders are more likely to have implemented these technologies. But given today's elevated threat landscape, *all* organizations should strongly consider implementation of these safeguards.

Technology safeguards currently in place	All A&D respondents	A&D leaders
Malicious code detection tools	79%	90%
Centralized user data store	69%	87%
Mobile device management	65%	73%
Privileged user access	66%	80%
Asset management tools	63%	77%
Identity management technology	63%	80%
Data loss prevention tools	62%	77%
Encryption of smartphones	61%	80%
Virtual desktop interface	59%	77%
Code analysis tools	59%	73%

Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

What business imperatives and processes will A&D respondents prioritize this year?

Some of the highest priorities cited by respondents include technologies that can help the organization protect its most valuable assets and protect the infrastructure.

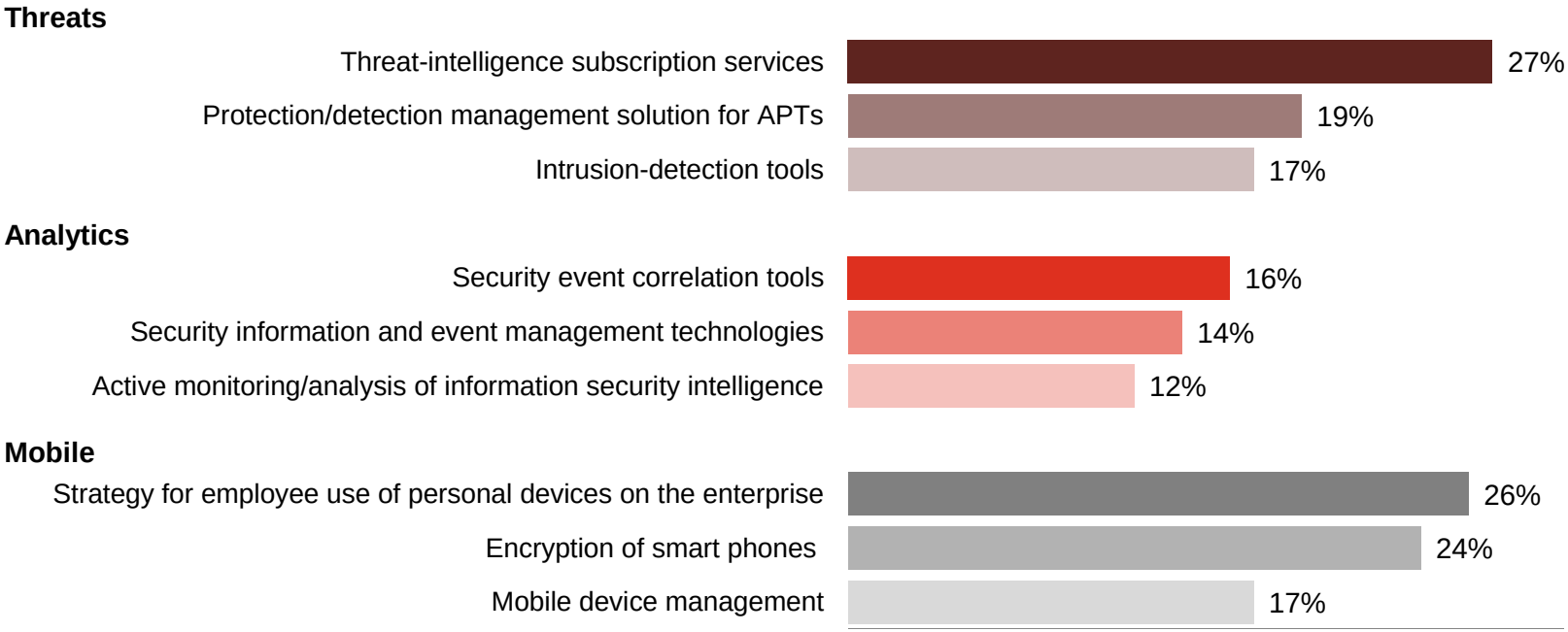
Safeguards not in place but a top priority over the next 12 months

Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and A&D respondents are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices. .

Safeguards not in place but a top priority over the next 12 months

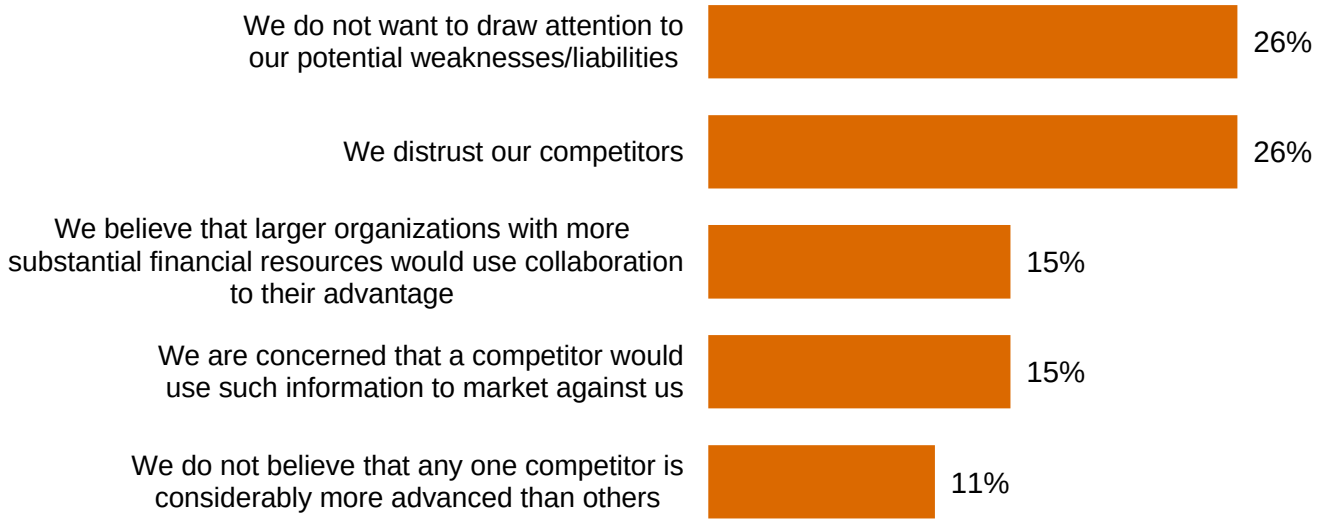


Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

59% of A&D respondents collaborate with others to improve security.

Collaboration can be an effective offensive tool in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, for instance, we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.[1] Among respondents that do not collaborate, a lack of trust is key.

Reasons for not collaborating on information security



[1] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

Effective security demands that A&D companies align policies and spending with business objectives.

A high level of A&D respondents say security policies and spending are aligned with business objectives. This suggests they understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

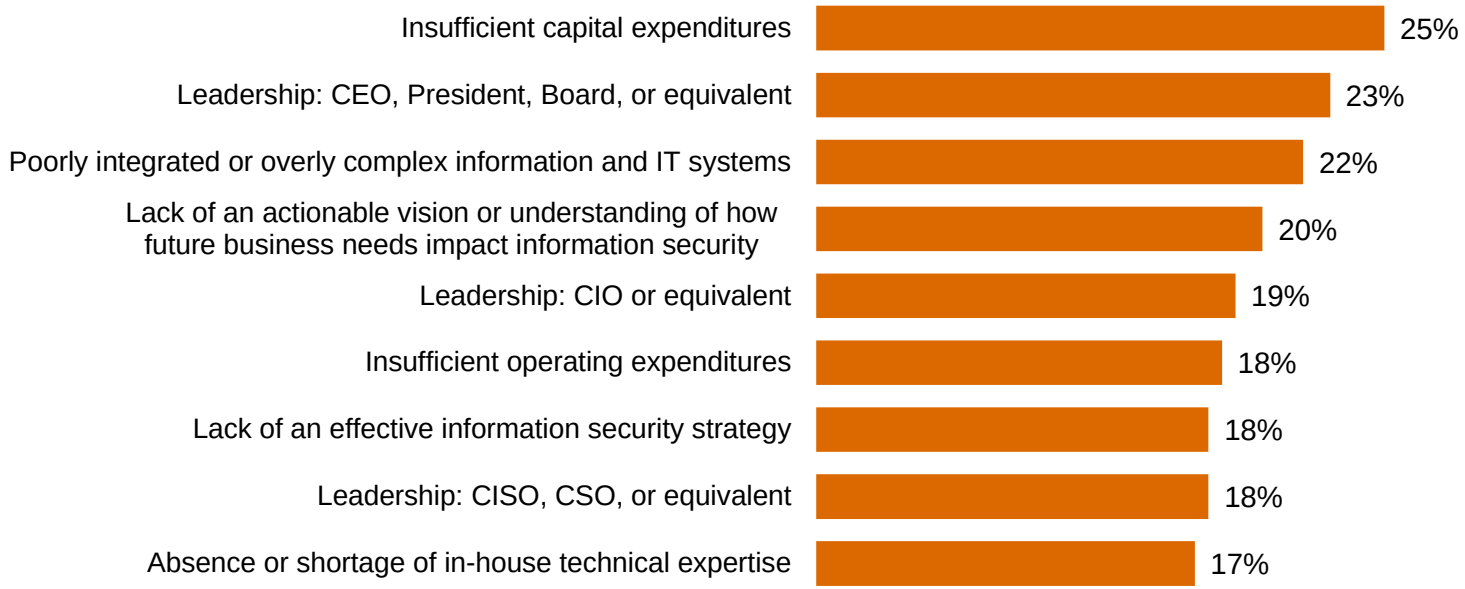
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

More money, effective leadership, and better integrated IT are needed to advance security.

These are critical because an effective approach to security requires adequate funding and informed, committed leadership at the top.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are 10 key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

US Aerospace & Defense Contacts

Scott Thompson
Partner
860.241.7296
scott.thompson@us.pwc.com

Quentin Orr
Managing Director
267.330.2699
e.quentin.orr@us.pwc.com

John Pearce
Director
703.346.9071
john.pearce@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

Automotive

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders can bypass perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global automotive industry are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising and confidence is high.

But while many organizations have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few organizations have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that organizations identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

A global, cross-industry survey of business and IT executives

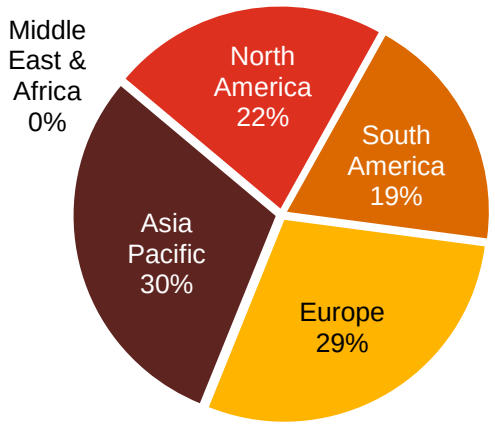
The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 209 respondents from the automotive industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

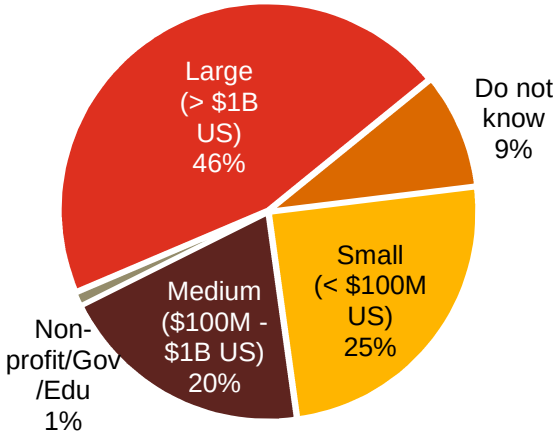
Demographics

46% of automotive respondents work for large organizations (more than $1 billion in revenue), an increase of 35% over last year.

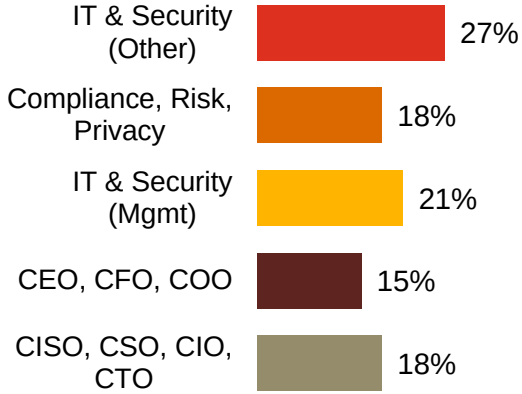
Automotive respondents by region of employment



Automotive respondents by company revenue size



Automotive respondents by title



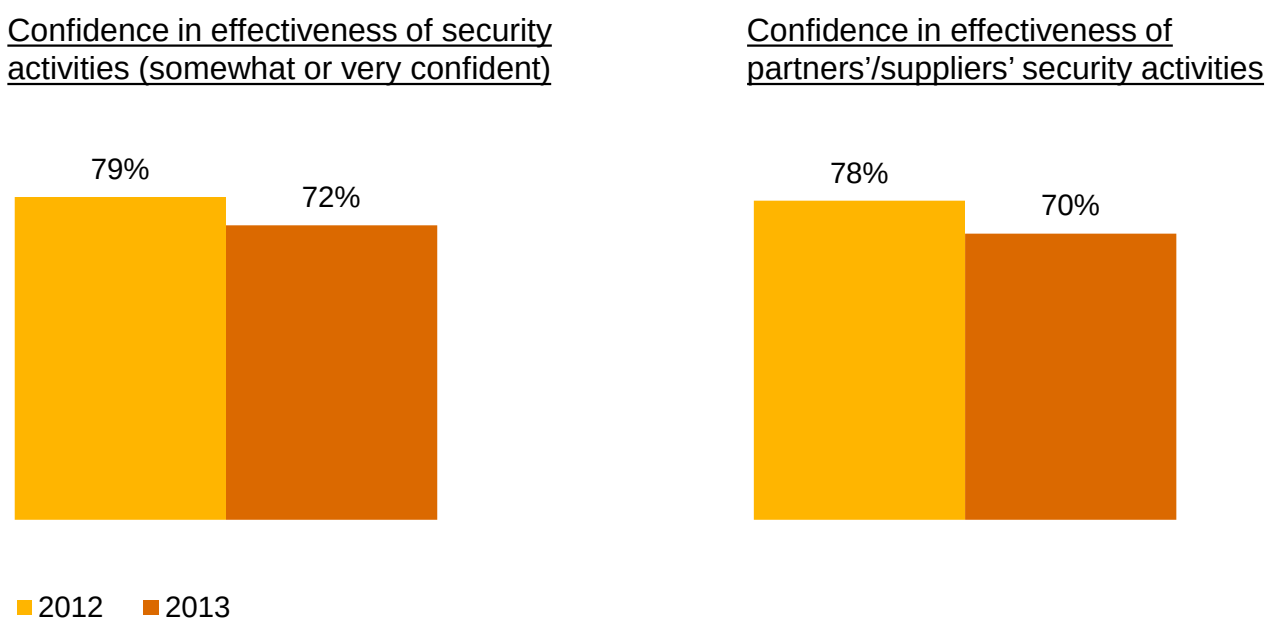
(Numbers reported may not reconcile exactly with raw data due to rounding.)

Section 2

Confidence in an era of advancing risks

Confidence is high: 72% of automotive respondents believe their security activities are effective.

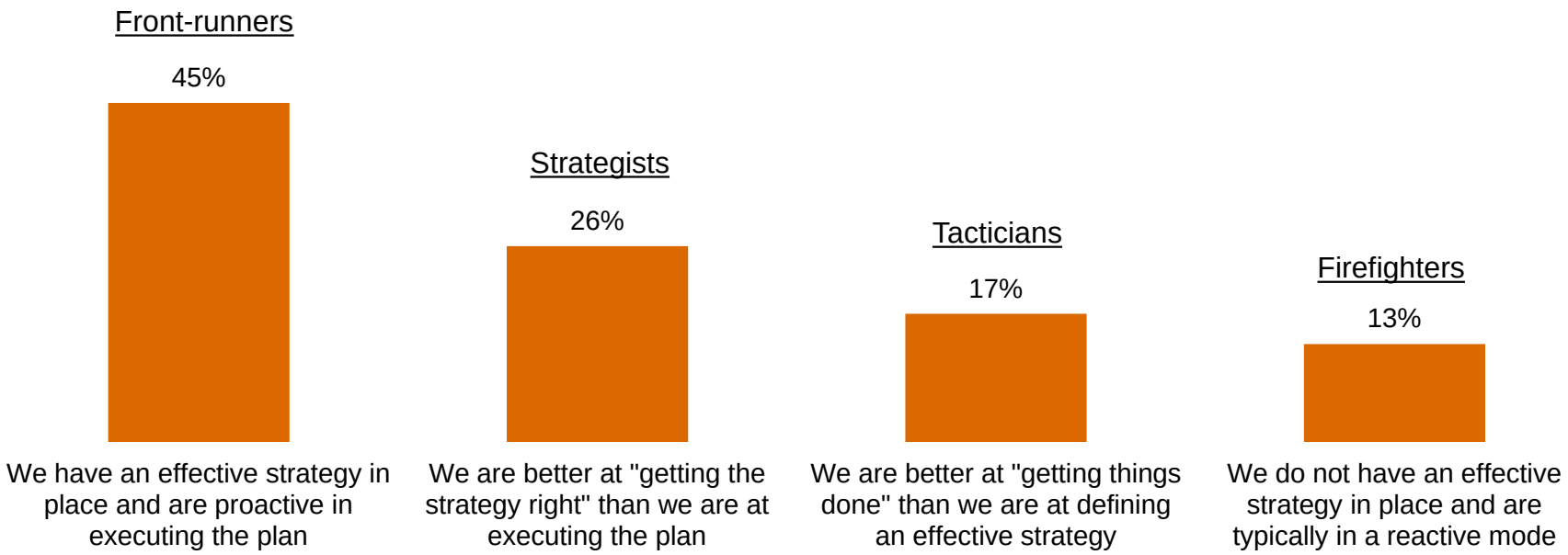
Almost as many—70%—believe that their partners and suppliers have effective security in place. This confidence, however, has declined over last year.



Question 39: "How confident are you that your organization's information security activities are effective?" Question 40: "How confident are you that your partners'/suppliers' information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.")

Many respondents consider themselves "front-runners," ahead of the pack in security strategy and practices.

45% say they have an effective strategy in place and are proactive in executing the plan, up slightly over last year. More than one in four (26%) say they are better at getting the strategy right than executing the plan.



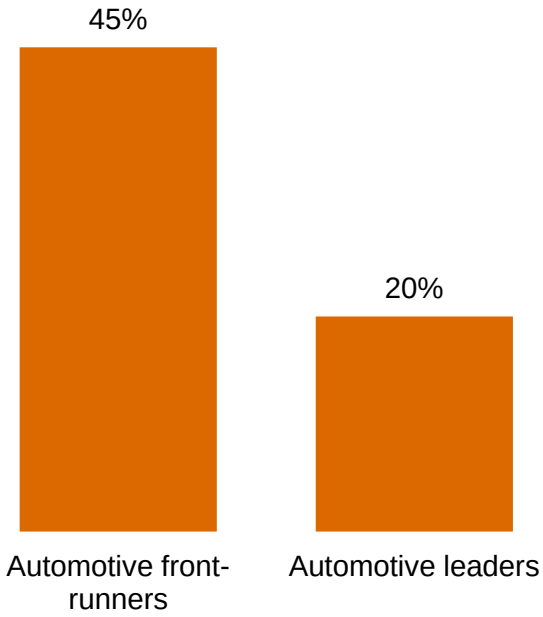
Question 27: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding.)

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured automotive respondents' self-appraisal against four key criteria to filter for leadership. To qualify, automotive companies must:

- Have an overall information security strategy
- Employ CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

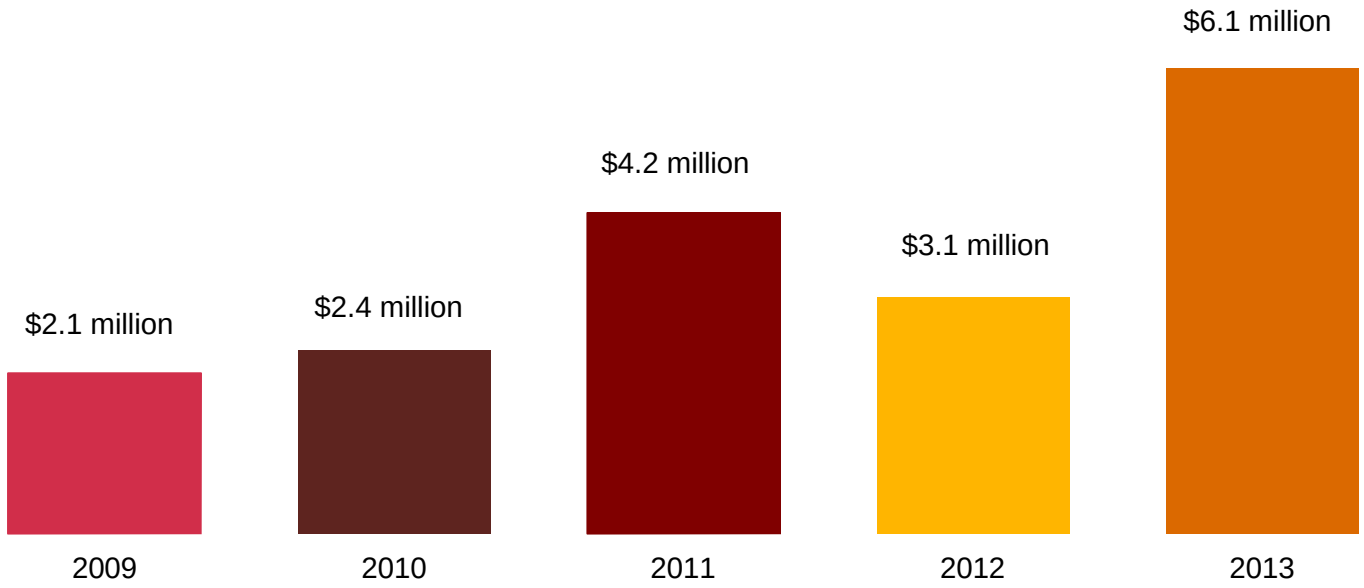


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Automotive information security budgets increase significantly.

Automotive security budgets average $6.1 million this year, a gain of 93% over 2012. Automotive companies understand that today's elevated threat landscape demands a substantial boost in security investment.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

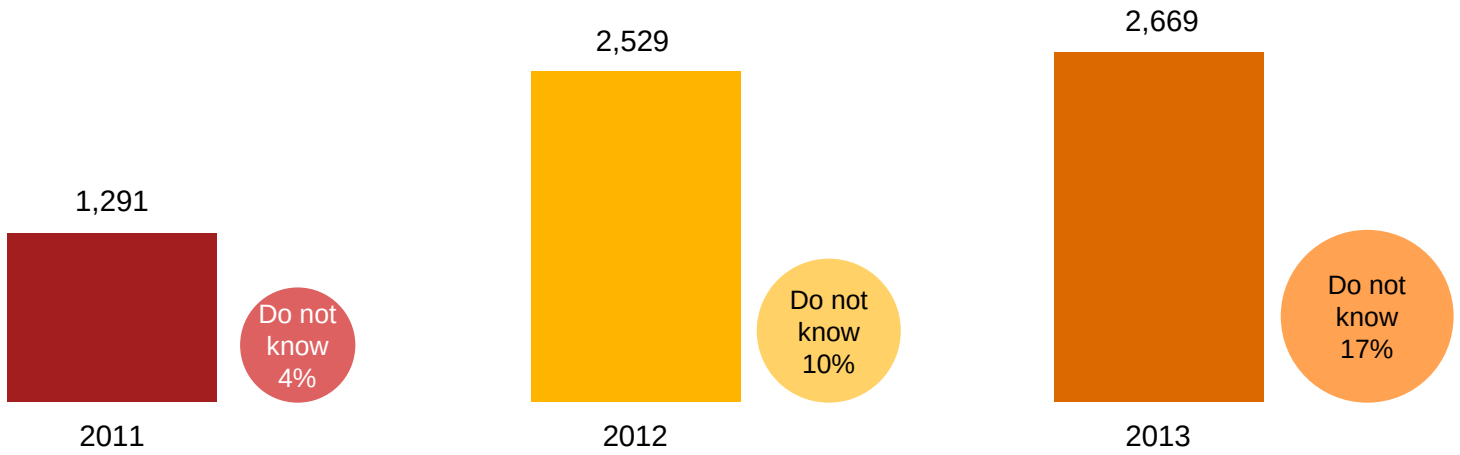
Section 3

Today's incidents, yesterday's strategies

*Automotive companies are detecting more security incidents.**

Automotive respondents detected 6% more incidents in the past 12 months, perhaps an indication of today's elevated threat environment. Given the costs and complexity of responding to incidents, it is surprising that financial losses associated with security incidents decreased 6% over last year.

Average number of security incidents in past 12 months



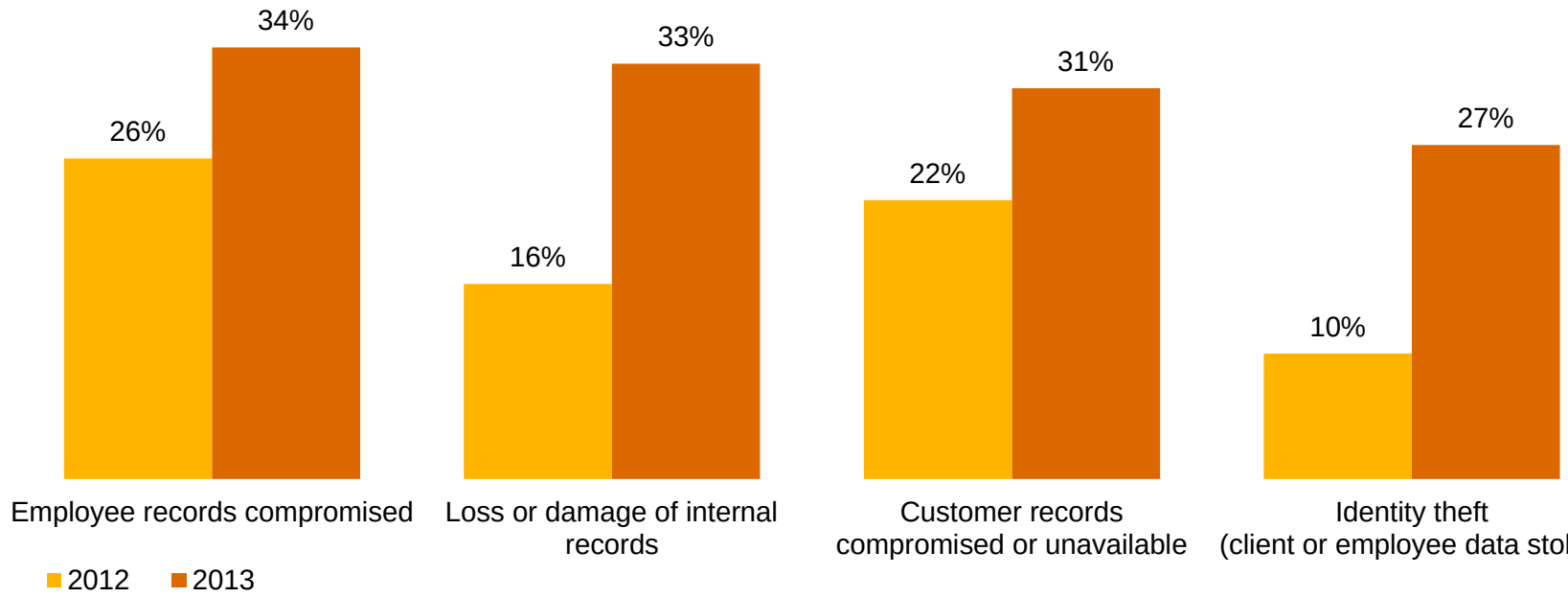
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

Automotive respondents report an increase in data loss as a result of security incidents.

Compromise of employee and customer records increased significantly over last year, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records jumped more than 100%.

Impact of security incidents

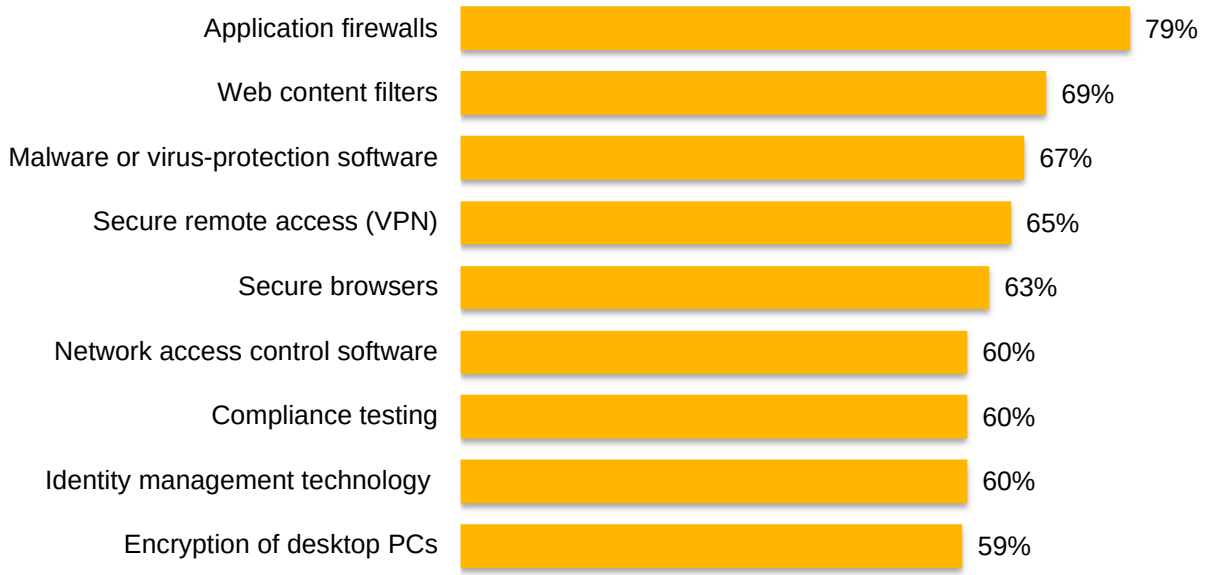


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

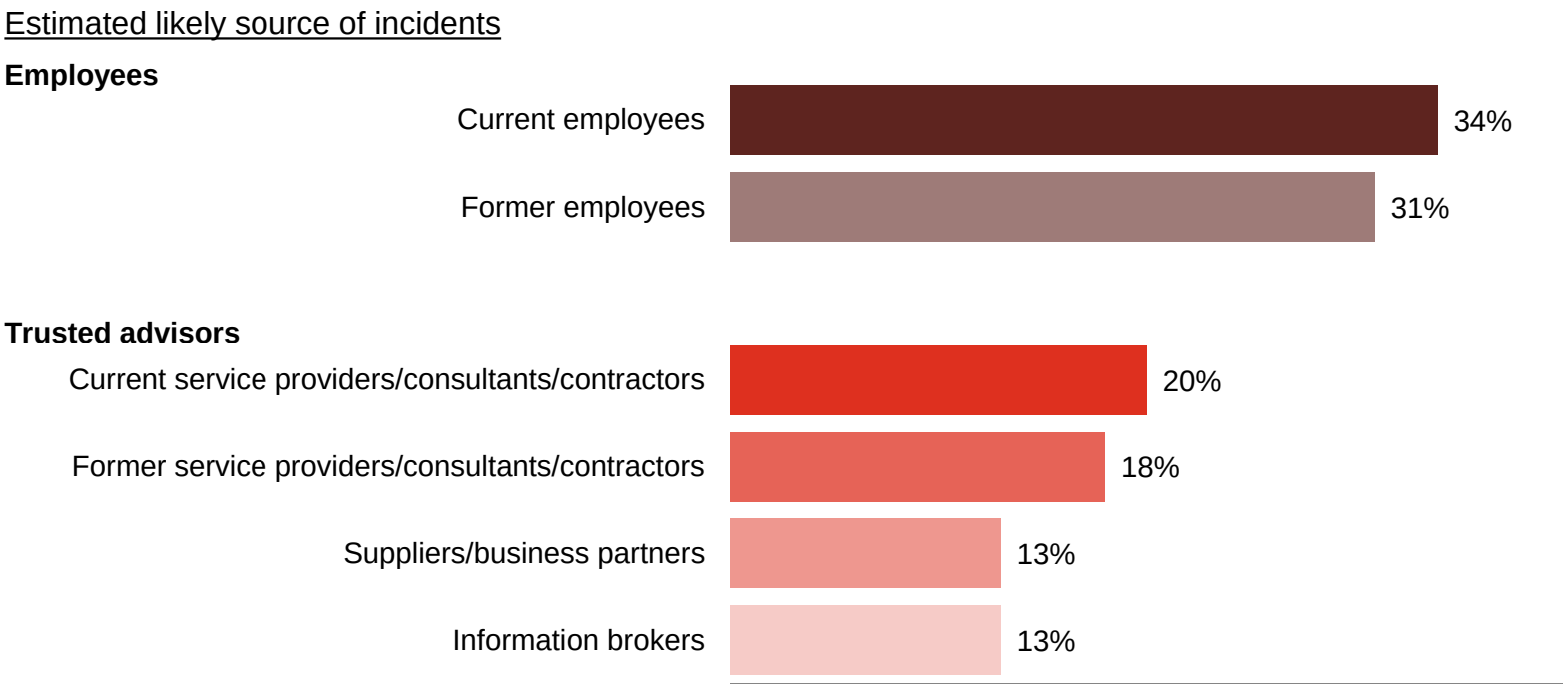
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most Auto respondents.

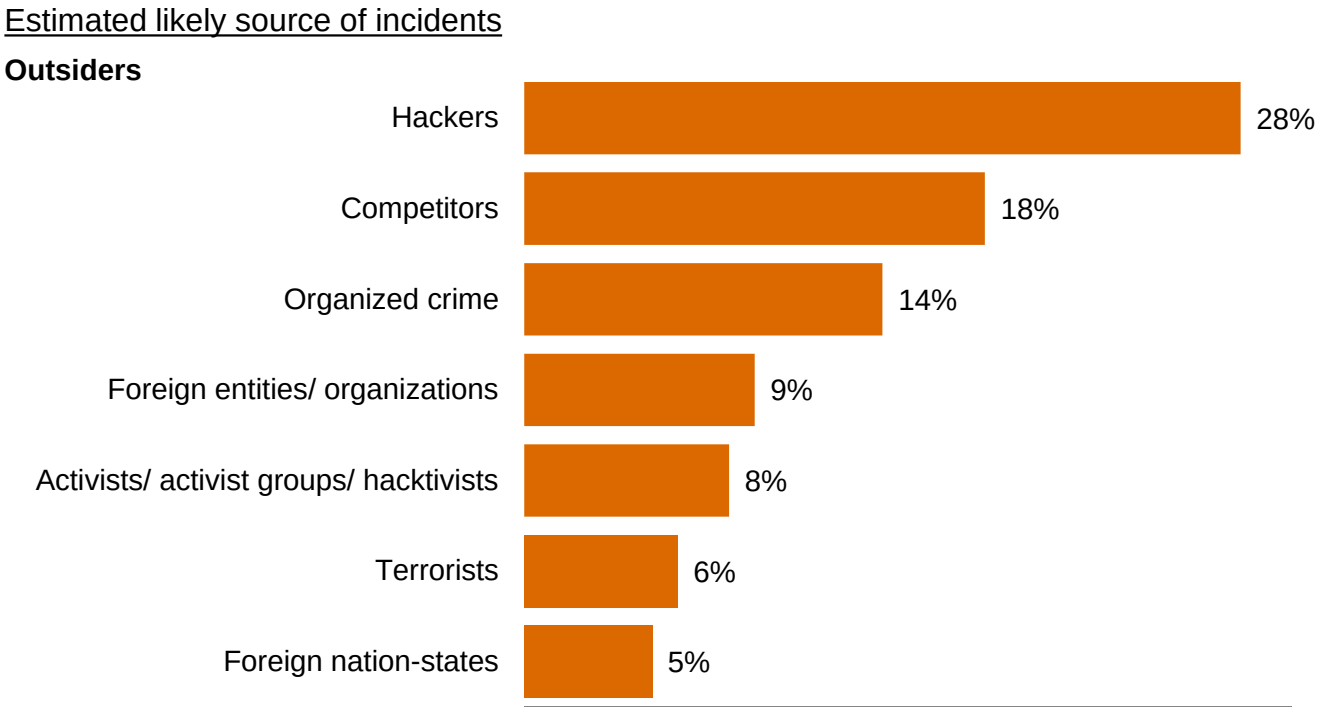
It's the people you know—current and former employees, as well as other insiders—who are most likely to perpetrate security incidents.



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, automotive firms are more likely to be hit by other outsiders.

Only 5% of respondents report security incidents perpetrated by foreign nation-states. Hackers and competitors represent a more likely danger.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

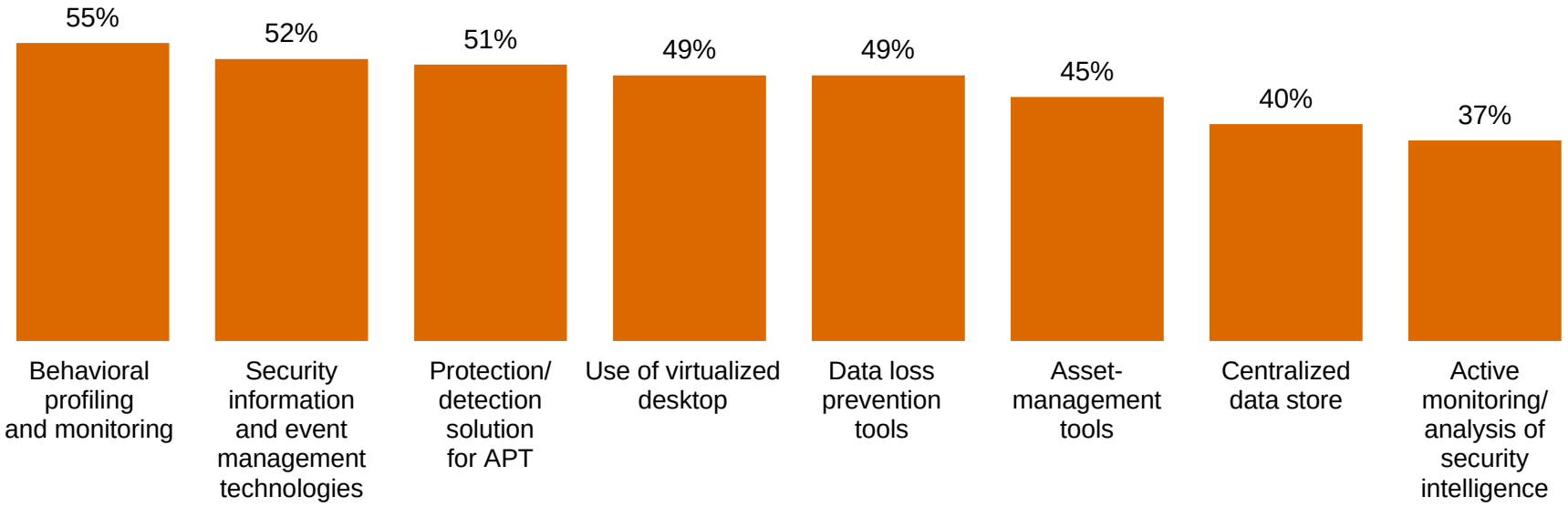
Section 4

A weak defense against adversaries

Many companies have not implemented technologies and processes that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place

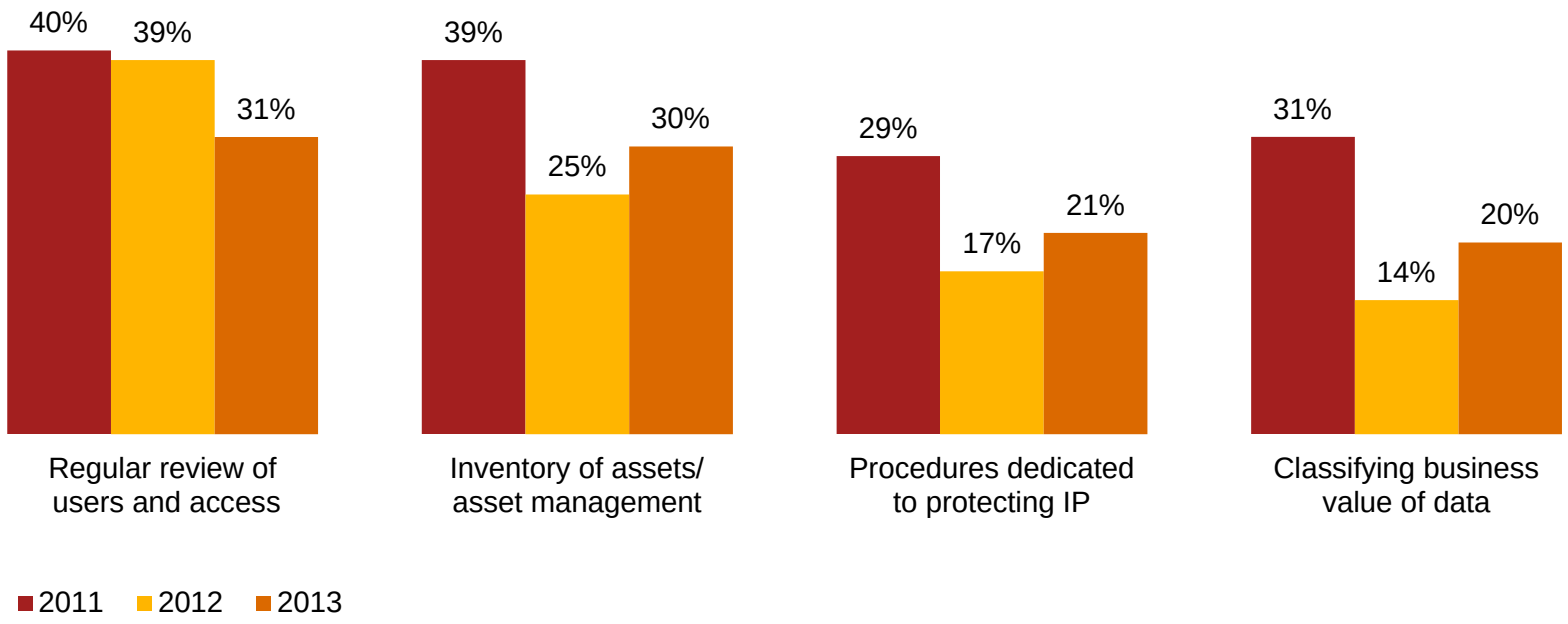


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite the potential consequences, many automotive companies do not adequately safeguard high-value data.

It is imperative that businesses identify, prioritize, and protect their "crown jewels." Most automotive respondents, however, have not yet implemented basic policies necessary to safeguard intellectual property (IP).

Have policies to help safeguard IP and trade secrets

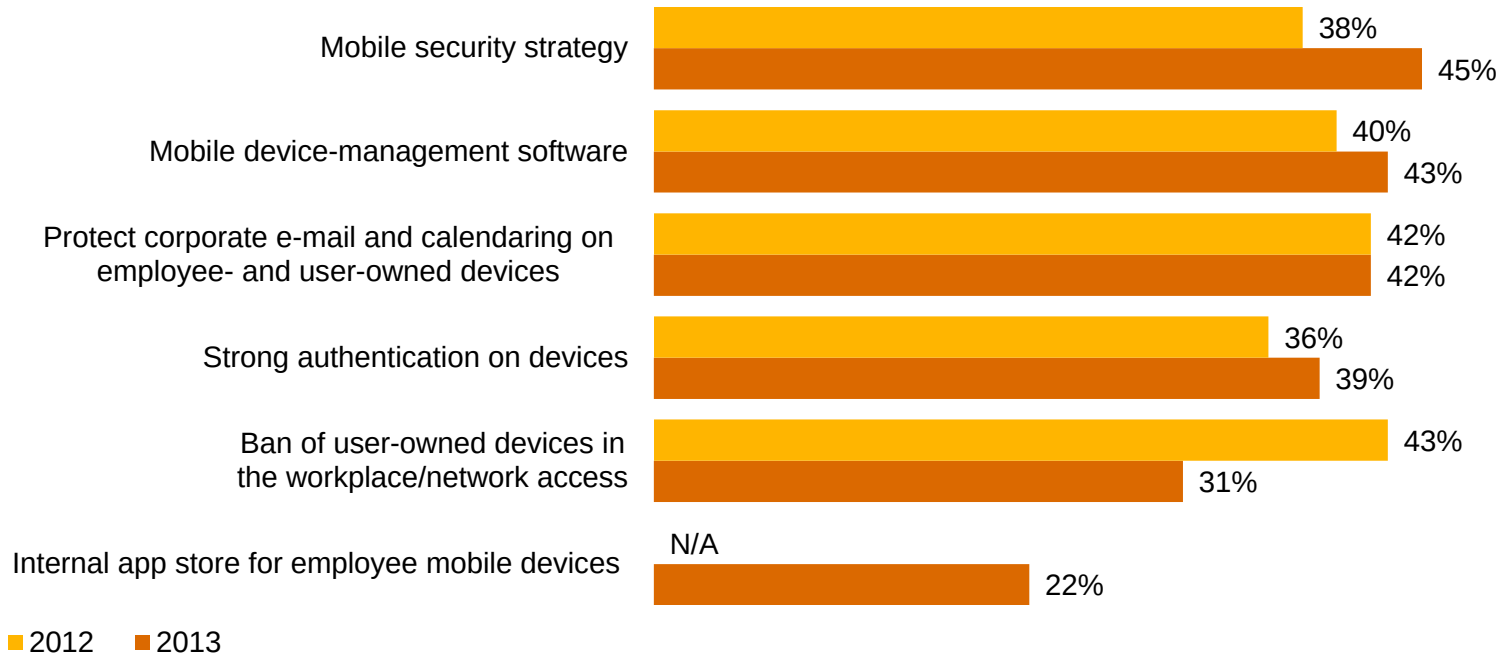


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace with use.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet automotive companies' efforts to implement mobile security programs do not show significant gains over last year, and continue to trail the proliferating use of mobile devices.

Initiatives launched to address mobile security risks

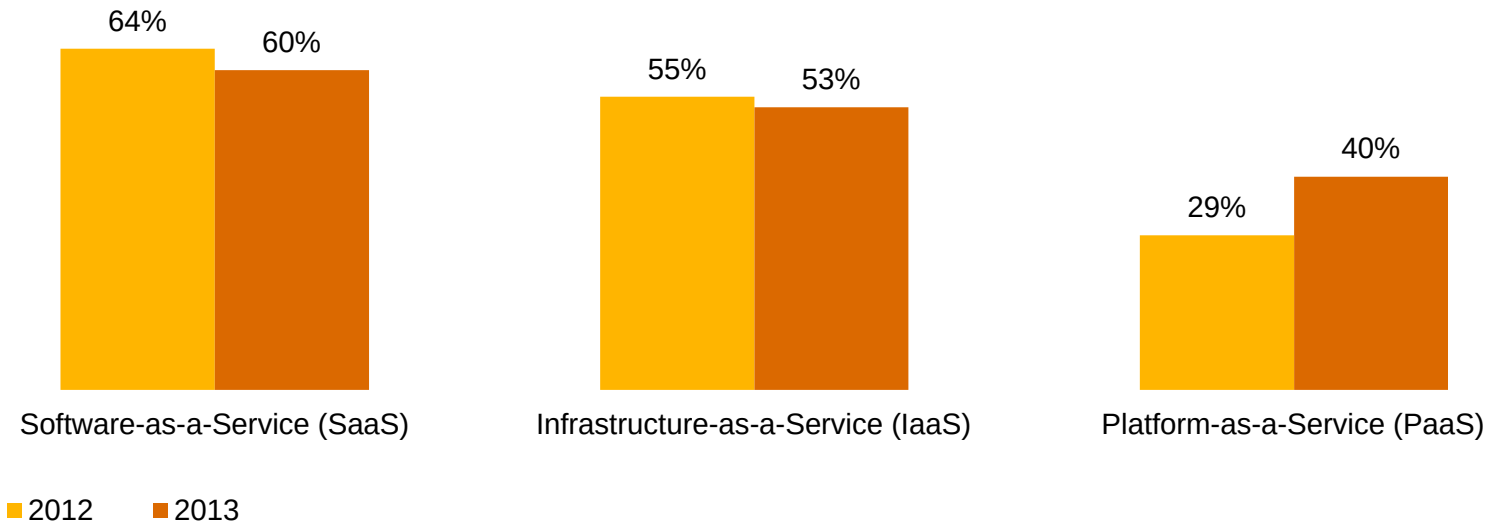


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Almost half of automotive respondents use cloud computing, but they often do not include cloud in their security policies.

While 49% of respondents use cloud services—and 60% say the technology has improved security—only 20% include provisions for cloud in their security policy. SaaS continues to be the most widely implemented cloud service.

Type of cloud service used

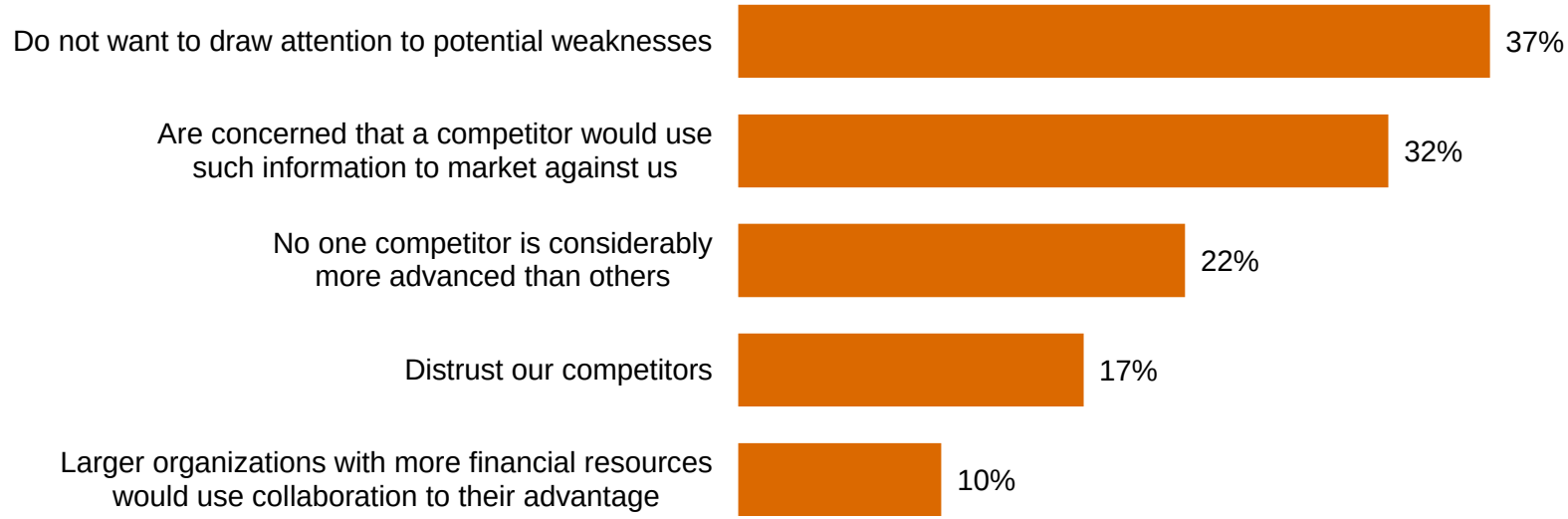


Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

30% of respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.[1]

Reasons for not collaborating on information security



[1] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

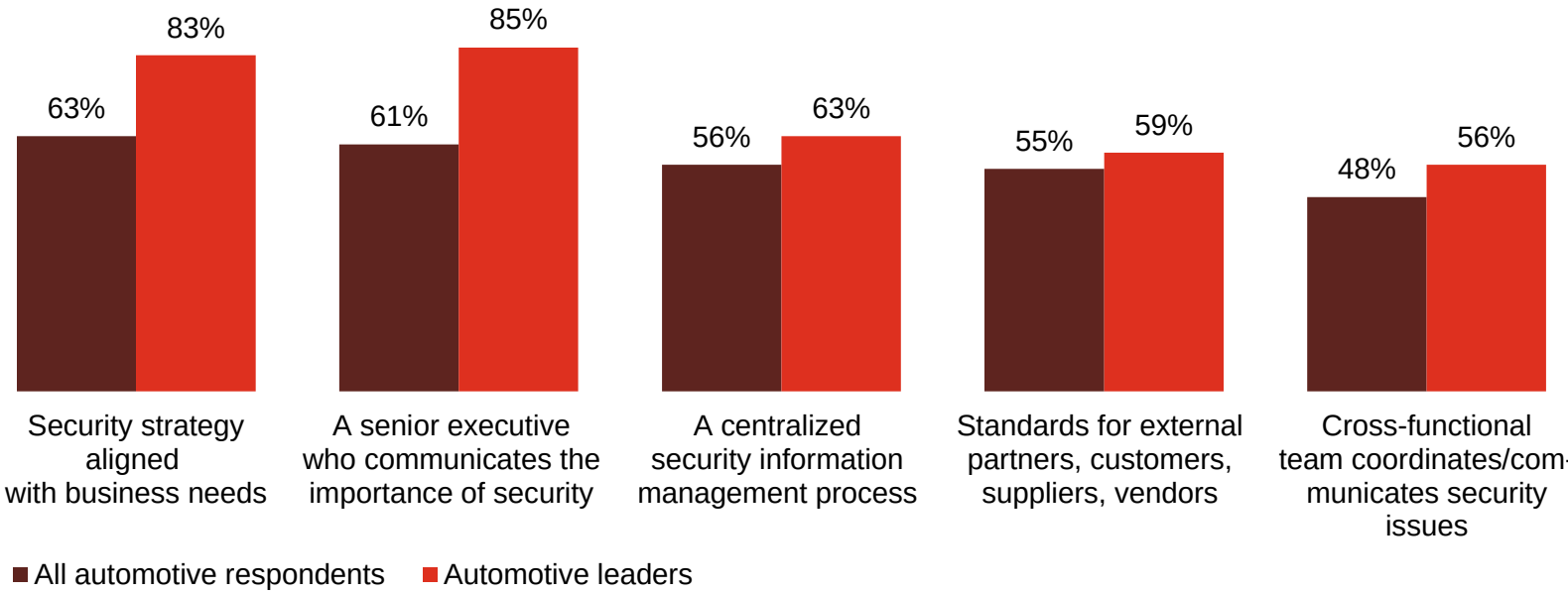
Section 5

Preparing for the threats of tomorrow

Automotive leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT issue.

Aligning security with business needs, setting standards for external partners, and improving executive communications show that leaders, in particular, are rethinking security fundamentals.

Security policies and safeguards currently in place: All respondents vs. leaders



Question 14: "What process information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?"

Many companies have invested in technology safeguards to secure their ecosystems against today's evolving threats.

Automotive leaders are more likely to have implemented these technologies. But given today's elevated threat landscape, *all* companies should strongly consider implementation of these safeguards.

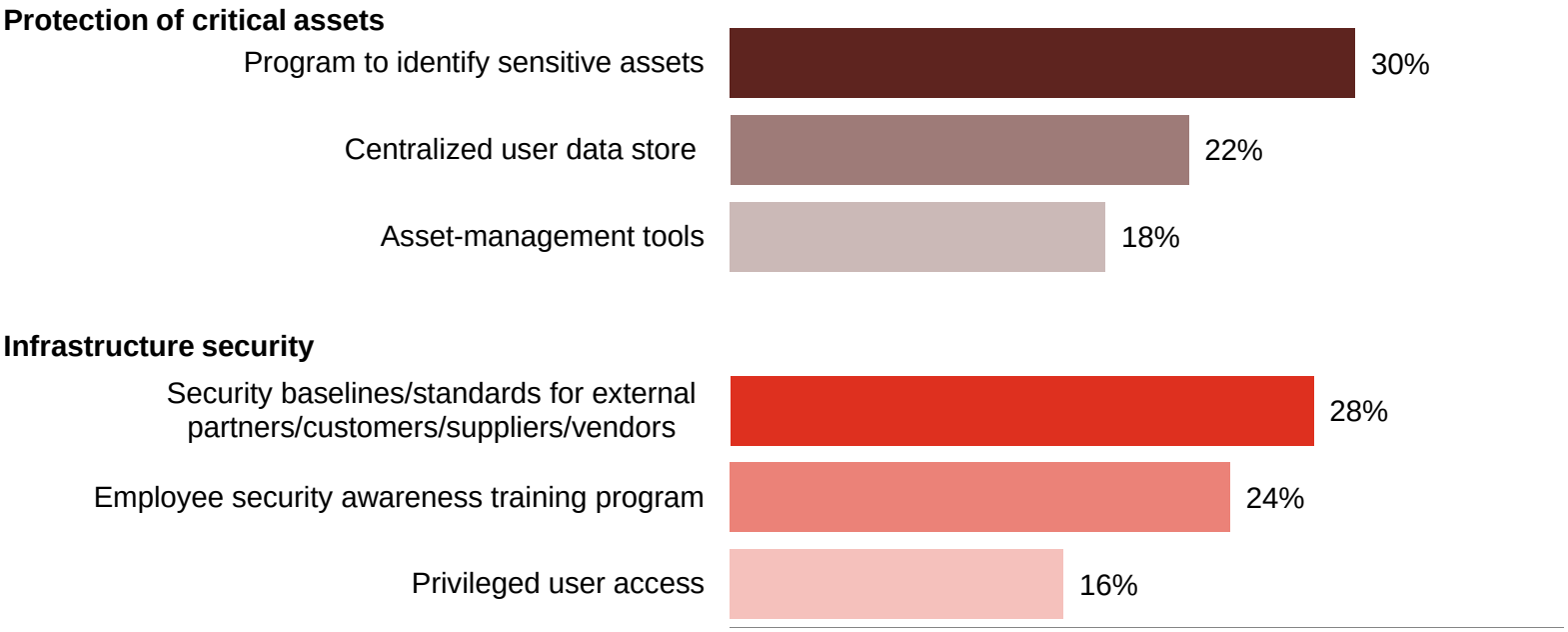
Technology safeguards currently in place	All automotive respondents	Automotive leaders
Malicious code detection tools	70%	85%
Vulnerability scanning tools	53%	71%
Data loss prevention tools	51%	63%
Virtualized desktop interface	51%	71%
Security event correlation tools	50%	68%
Protection/detection solution for APTs	49%	73%
Security information and event management technologies	48%	73%
Mobile device malware detection	46%	61%
Code analysis tools	45%	61%

Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

What business imperatives and processes will automotive respondents prioritize this year?

Some of the highest priorities include technologies that can help the organization protect its most valuable assets and gain strategic advantages.

Safeguards not in place but a top priority over the next 12 months

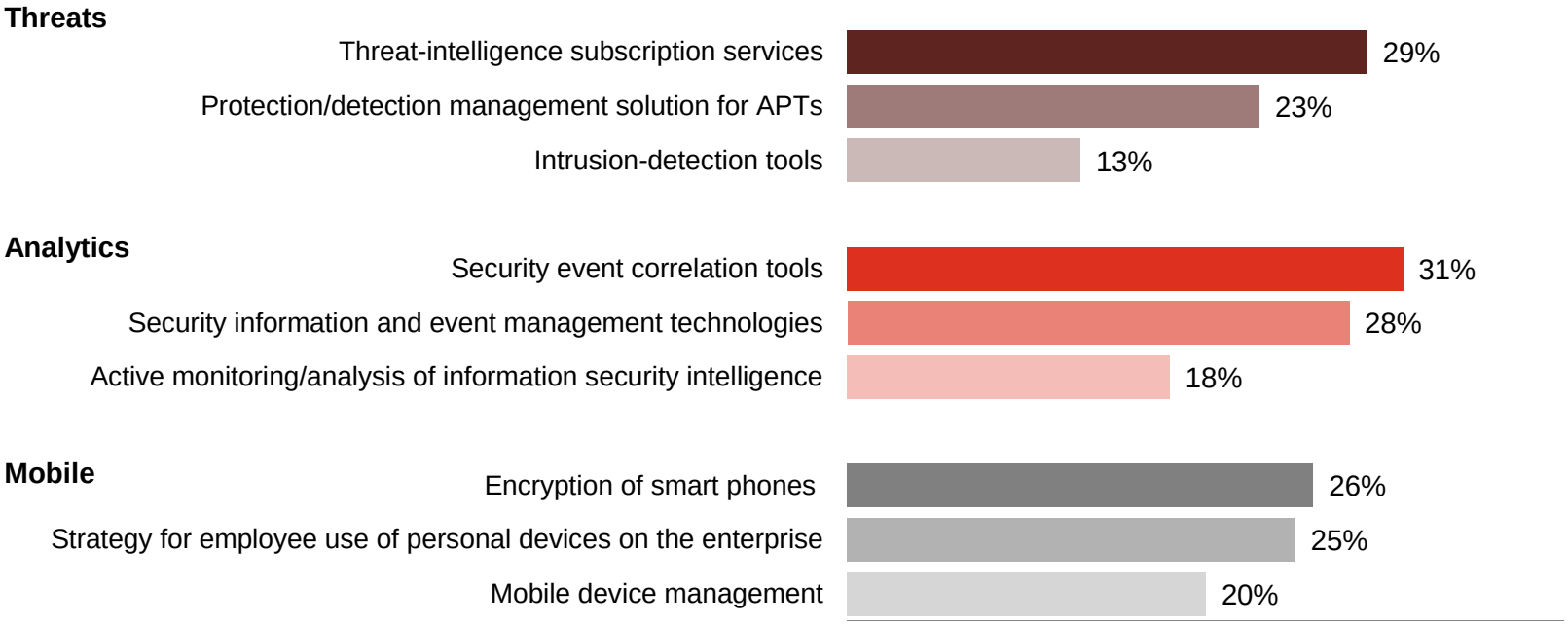


Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?"
Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and automotive companies are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Effective security demands that automotive companies align security policies and spending with business objectives.

Most automotive respondents say security policies and spending are aligned with business objectives. In other words, they are starting to understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

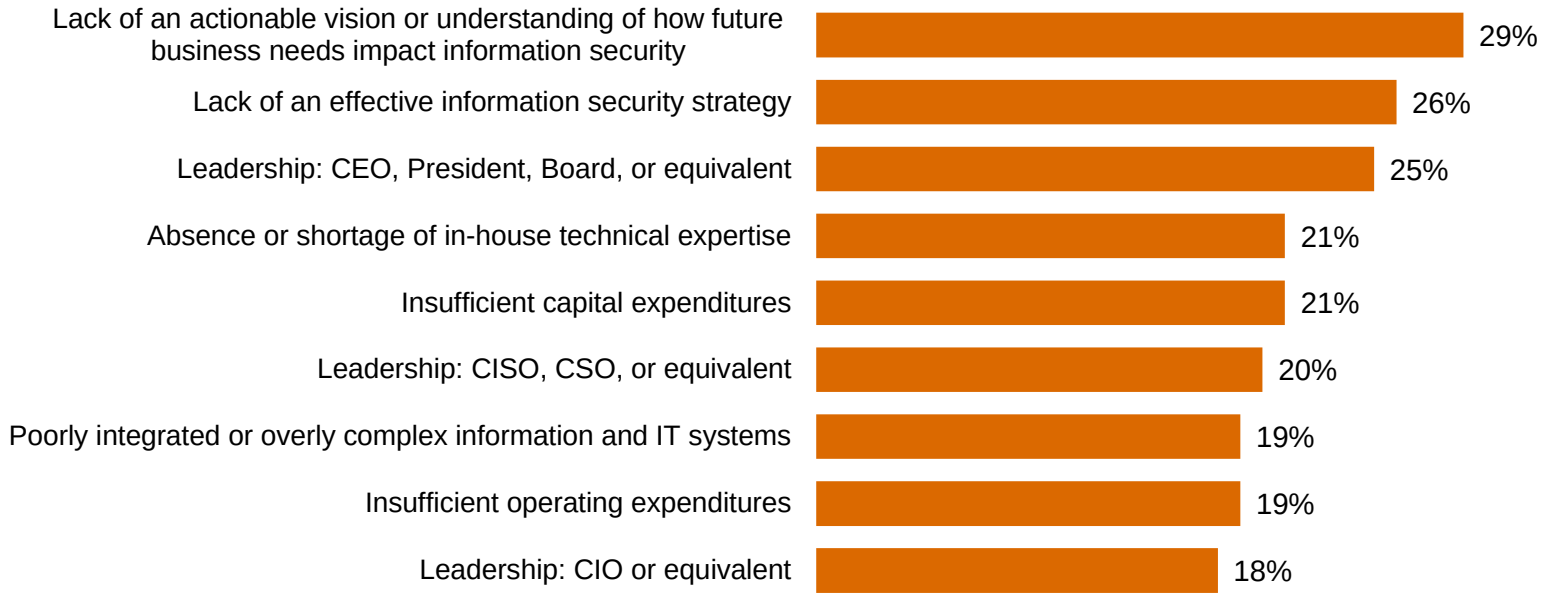
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

A more informed vision of future business needs and an effective IS strategy are needed to improve security.

An evolved approach to security also requires the support of top executives and an adequate budget that is aligned with business needs.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

US Automotive Contacts

Brian Decker
Partner
313.394.6263
brian.d.decker@us.pwc.com

Michael Compton
Principal
313.394.3535
michael.d.compton@us.pwc.com

Rik Boren
Partner
314.206.8899
rik.boren@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

Entertainment & Media

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders can bypass perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global entertainment and media (E&M) industry are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising and confidence is high.

But while many E&M organizations have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased dramatically. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few E&M organizations have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that E&M companies identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

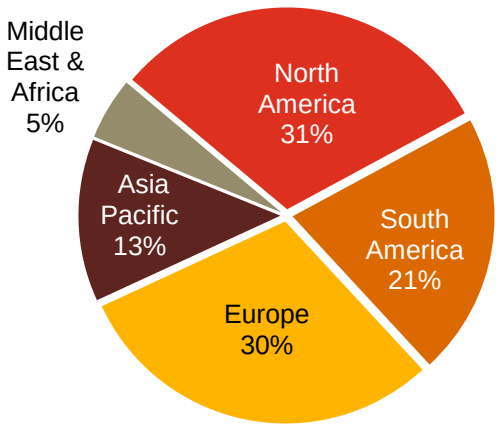
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

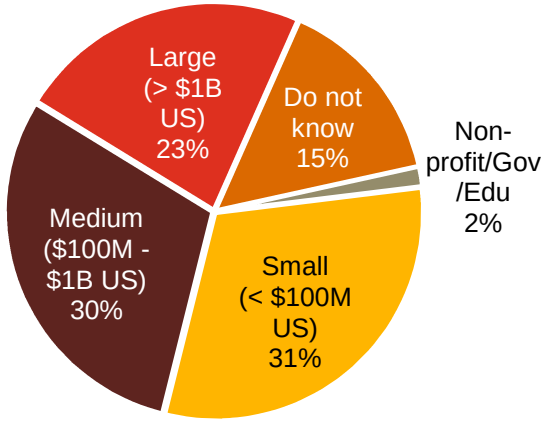
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 221 respondents from the entertainment and media industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

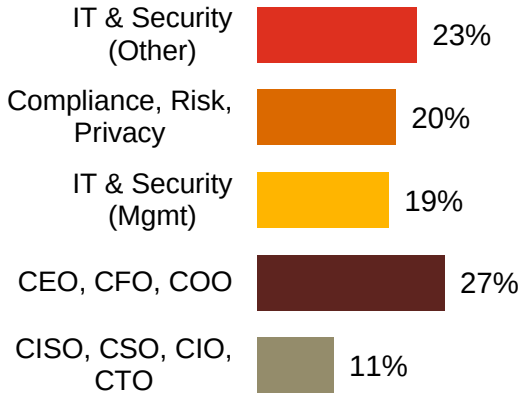
E&M respondents by region of employment



E&M respondents by company revenue size



E&M respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

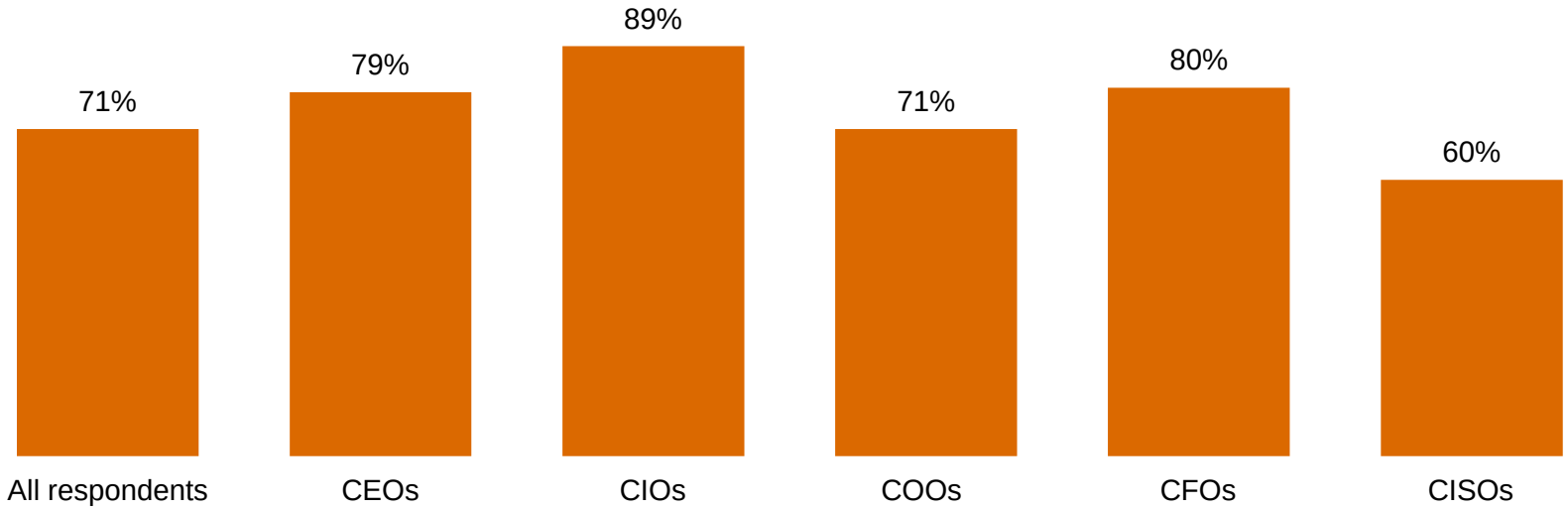
Section 2

Confidence in an era of advancing risks

71% of E&M respondents believe their security activities are effective, and most top executives are even more confident.

Confidence is soaring in the C-suite,* with 79% of E&M CEOs saying they are confident in their security program. Note that CISOs—those with direct responsibility for information security—are the least confident among executives.

Executive confidence in effectiveness of security activities (somewhat or very confident)

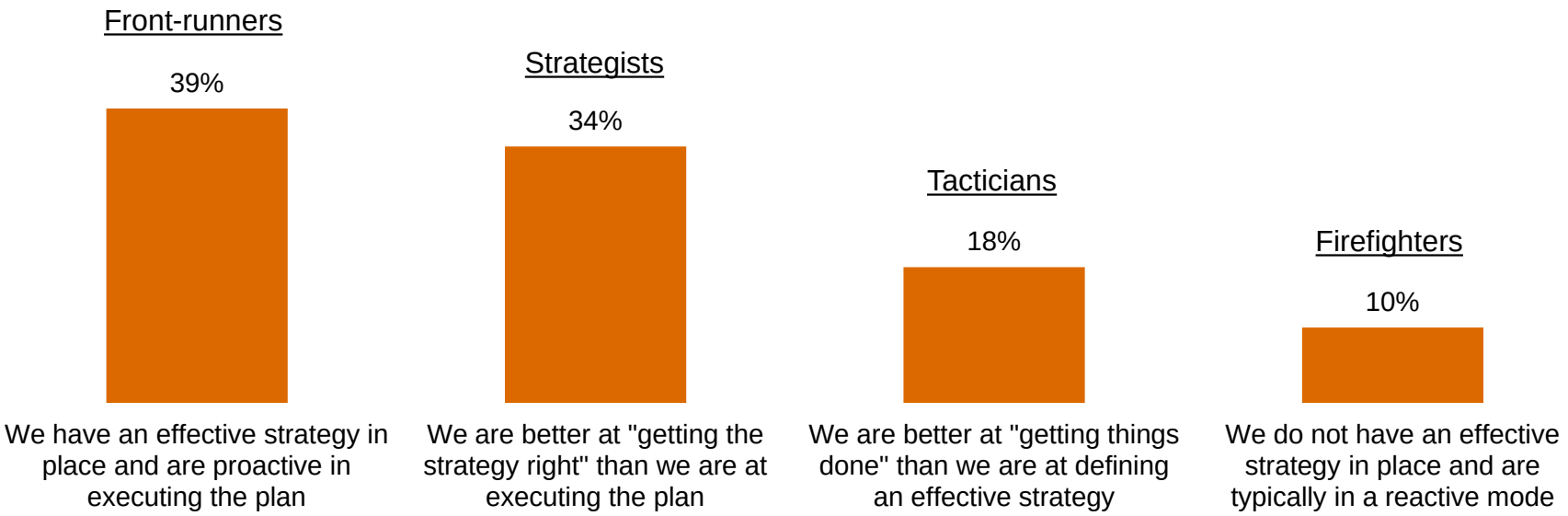


* CEOs, CFOs, and COOs

Question 39: “How confident are you that your organization’s information security activities are effective?” (Respondents who answered “Somewhat confident” or “Very confident.”) Question 1: “My job title most closely resembles”

39% of respondents consider themselves "front-runners," ahead of the pack in security strategy and practices.

More than a third of E&M respondents say they have an effective strategy in place and are proactive in executing the plan, indicating a sense of overall confidence. Those who consider themselves primarily proficient in strategy showed the biggest increase over last year.



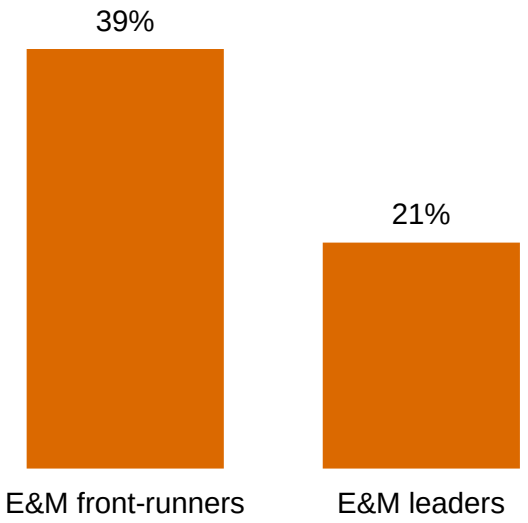
Question 27: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding.)

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured E&M respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

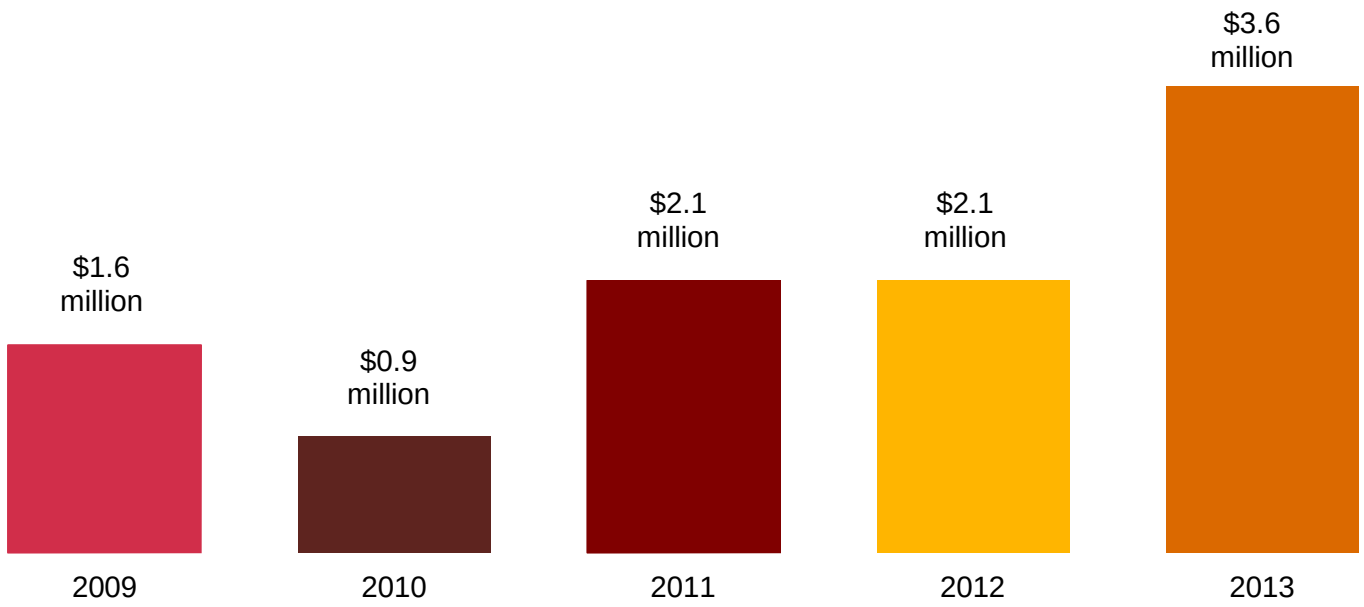


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

E&M information security budgets increase significantly.

E&M security budgets average $3.6 million this year, a gain of 76% over 2012. Organizations understand that today's elevated threat landscape demands a substantial boost in security investment.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

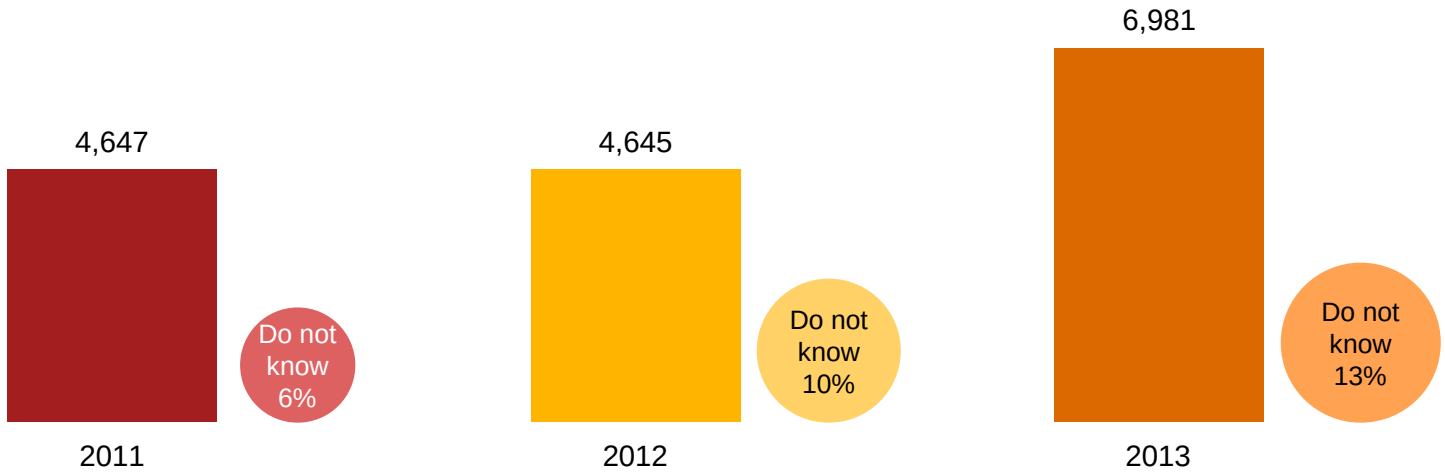
Section 3

Today's incidents, yesterday's strategies

*E&M respondents detect more security incidents.**

E&M respondents detected 50% more security incidents over the past 12 months, perhaps an indication of today's elevated threat environment. Given the costs and complexity of responding to incidents, it is surprising that financial losses associated with security incidents decreased 10% over last year.

Average number of security incidents in past 12 months



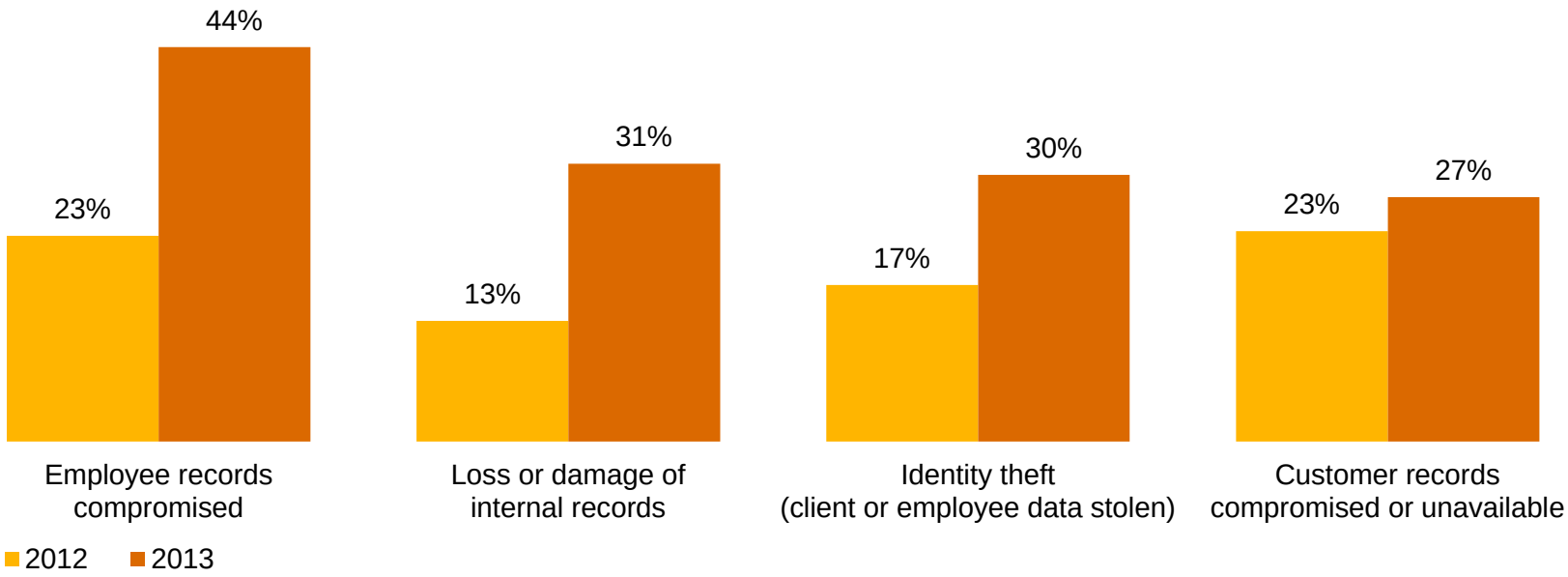
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents."

E&M respondents reported increases in data loss as a result of security incidents.

Compromise of employee information almost doubled over last year, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records jumped 130%.

Impact of security incidents

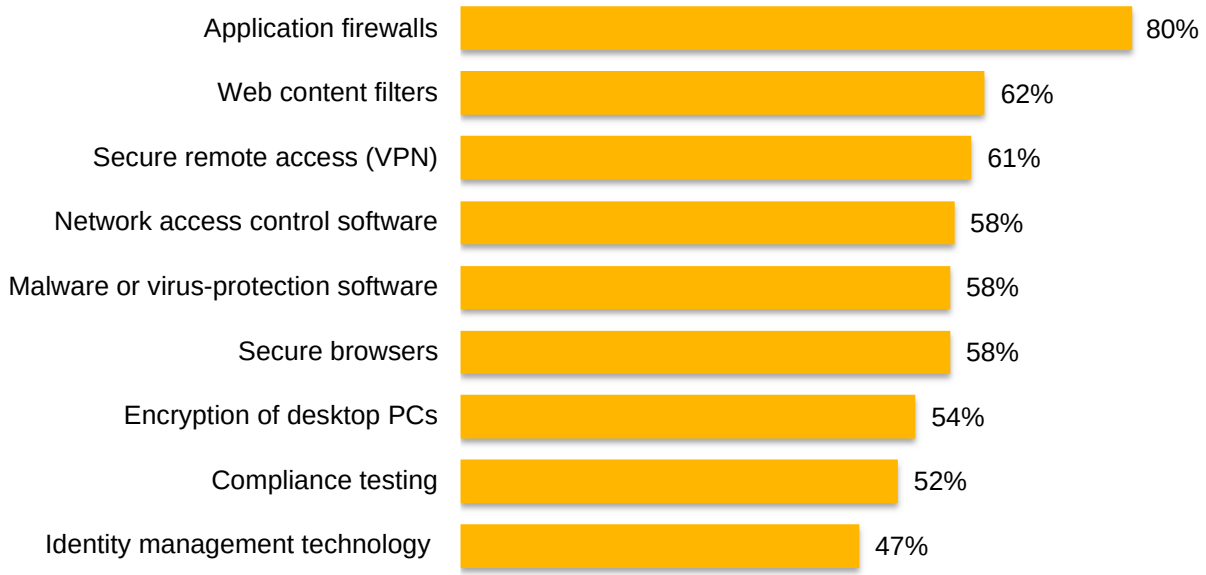


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

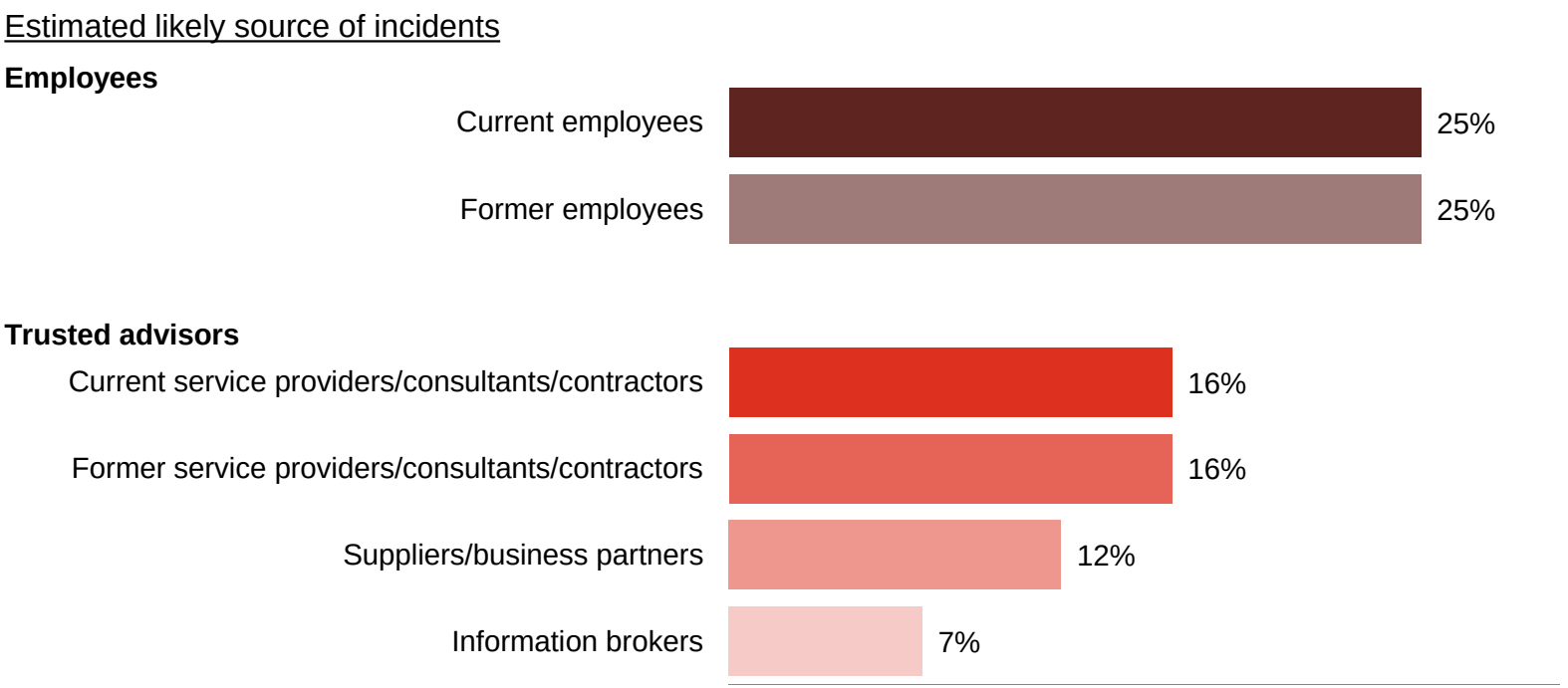
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most E&M respondents.

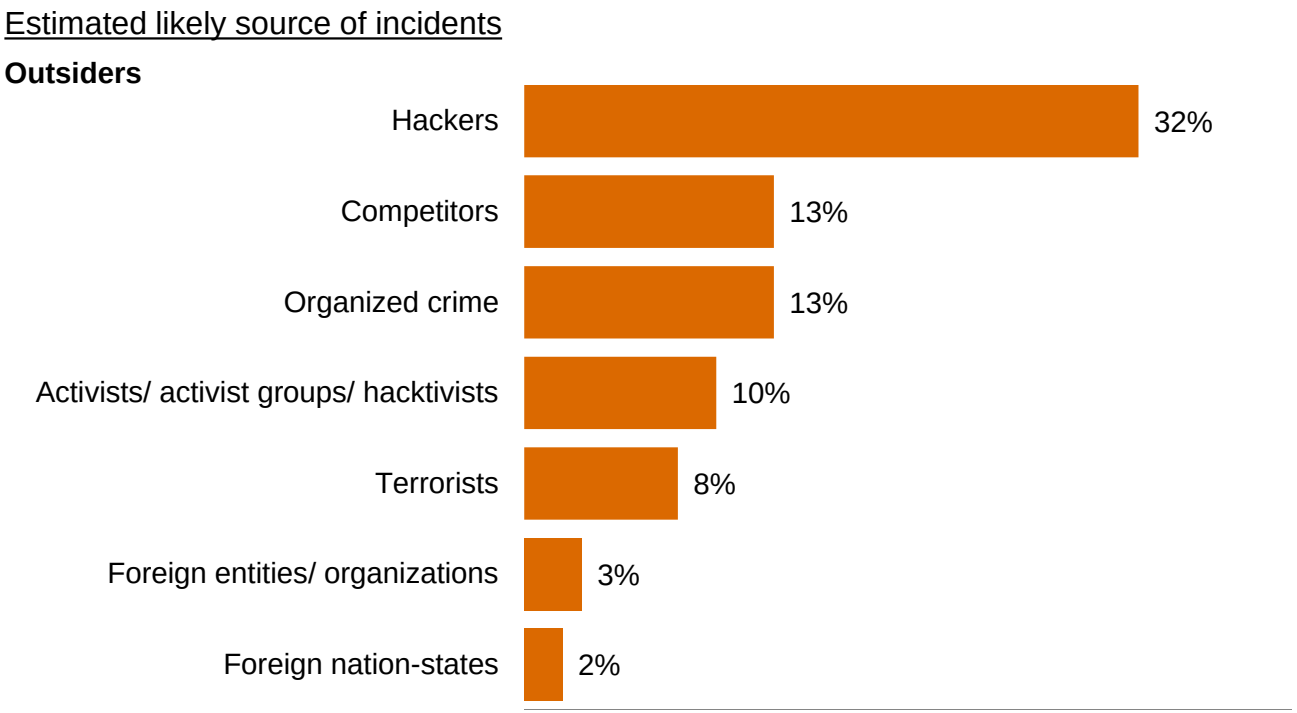
It's the people you know—current and former employees, as well as other insiders—who are most likely to perpetrate security incidents.



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, E&M companies are more likely to be hit by other outsiders.

Only 2% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

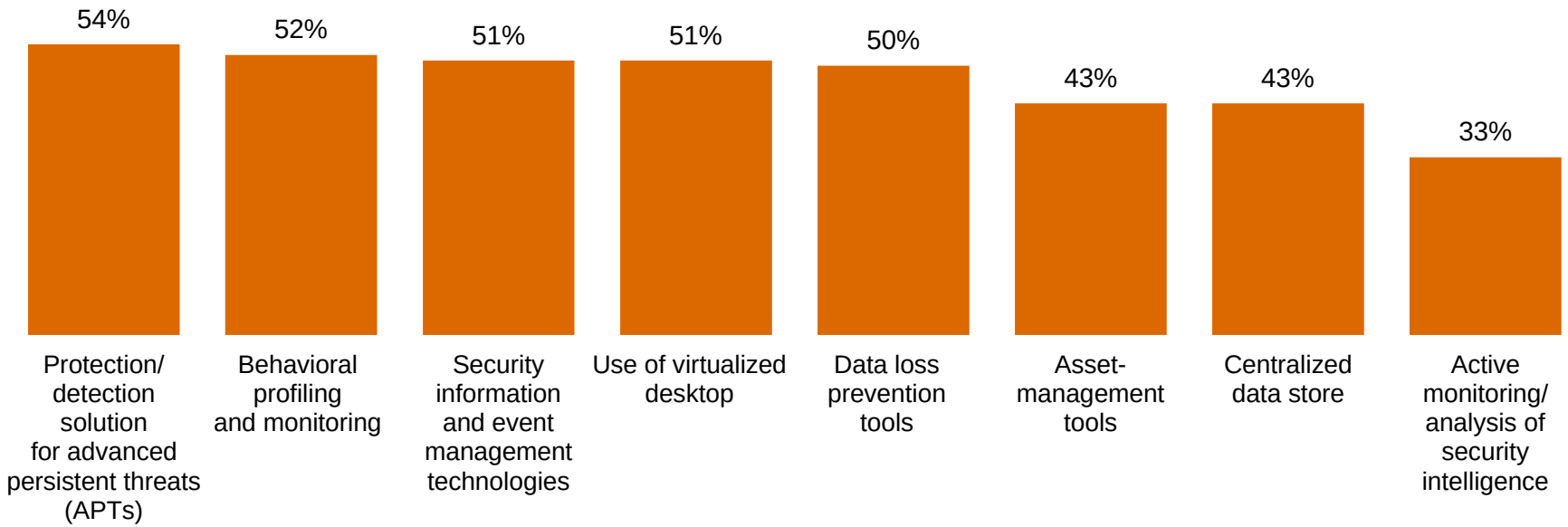
Section 4

A weak defense against adversaries

Many E&M companies have not implemented technologies and processes that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place

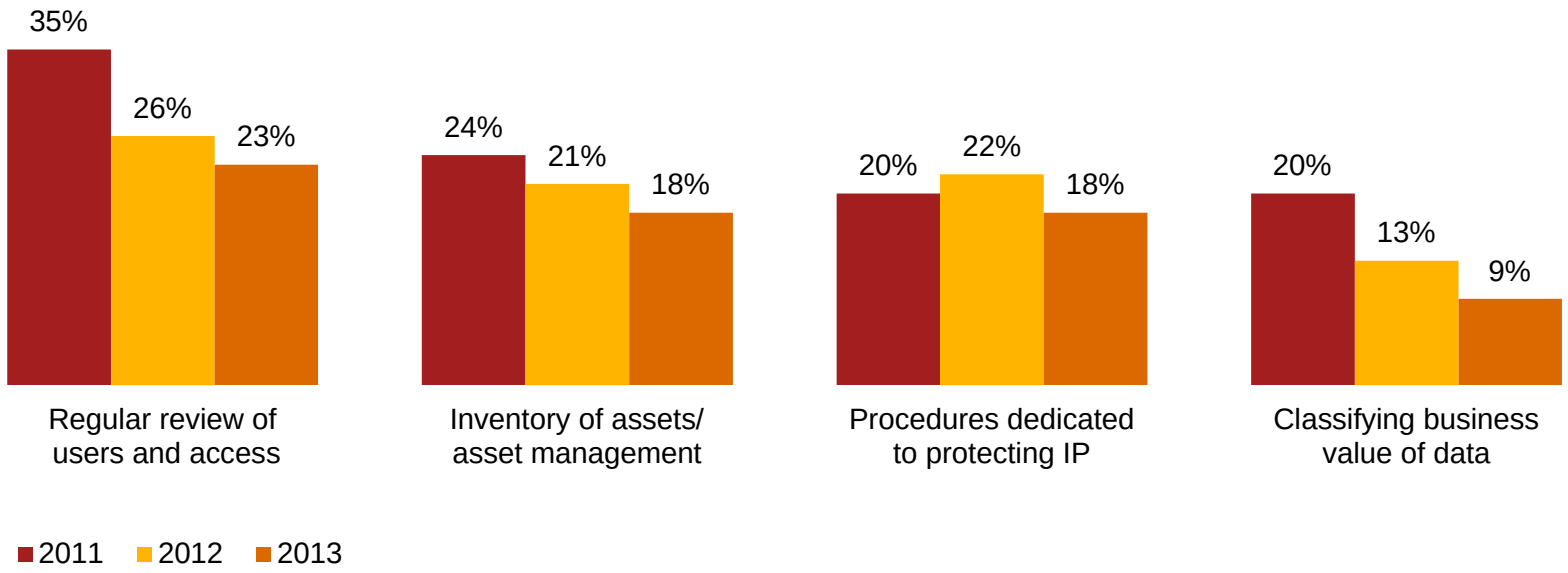


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite the potential consequences, many E&M companies do not adequately safeguard their high-value information.

It is imperative that organizations identify, prioritize, and protect their "crown jewels." But implementation of basic policies to safeguard intellectual property (IP) is declining among E&M respondents.

Have policies to help safeguard IP and trade secrets

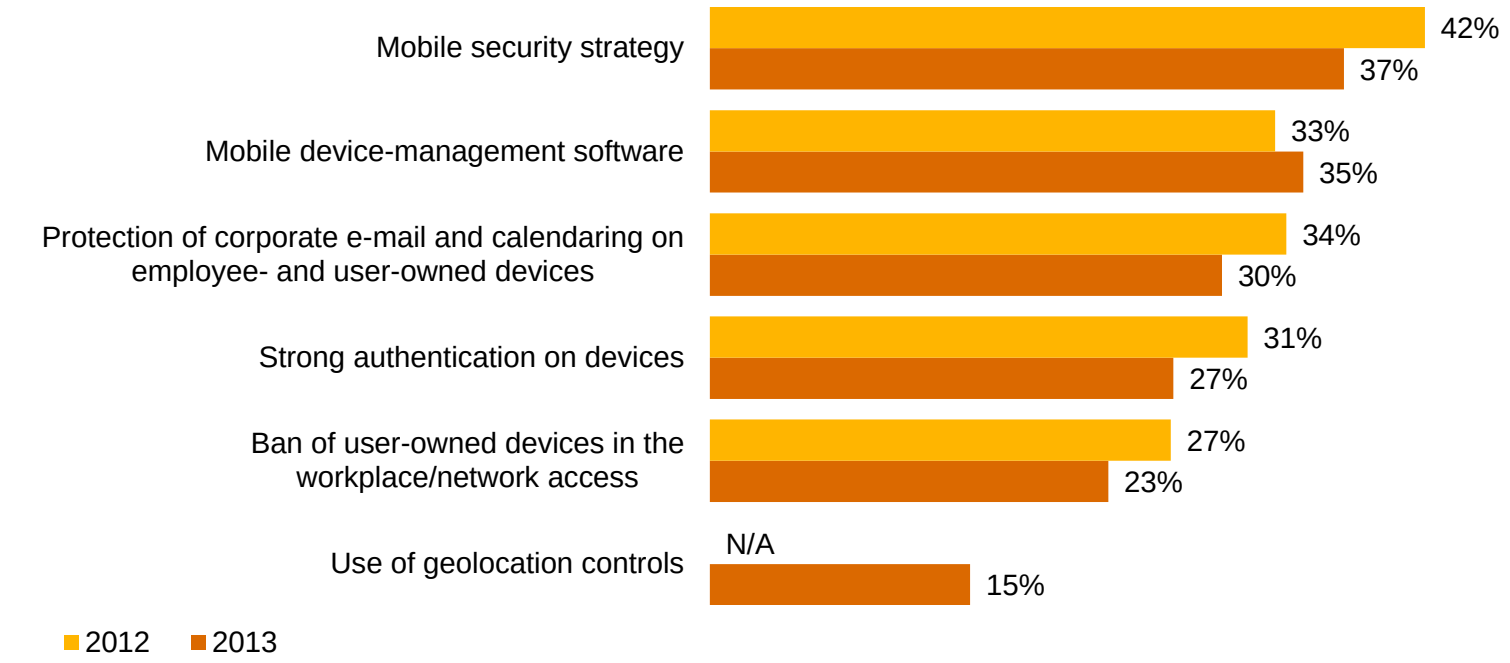


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security initiatives is declining.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet E&M efforts to implement mobile security programs diminished over last year, and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

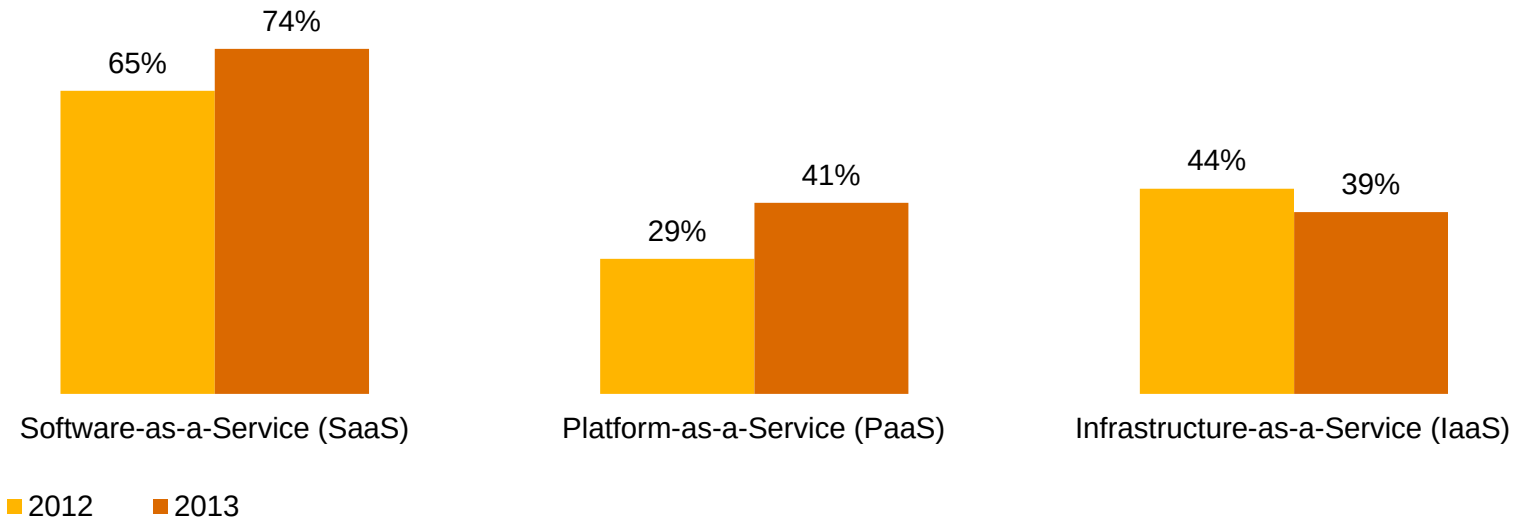


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Almost half of E&M respondents use cloud computing, but they often do not include cloud in their security policies.

While 47% of respondents use cloud services—and 53% say the technology has improved security—only 13% include provisions for cloud in their security policy. Among E&M companies, SaaS remains dominant but PaaS shows solid growth.

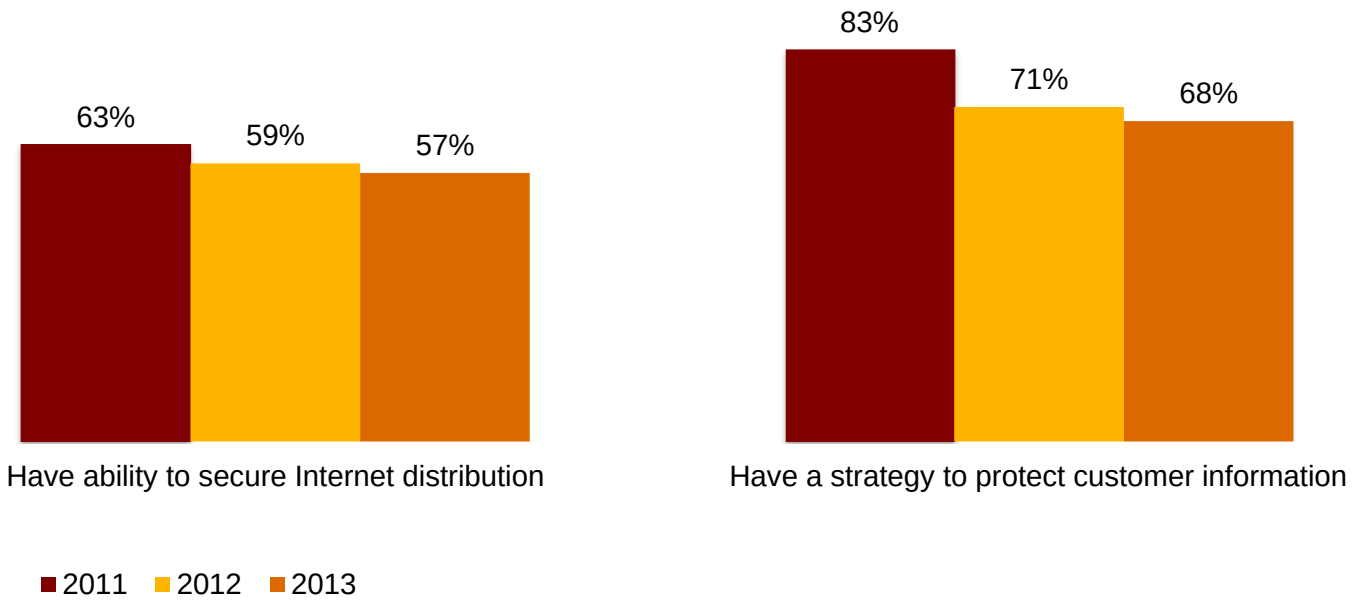
Type of cloud service used



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

Confidence in two key capabilities—secure distribution via the Internet and protection of customer data—is declining.

As E&M content distribution becomes increasingly digital, these declines could ultimately impact the bottom line.



(Asked only of E&M respondents) Question 1: "Do you have adequate in-house security expertise to secure Internet media distribution?"
(Asked only of E&M respondents) Question 4A: "Do you believe your company has a solid strategy for protecting customer information?"
(Not all factors shown.)

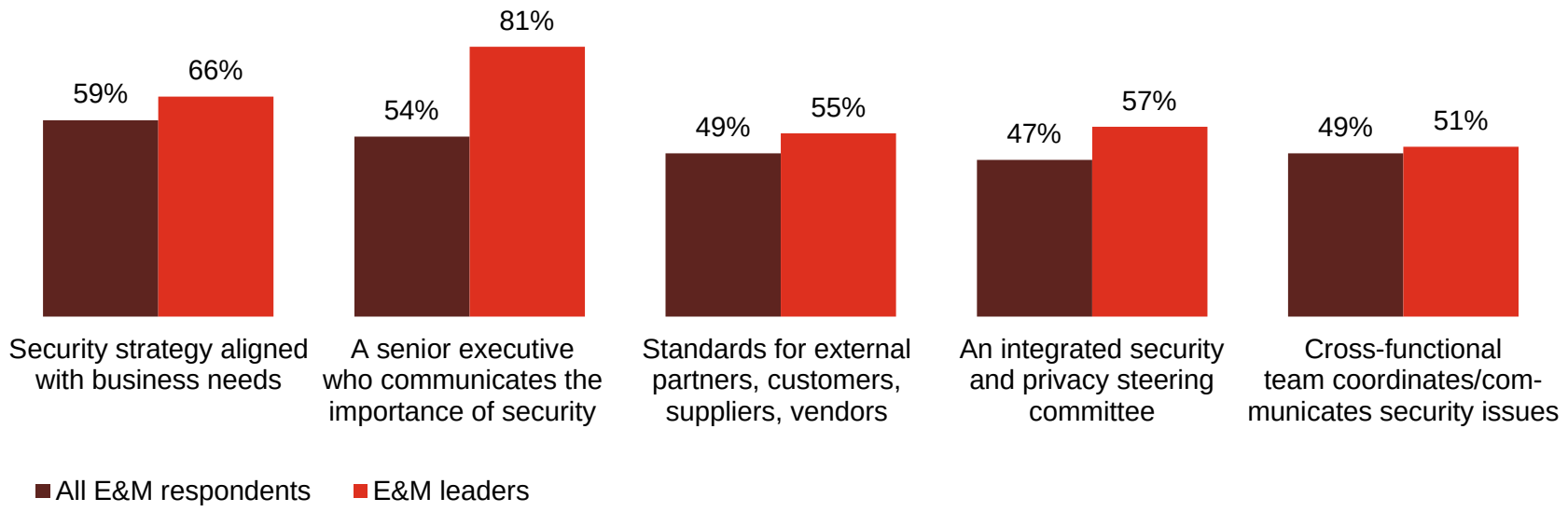
Section 5

Preparing for the threats of tomorrow

E&M leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT challenge.

E&M leaders, in particular, are rethinking the fundamentals of security by aligning security with business needs, setting standards for external partners, and improving communications.

Security policies and safeguards currently in place: All respondents vs. leaders

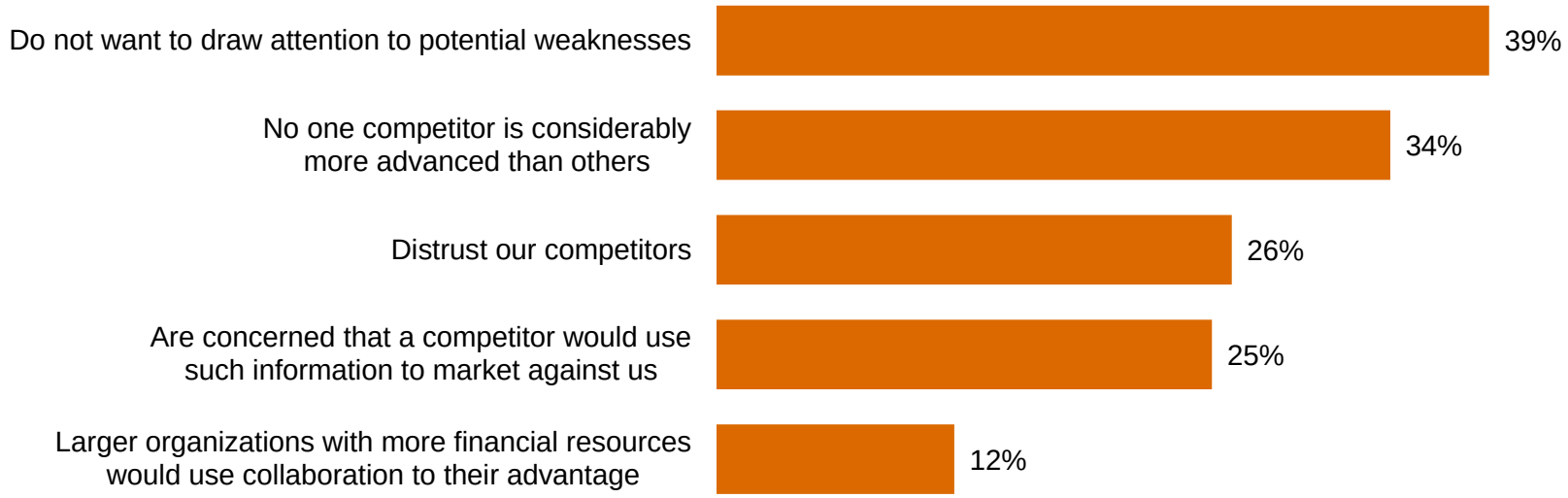


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?"

Most E&M companies share information on piracy efforts, and 51% collaborate with others to improve security.

Collaboration to improve security is essential in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.[1] Some respondents, however are hesitant to share information.

Reasons for not collaborating on information security

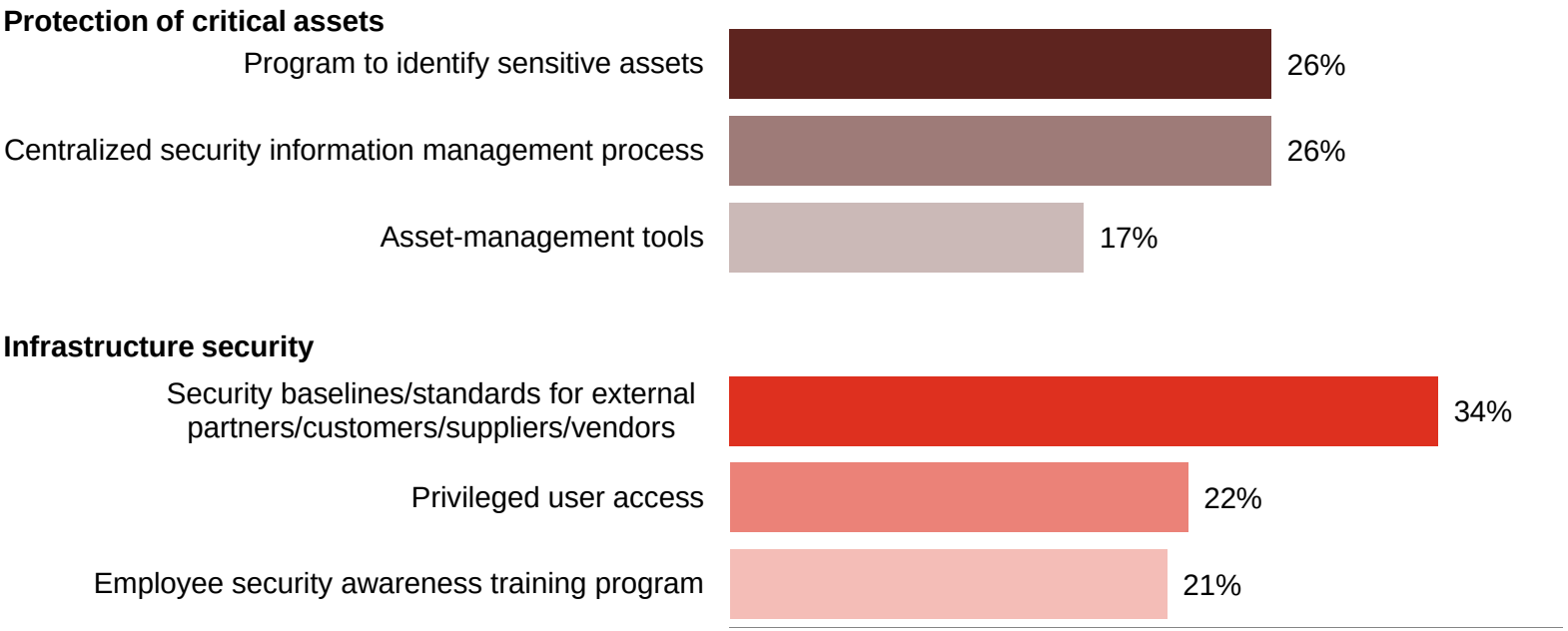


[1] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

What business imperatives and processes will E&M companies prioritize this year?

Some of the highest priorities cited by E&M respondents include technologies that can help identify valuable assets and security standards for third parties.

Safeguards not in place but a top priority over the next 12 months

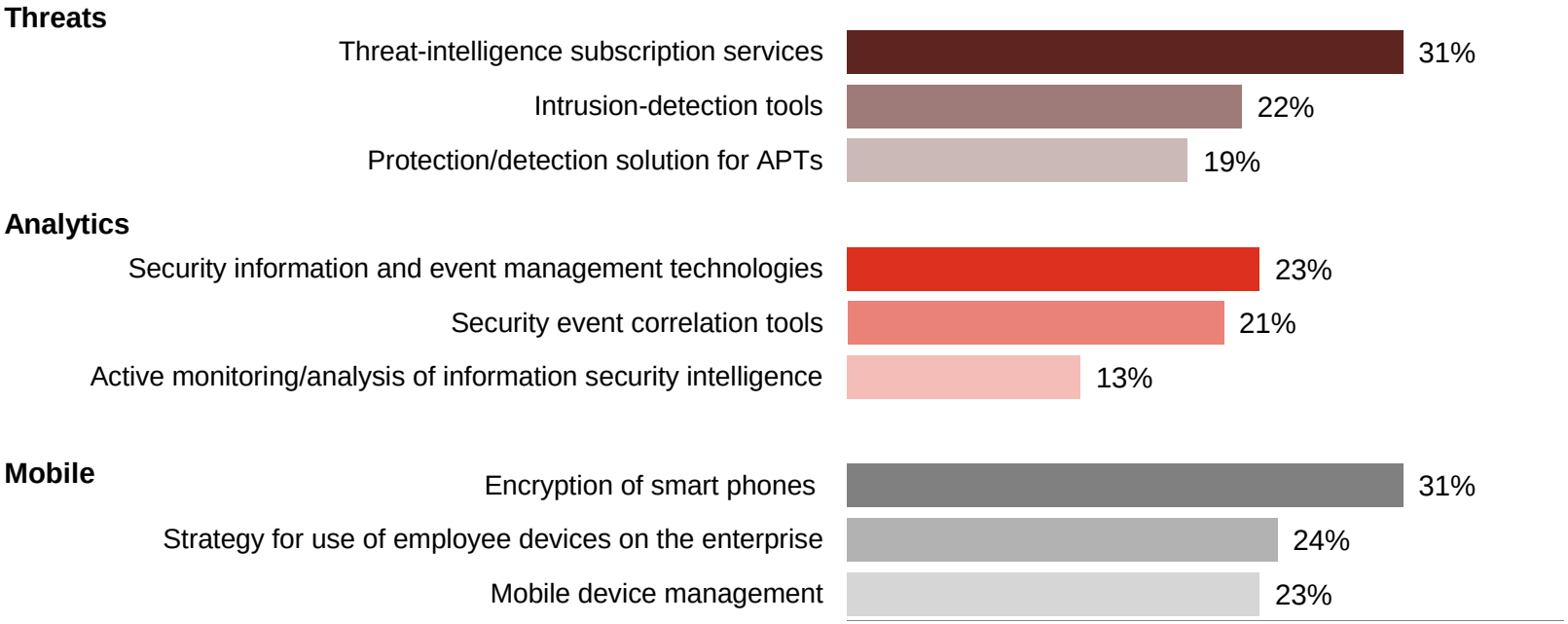


Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?"
Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and E&M organizations are prioritizing technologies that can help them better understand threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Effective security demands that E&M companies align security spending and policies with business objectives.

A higher level of E&M respondents say security spending is aligned with business objectives this year. In other words, they are starting to understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

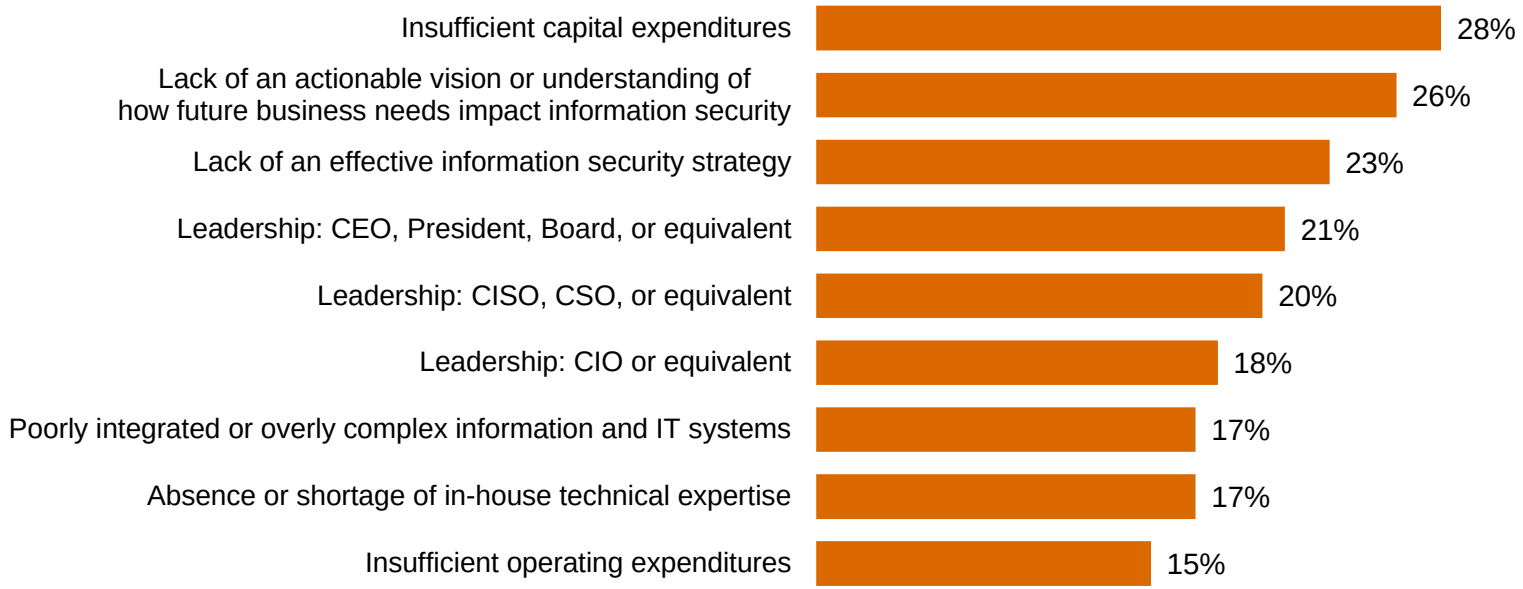
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"
Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?"

More money, an informed vision, and committed leadership are needed to overcome obstacles to advancing security.

These are critical because an evolved approach to security requires the support of informed top executives and an adequate budget that is aligned with business needs.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

US Entertainment & Media Contact

Deborah Bothun
Principal
213.217.3302
deborah.k.bothun@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

PwC

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

Financial Services

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Compliance is not enough as threats advance faster than security.

The results of The Global State of Information Security® Survey 2014 show that financial services companies are spending more on information security than ever before and have improved many of their security practices. Our research indicates that regulatory compliance is still a significant driver of security spend in the industry. Yet incidents continue to occur as a result of unprecedented attacks, ranging from distributed denial of service to advanced persistent threats (APTs).

Why is this happening? We believe most organizations are defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Sophisticated intruders are bypassing traditional perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives or key customers.

38%

of financial services respondents say complex, rapidly evolving, and sophisticated technologies such as high-frequency trading systems pose a "significant challenge" for the future success of their organization's information security.

Gain advantages with an evolved approach to security

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

To be effective, security should move beyond compliance and be aligned with the business—and championed by the CEO and board—to emphasize threat awareness, asset protection, and motives of opponents. Security risks, including evolving cybersecurity threats, should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels, similar to how credit losses are managed.

In this new model of information security, knowledge is power. Seize it.

The new realities of cyber threats

Disappearing boundaries: Cyber threats destroy or dissolve boundaries, making attribution or legal action very difficult.

Shrinking cost and effort: The cost of developing and launching cyber campaigns is decreasing drastically, making them easily scalable and customizable.

Cheap and easy intelligence: Accessible 24/7, socially connected networks provide a rich source of data and an easy attack platform.

Far-reaching impact: Attack profiles and targets have matured to impact brand, reputation, intellectual property, and the bottom line.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

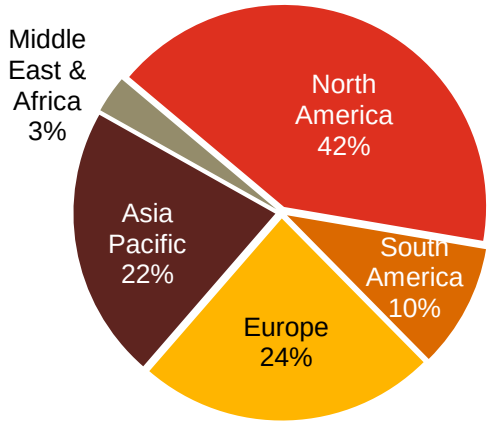
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

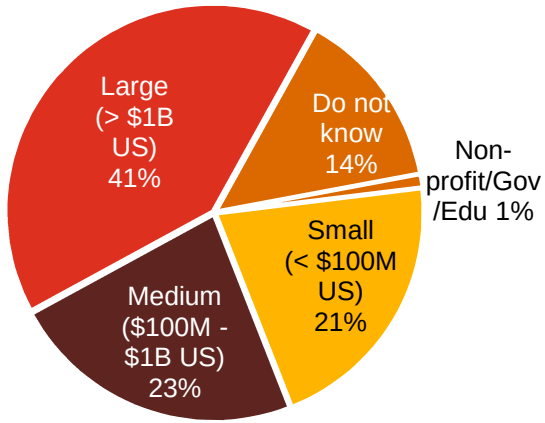
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 993 respondents from the financial services industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

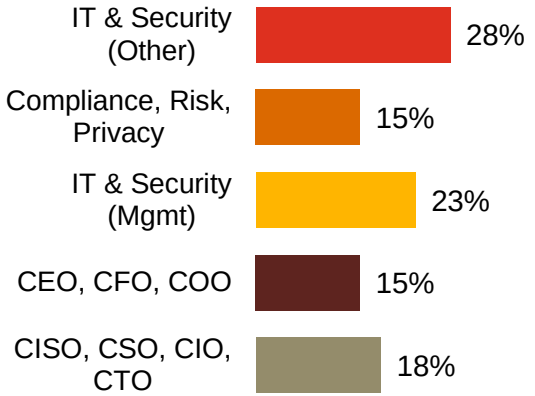
Financial services respondents by region of employment



Financial services respondents by company revenue size



Financial services respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

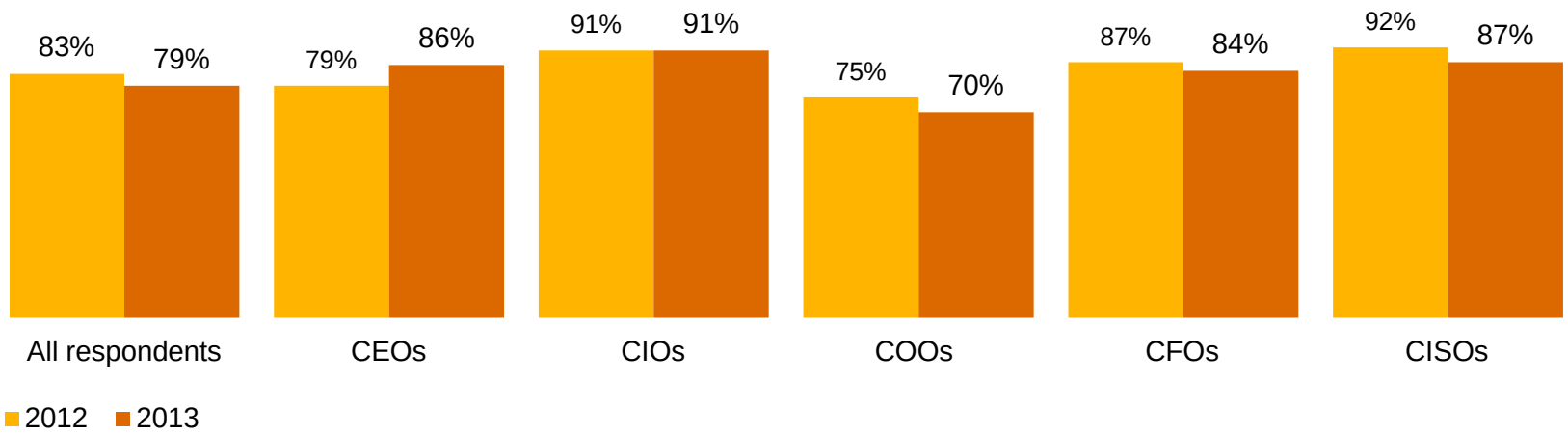
Section 2

Confidence in an era of advancing risks

79% of respondents say their security activities are effective, a decline of 5% over last year.

Confidence is still high in the C-suite*, with 86% of CEOs saying they believe their security program is effective. Across all respondents, however, confidence dropped 5% over last year, likely a result of today's enhanced threat environment. In fact, for the first time, the OCC has ranked cyber threats as a major factor heightening banks' operational risks.[1]

Executive confidence in effectiveness of security activities (somewhat or very confident)



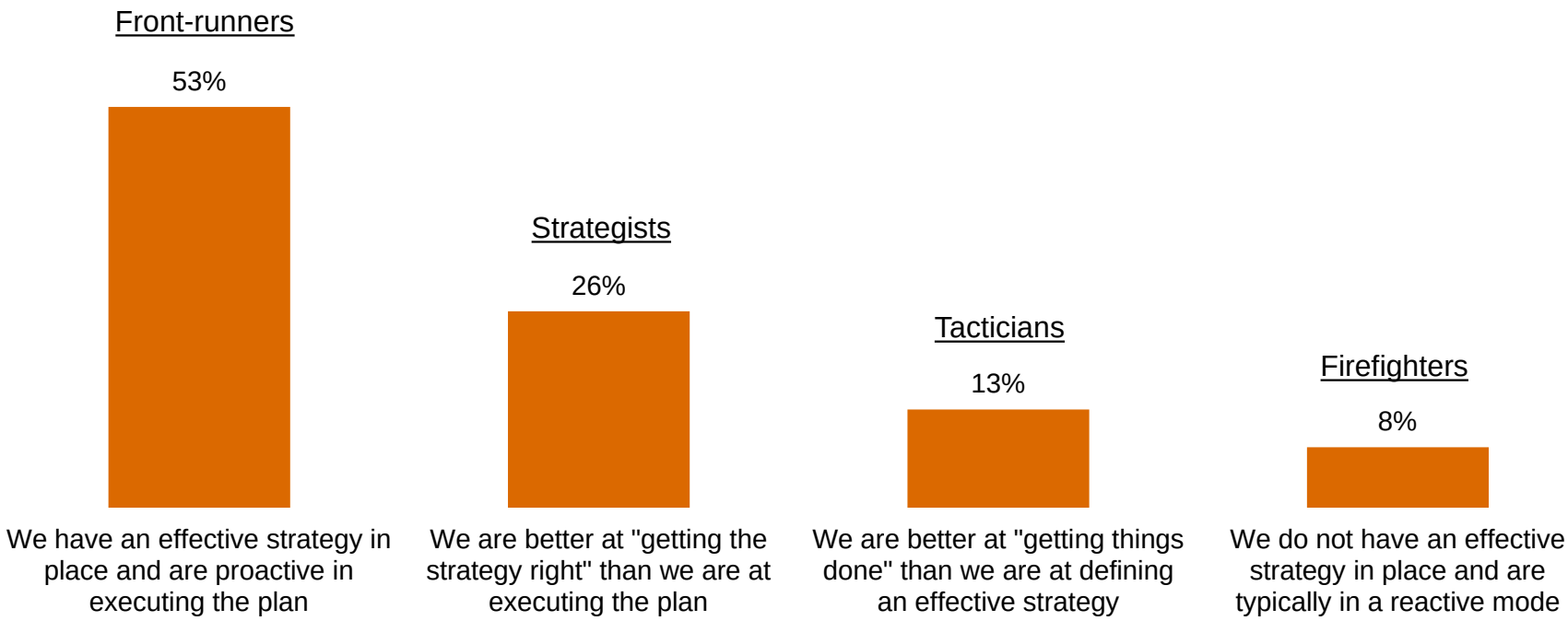
* CEOs, CFOs, and COOs

[1] Office of the Comptroller of the Currency, Semiannual Risk Perspective, Spring 2013

Question 39: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.") Question 1: "My job title most closely resembles"

53% of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

More than half of financial services respondents say they have an effective strategy in place and are proactive in executing the plan. About one in four (26%) say they are better at getting the strategy right than executing the plan.

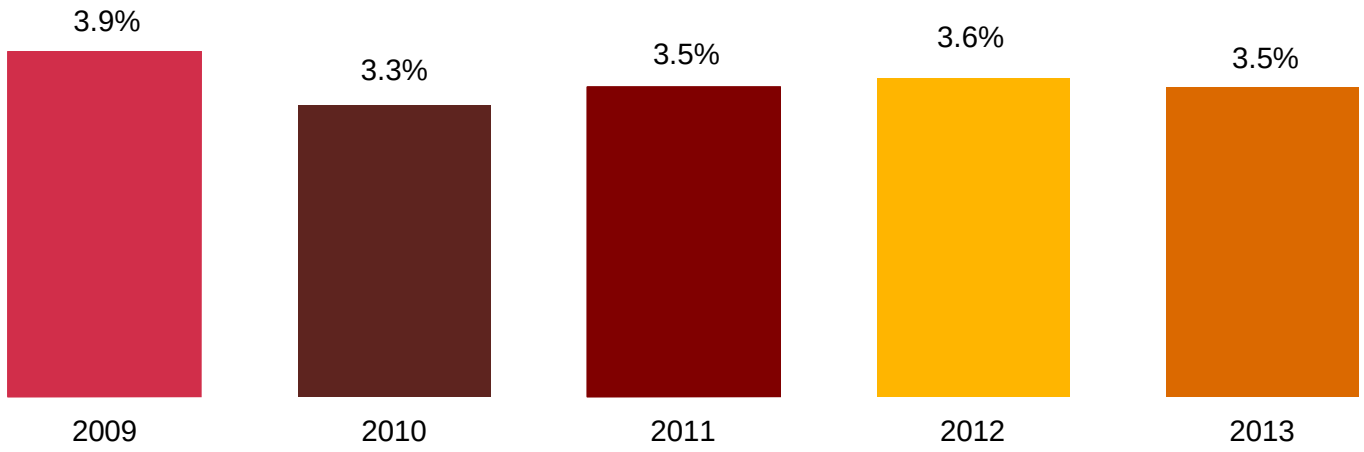


Question 27: "Which statement best characterizes your organization's approach to protecting information security?"

The share of IT budget has held steady, but as overall IT spending has increased, security budgets have also expanded.

As illustrated below, security's share of IT spend has held constant at approximately 3.5% in recent years. As overall IT budgets have recovered from post-financial crisis lows, however, spending on information security has increased in tandem.

Percent of IT budget spent on security



Question 7: "What is your organization's total information technology budget for 2013?" Question 8: "What is your organization's total information security budget for 2013?"

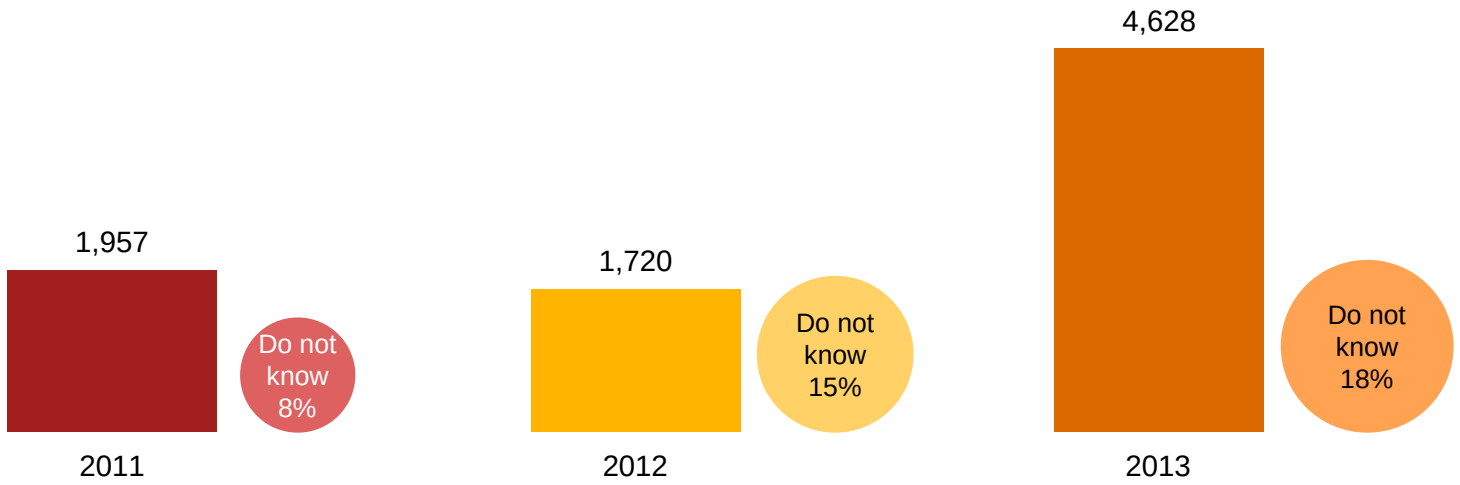
Section 3

Today's incidents, yesterday's strategies

*Financial services respondents are detecting significantly more security incidents.**

The average number of detected incidents increased by 169% over last year, evidence of today's elevated threat environment and perhaps respondents' improved ability to identify incidents. Average total financial losses have increased significantly over 2012, which is not surprising given the cost and complexity of responding to threats.

Average number of security incidents in past 12 months



* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

The constantly evolving cyber-threat landscape is driving the increase in security incidents.

The marked increase in the number of detected incidents, in our view, is likely driven by the changing cyber-threat landscape. As the digital channel in financial services continues to evolve, cybersecurity has become a business risk, rather than simply a technical risk.

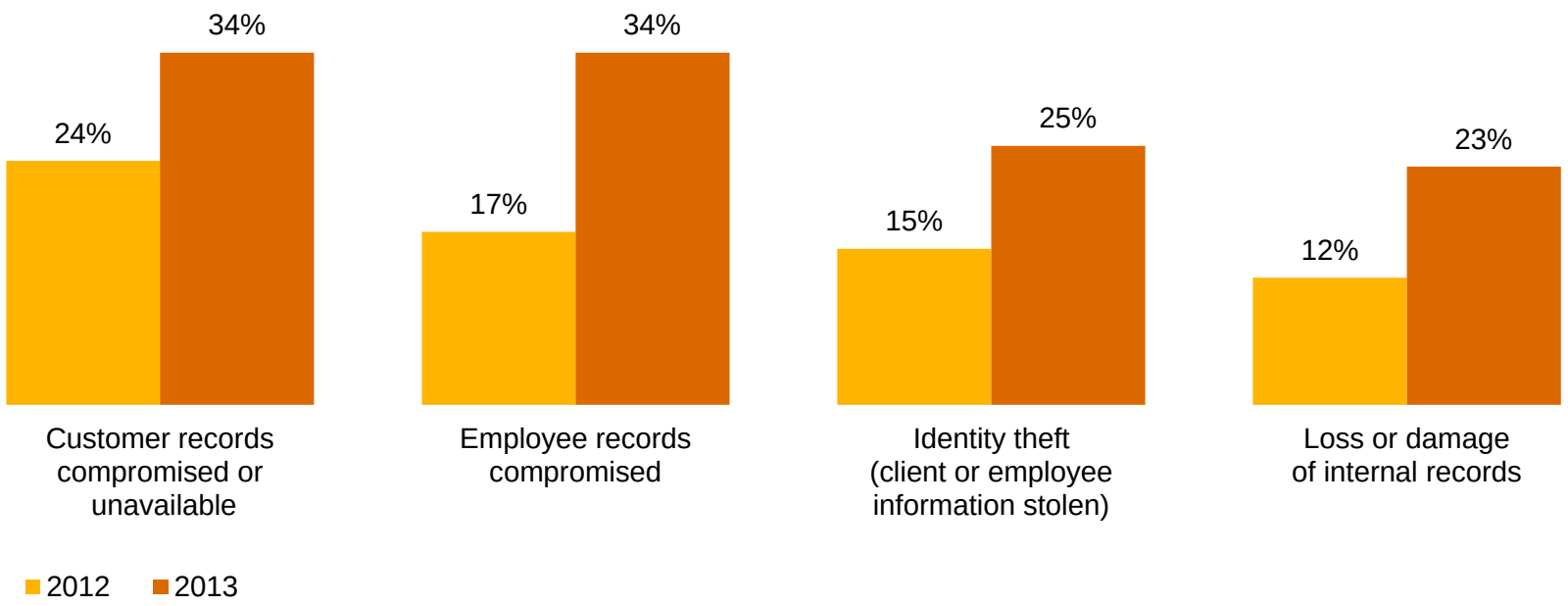
Lines between the threats are blurring

	Motivators	Threat vectors	Impact
Nation-states	• Global competition • National security • Fraud	• Targeted, long-term cyber campaigns with strategic focus • Insider • Third-party service providers	• Loss of intellectual property • Disruption to critical infrastructure • Monetary loss • Regulatory
Cyber criminals	• Illicit profit • Fraud • Identify theft	• Individual identity theft • Data breaches and intellectual property theft • Insider • Third-party service providers	• Loss of identity • Monetary loss • Intellectual property loss • Privacy • Regulatory
Cyber terrorists/ individual hackers	• Ideological • Political • Disenfranchised • Malicious havoc	• Opportunistic vulnerabilities • Insider • Third-party service providers	• Destabilize, disrupt and destroy cyber assets of financial institutions • Regulatory
Hacktivists	• Political cause rather than personal gain • Ideological	• Targeted organizations that stand in the way of their cause • Insider • Third-party service providers	• Disruption of operations • Destabilization • Embarrassment • Public relations • Regulatory

Financial services respondents report a significant increase in data loss as a result of security incidents.

Compromise of employee and customer records remain the most cited impacts, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records almost doubled over 2012.

Impact of security incidents

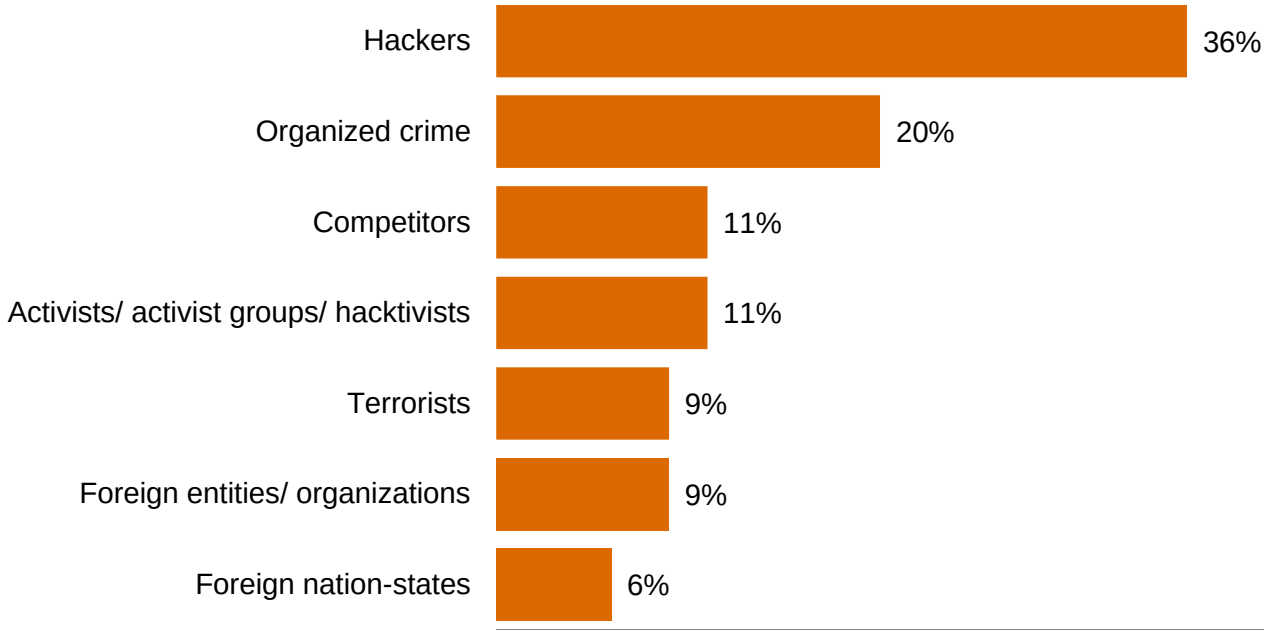


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

While attacks backed by nation-states make headlines, financial services firms are more often hit by other outsiders.

Only 6% of financial services respondents report security incidents perpetrated by foreign nation-states. Hackers and organized crime pose a much more likely danger.

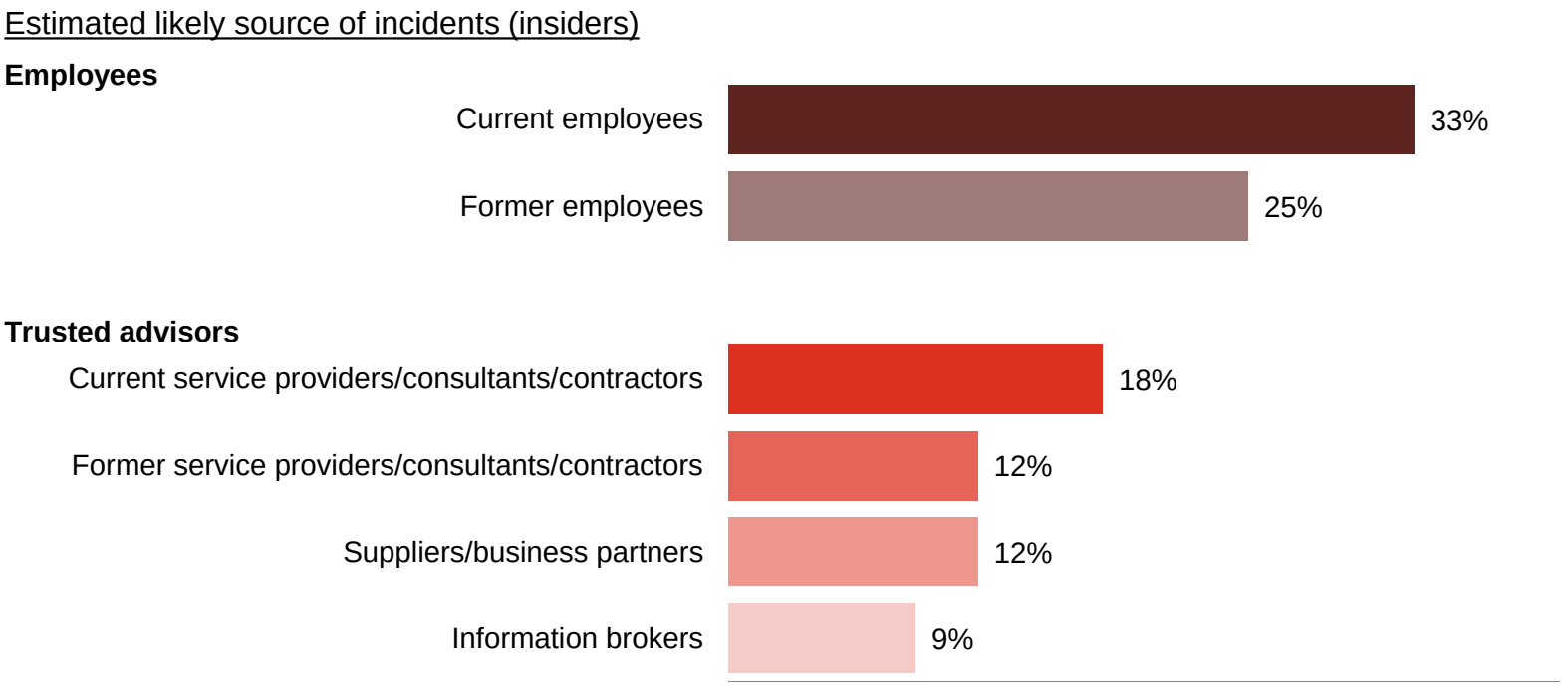
Estimated likely source of incidents (outsiders)



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most financial services respondents.

It's the people you know—current and former employees, as well as other insiders—who are most likely to perpetrate security incidents.



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

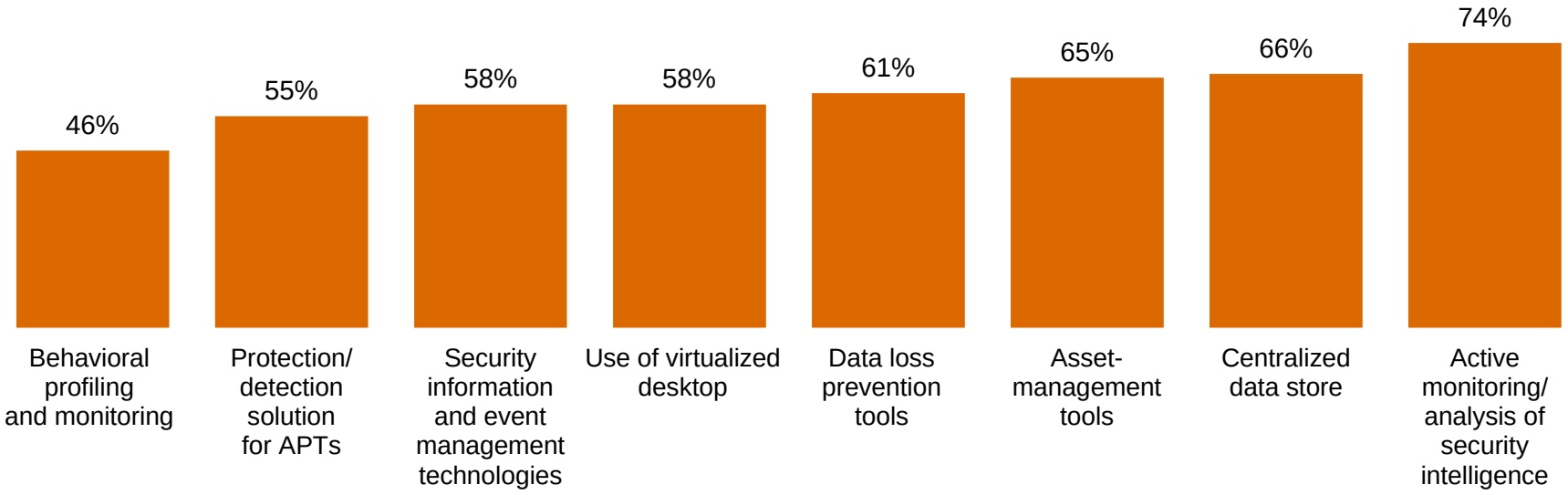
Section 4

A weak defense against adversaries

Respondents have not fully implemented technologies and processes that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place than traditional "block and tackle" security. The types of tools below—behavioral profiling and safeguards against APTs, in particular—can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Security safeguards currently in place

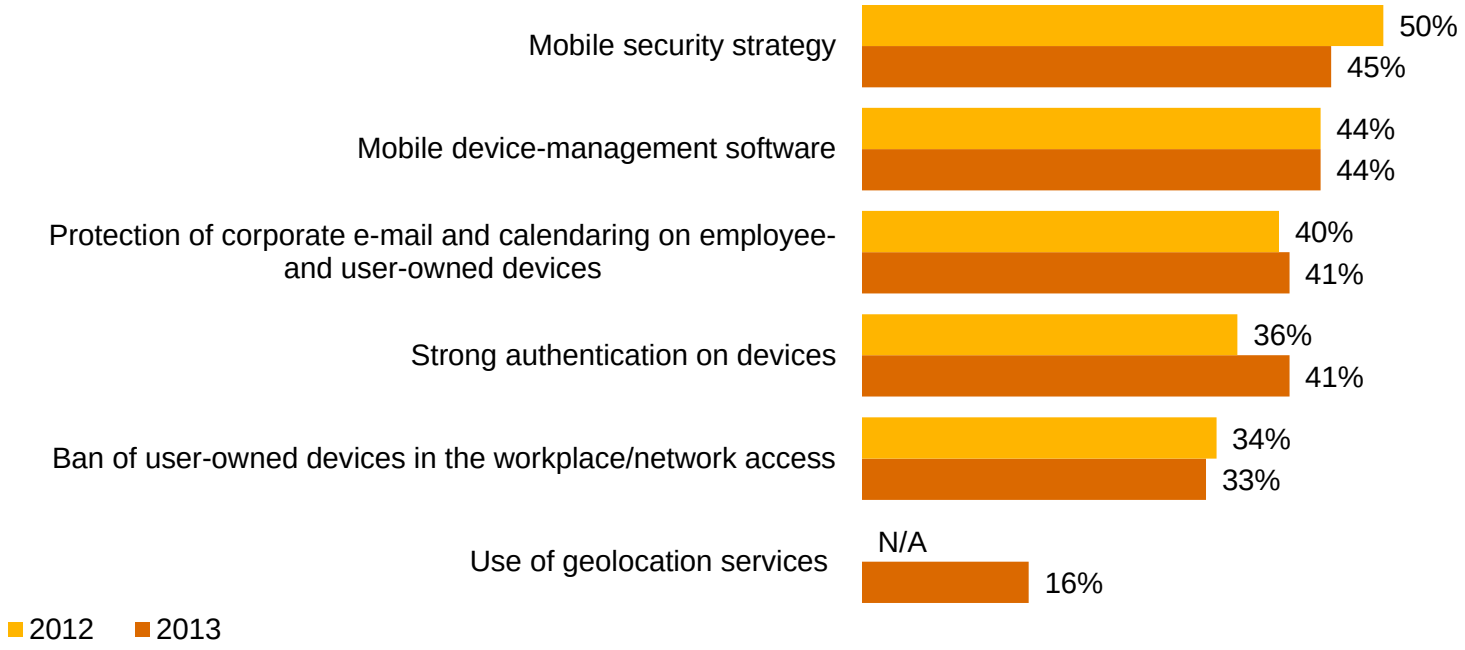


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet financial services companies' efforts to implement mobile security do not show significant gains over last year, and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

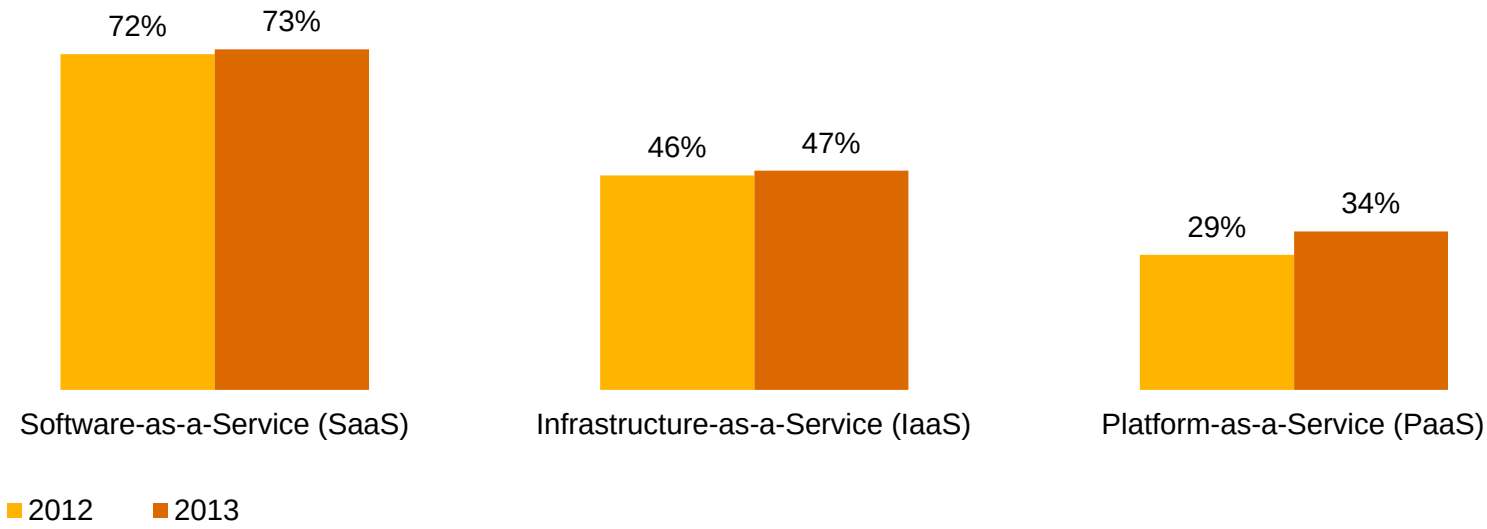


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Almost half of respondents use cloud computing, but they often do not include cloud in their security policies.

While 46% of financial services respondents use cloud computing—and among those who do, 53% report better security—only 18% include provisions for cloud in their security policy. SaaS is the most widely adopted cloud service, but PaaS shows growth.

Type of cloud service used

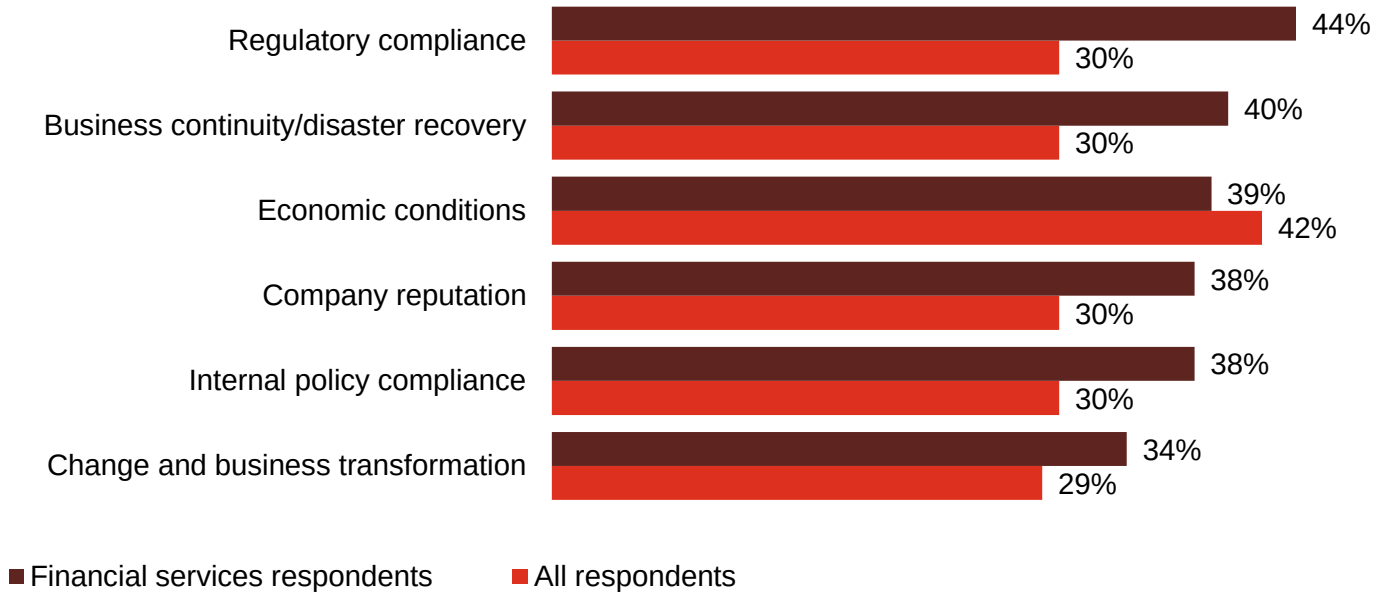


Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

Regulatory compliance remains the top driver of security spending for financial services respondents.

Compared with other industries, financial services respondents prioritize regulatory compliance as a driver for security spending. That's not surprising in a highly regulated industry, but a security model centered on existing compliance standards may not adequately address today's evolving security threats.

Drivers of information security spending



Question 35: "What business issues or factors drive your company's information security spending?" (Not all factors shown.)

Section 5

Preparing for the threats of tomorrow

Respondents rank evolving technologies and third-party standards as significant challenges to security.

Complex technologies such as high-frequency trading systems are a top concern among financial services respondents.

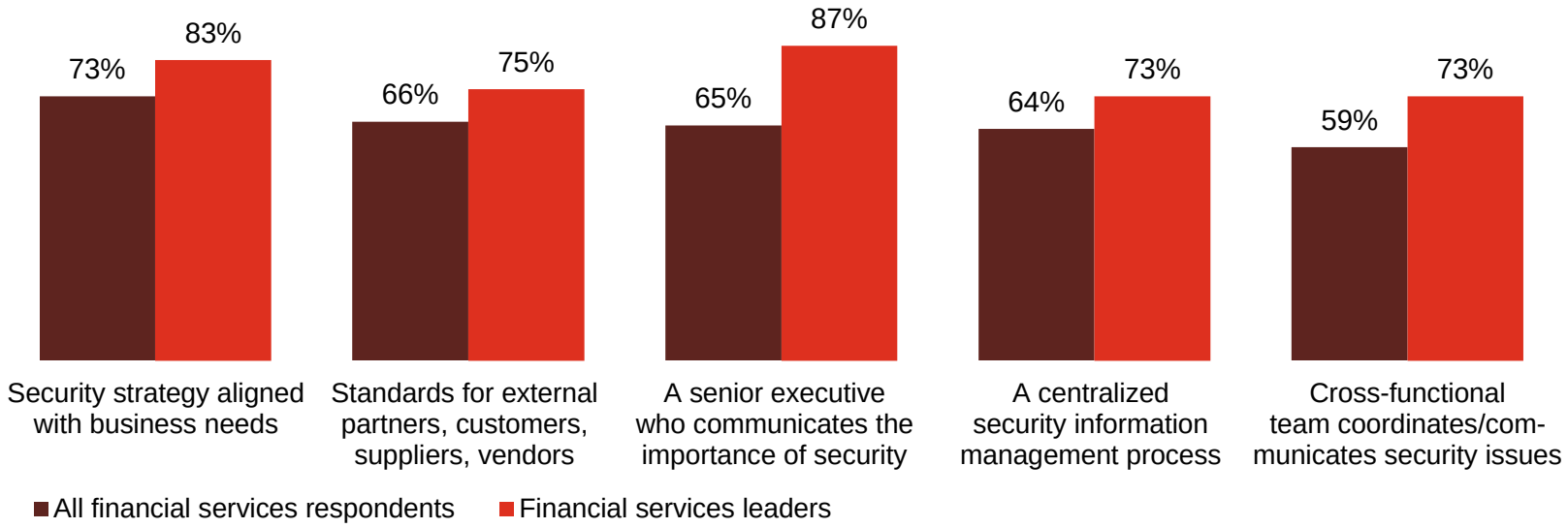
Top challenges to information security

(Asked only of financial services respondents) Question 4: “Please state the degree to which the following are challenges for the future success of your organization’s information security efforts?” (Respondents who answered “Significant challenge”) (Not all factors shown.)

Leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT challenge.*

Aligning security with business needs, setting standards for external partners, and improving communications show leaders, in particular, are rethinking the basics of security.

Security policies and safeguards currently in place: All respondents vs. leaders



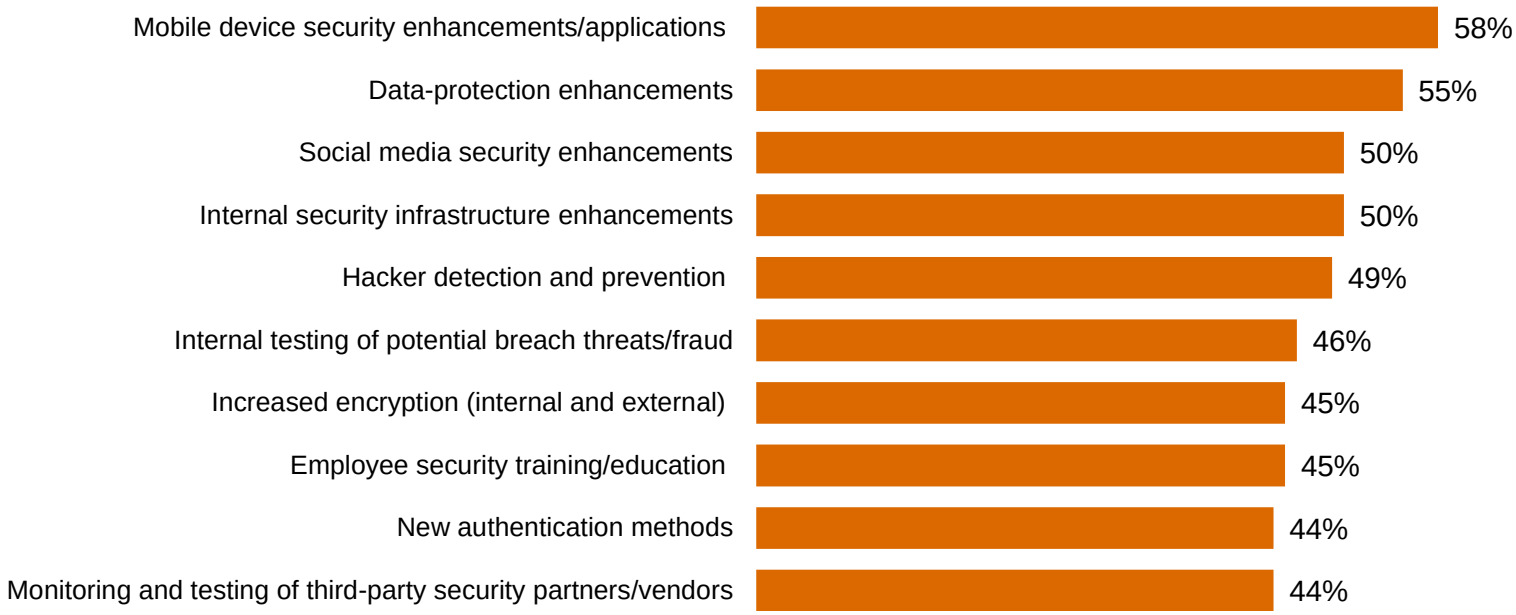
* We define leaders by the following criteria: Have an overall information security strategy; employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel; have measured and reviewed the effectiveness of security within the past year; and understand exactly what type of security events have occurred in the past year.

Question 14: "What process information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?"

What business imperatives and processes will financial services respondents prioritize over the next 12 months?

Some of the highest priorities include enhanced security for mobile devices and social media.

Over the next 12 months, organization will increase spending for:

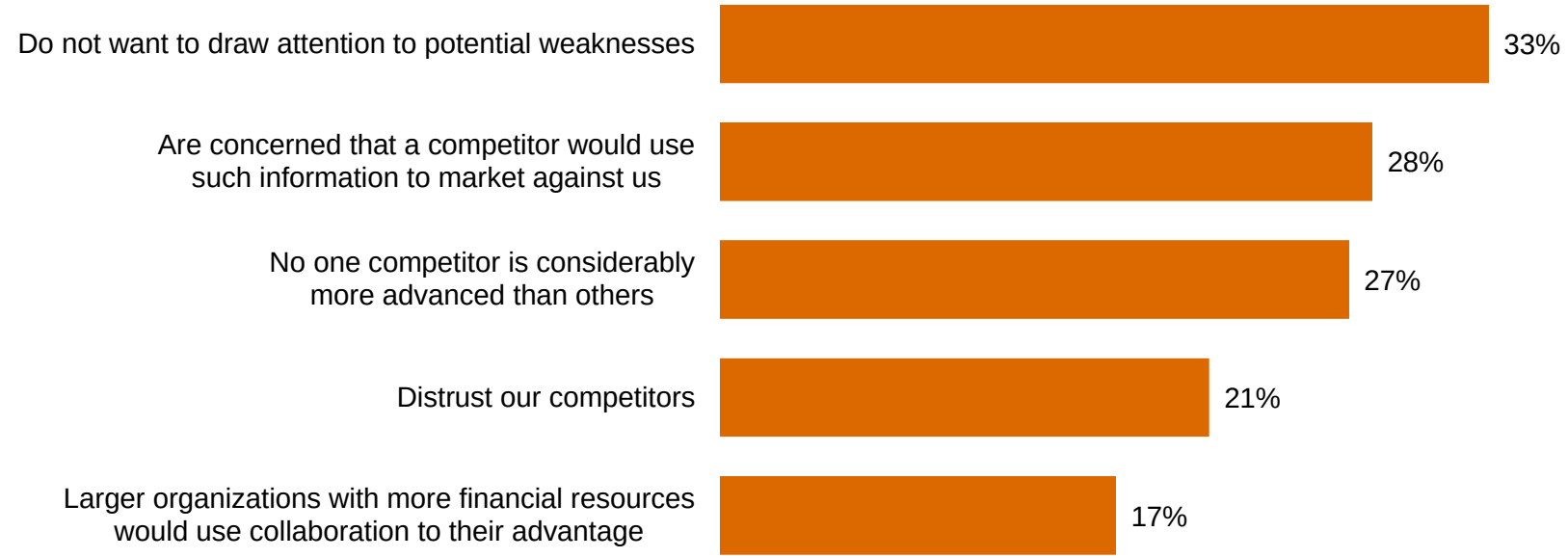


(Asked only of financial services respondents.) Question 3: “Please indicate whether your organization will increase or decrease spending on information security over the next 12 months for?” (Not all factors shown.)

55% of respondents collaborate with others to improve security, leveraging a powerful tool.

Compared with other industries, a higher percentage of financial services firms report they collaborate with others to advance security and better understand the threat landscape. Some, however, remain hesitant to share information, and that can impede security.

Reasons for not collaborating on information security

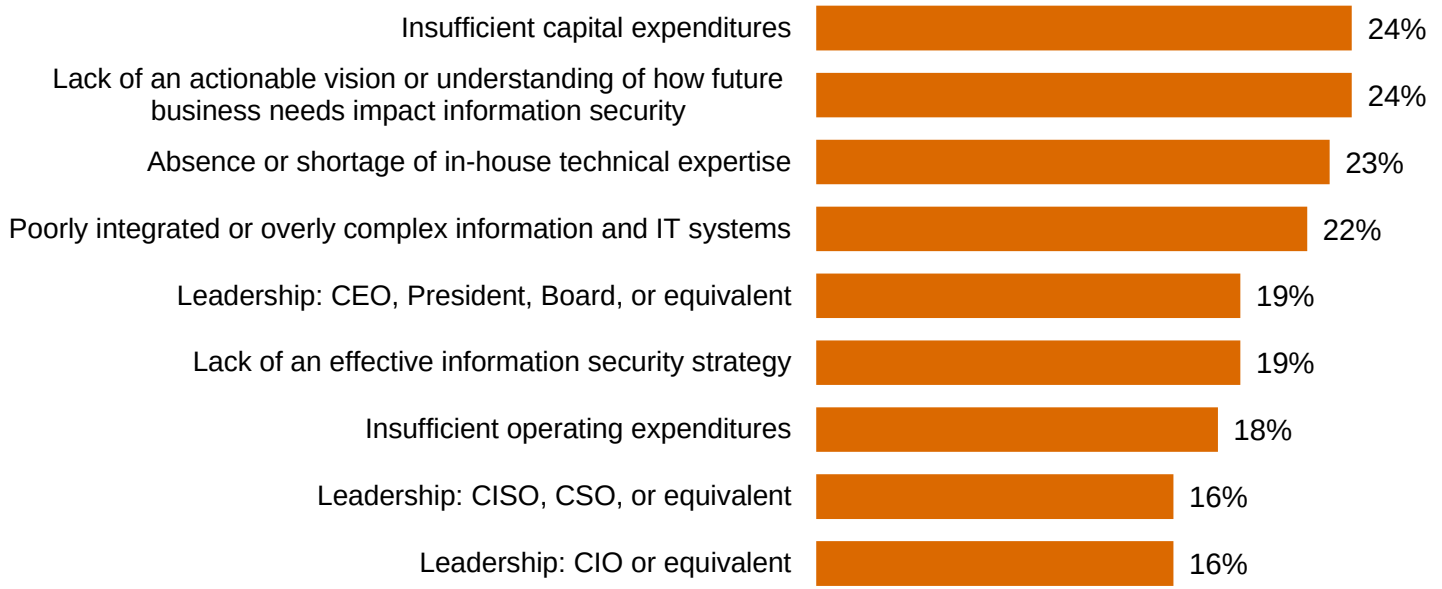


Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

More money and an actionable vision are needed to overcome obstacles to advancing security.

This is critical because effective security requires an adequate budget that is aligned with future business needs, as well as the support of top executives.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Effective security also demands that organizations align policies and spending with business objectives.

This year, more financial services respondents say security policies and spending are aligned with business goals. This suggests they are starting to understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are 10 key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Leading security practices for financial services companies.

Security is a board-level business imperative	
Advance your security strategy and capabilities.	• An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge. • You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
Board and CEO drive security governance.	• Security risks are operational risks and should be reviewed regularly by the board. • Strong support and communication from the board and CEO can break down traditional silos, leading to more collaboration and partnerships.
Strong multi-party governance group should manage security risk.	• An executive with direct interaction with the CEO, General Counsel and Chief Risk Officer should lead security governance. • Security governance group should include representatives from legal, HR, risk, technology, security, communications, and the lines of business. • The cybersecurity governance group should meet regularly (monthly or quarterly) to discuss the current threat landscape, changes within the organization that impact risk levels, and updates to remediation programs and initiatives.
Security threats are business risks	
Security program is threat-driven and assumes a continuous state of compromise.	• Security risks are among the top 10 operational risks. • Adopt the philosophy of an assumed state of compromise, focusing on continuous detection and crisis response in addition to traditional IT security focus of protection and mitigation. • Security risks include theft of intellectual property, attacks on brand, and social media. • You should anticipate threats, know your vulnerabilities, and be able to identify and manage the associated risks. • Focus on your adversaries: who might attack the business and their motivations.
Ensure cooperation among third parties.	• Proactively make certain that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Leading security practices for financial services companies (cont'd).

Protect the information that really matters	
Identify your most valuable information.	• Know where these "crown jewels" are located and who has access to them. • Allocate and prioritize resources to protect your valuable information.
Establish and test incident-response plans	
Incident response should be aligned at all levels within the organization.	• Incident response should integrate technical and business responses. • Response is aligned at all levels by integrating the technical response (led by IT) and business response (led by business with input from legal, communications, the senior leadership team, and HR).
Security incident response should be tested using real-world scenarios.	• Improve planning and preparedness through table-top simulations of recent industry events and likely attack scenarios. • Frequently conduct table-top simulations. • Response to various attack scenarios and crisis should be pre-scripted in a "play book" format.
Gain advantage through Awareness to Action	
Security is driven by knowledge, an approach we call Awareness to Action.	• All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring. • Organizations should create a culture of security that starts with commitment of top executives and cascades to all employees. • Organizations should engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

US Financial Services Contacts

Joe Nocera
Principal
312.298.2745
joseph.nocera@us.pwc.com

Shawn Connors
Principal
646.471.7278
shawn.joseph.connors@us.pwc.com

Andrew Toner
Principal
646.471.8327
andrew.toner@us.pwc.com

Christopher Morris
Principal
617.530.7938
christopher.morris@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

PwC

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

Healthcare Providers

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global healthcare provider industry are heeding the need to fund enhanced security activities and have improved technology safeguards, processes, and strategies. Budgets are rising and confidence is high.

But while many healthcare provider organizations have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased, as has the cost of breaches. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many healthcare provider executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few healthcare provider organizations have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that healthcare providers identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the organizational strategy, one that is championed by the CEO and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

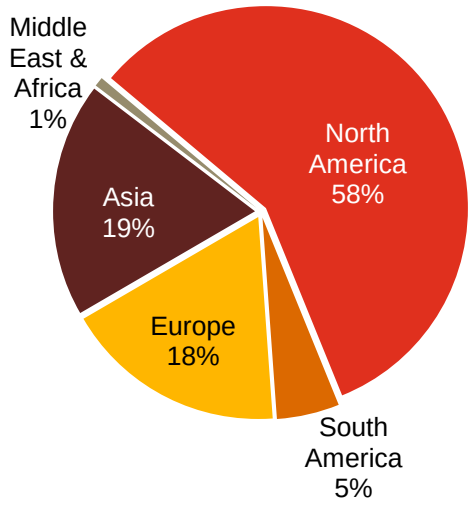
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

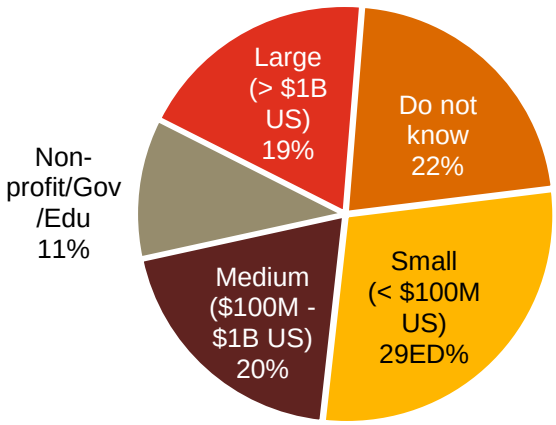
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from organizations with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 398 respondents from the healthcare provider industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

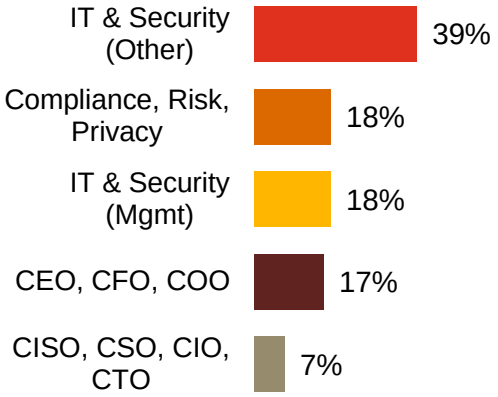
Healthcare respondents by region of employment



Healthcare respondents by company revenue size



Healthcare respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

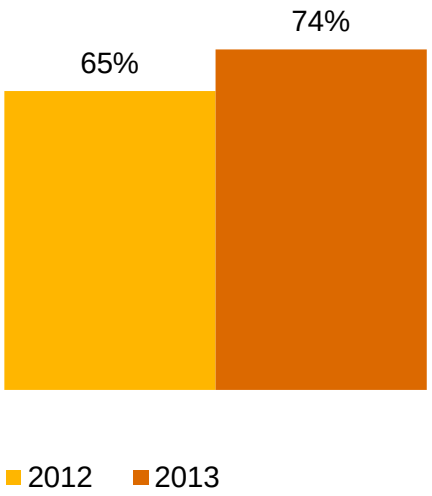
Section 2

Confidence in an era of advancing risks

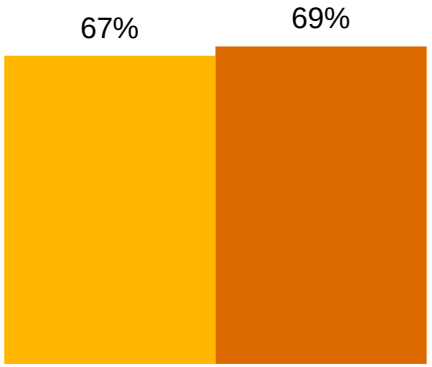
Confidence is rising: 74% of healthcare provider respondents believe their security activities are effective.

Confidence in security programs increased 14% over last year. The number of respondents who report confidence in their partners' and suppliers' security programs is slightly higher.

Confidence in effectiveness of security activities



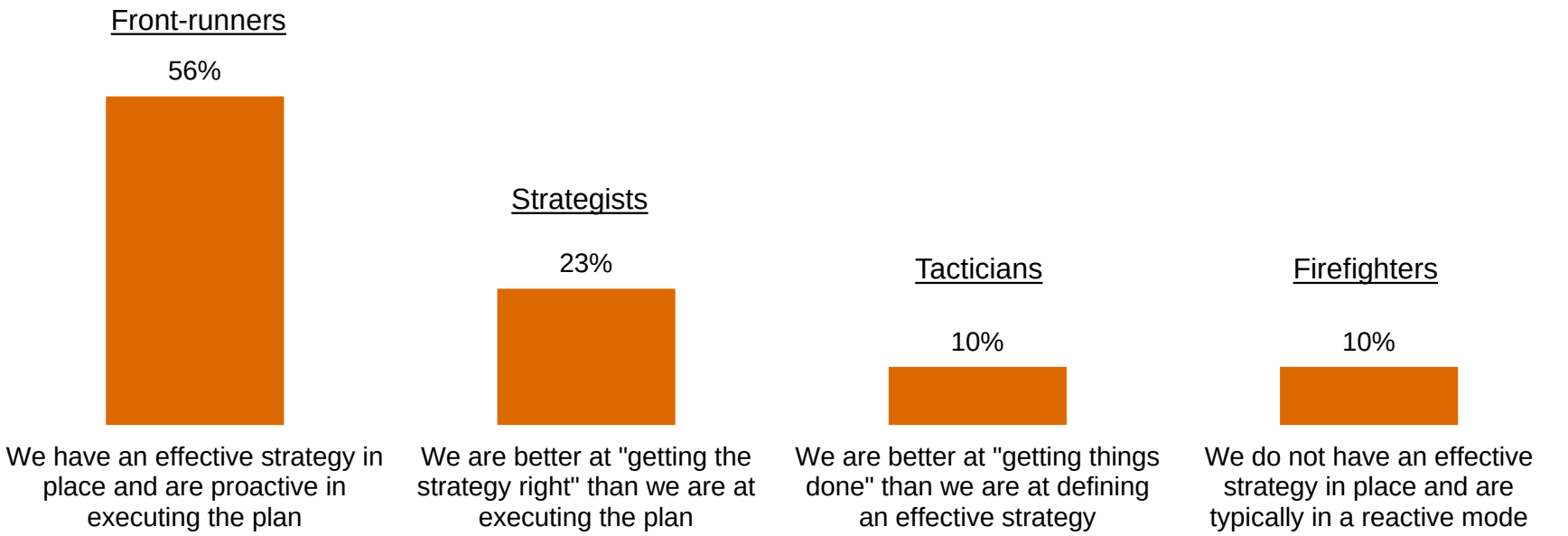
Confidence in effectiveness of partners'/suppliers' security activities



Question 39: "How confident are you that your organization's information security activities are effective?" Question 40: "How confident are you that your partners'/suppliers' information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.")

56% of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

More than half of healthcare provider respondents say they have an effective strategy and are proactive in executing the plan, a 33% increase over last year. Almost one in four (23%) report they are better at getting the strategy right than executing the plan.



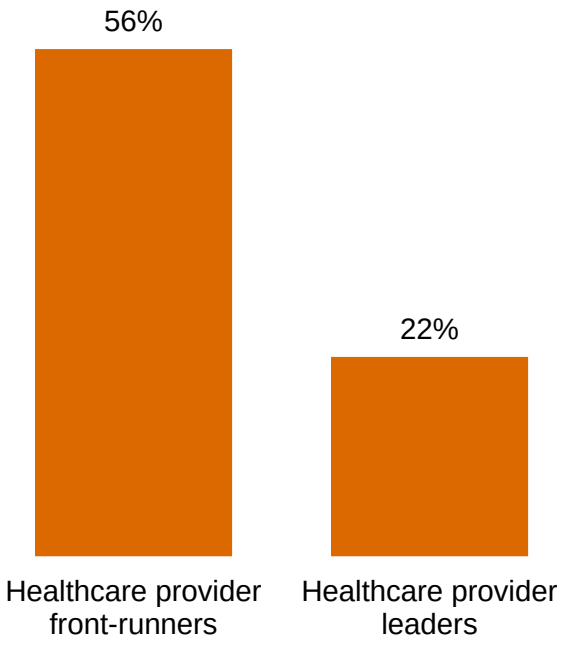
Question 27: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding.)

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured healthcare provider respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

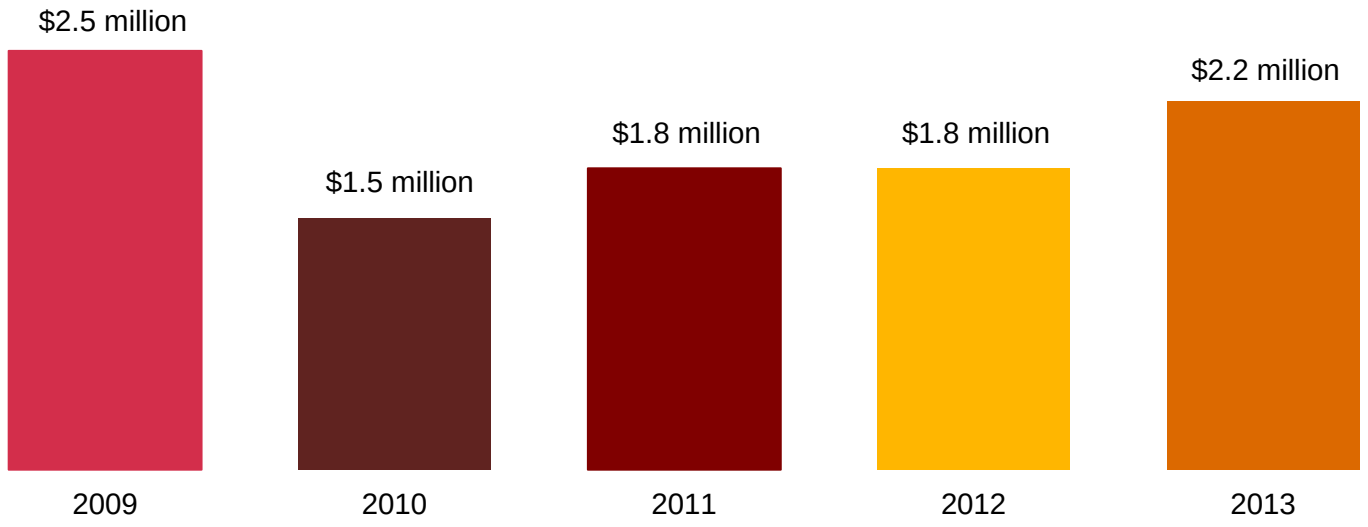


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Healthcare provider security budgets have increased.

Information security budgets average $2.2 million this year, an increase of 20% over the year before. This boost suggests that healthcare providers understand that today's elevated threat landscape demands a greater investment in security.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

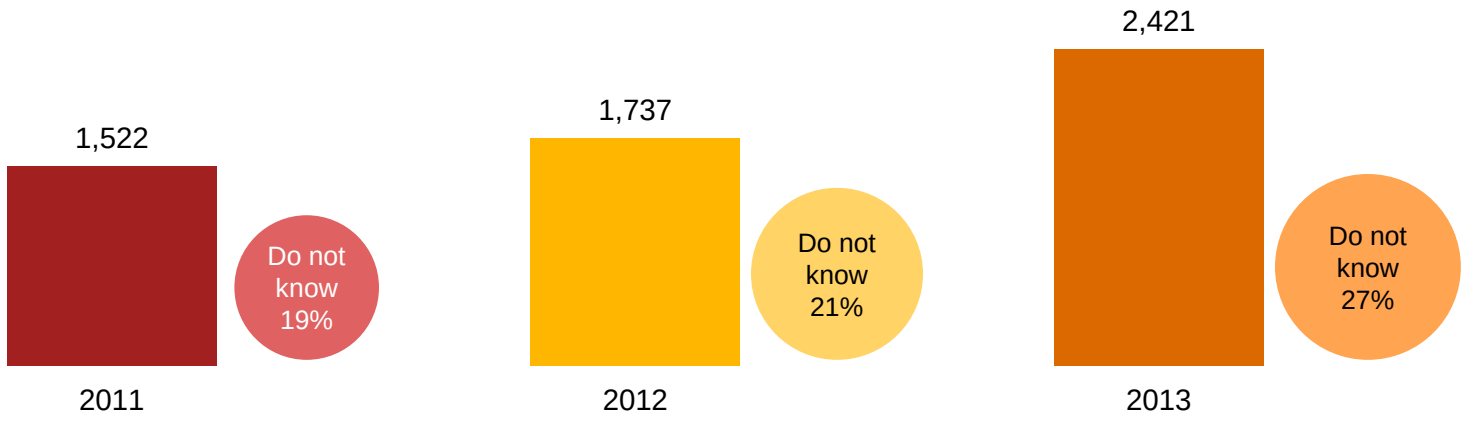
Section 3

Today's incidents, yesterday's strategies

*Healthcare provider respondents are detecting more security incidents.**

The number of incidents detected in the past 12 months increased by 39% over last year, perhaps an indication of today's elevated threat environment. Given the cost and complexity of responding to incidents, it is not surprising that financial losses as a result of incidents are up 10% over last year.

Average number of security incidents in past 12 months



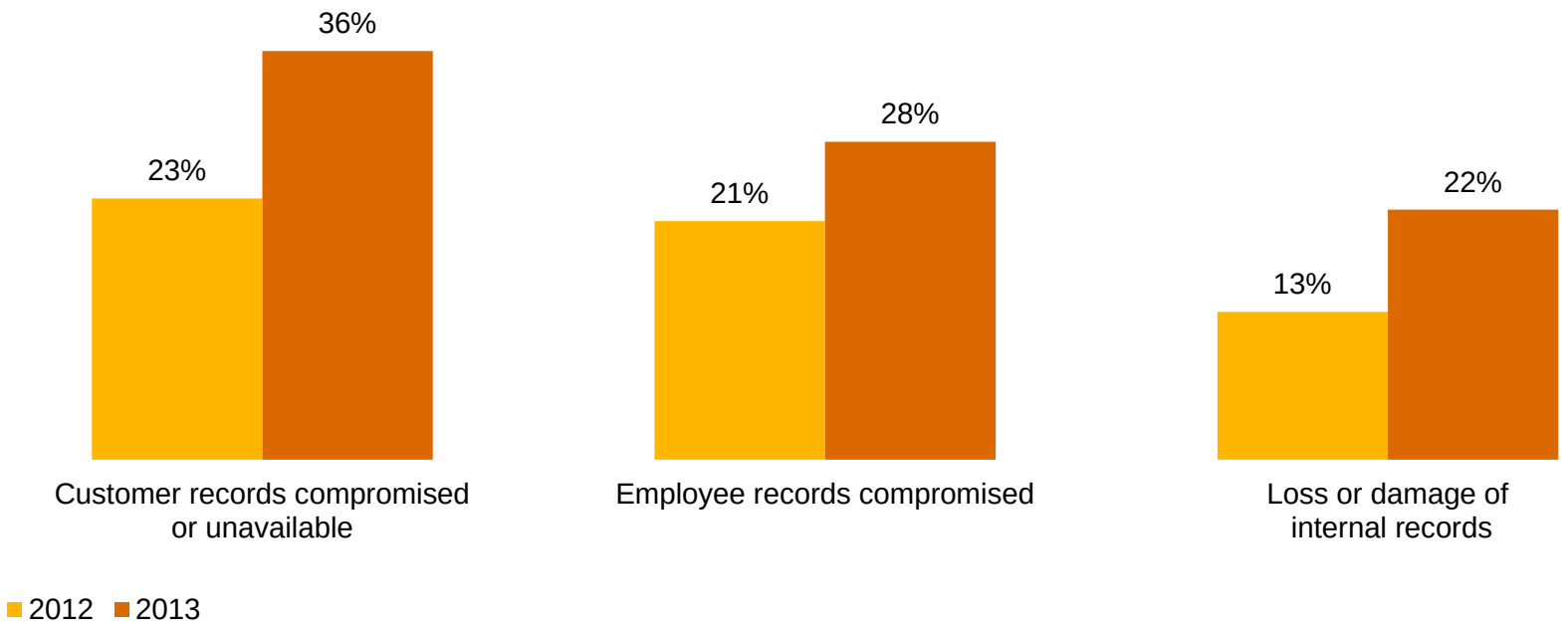
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

Healthcare provider respondents report an increase in customer data loss as a result of security incidents.

Compromise of customer records is up sharply this year, potentially jeopardizing a healthcare provider organization's most valuable relationships. Also significant: Loss or damage of internal records increased substantially over 2012.

Impact of security incidents

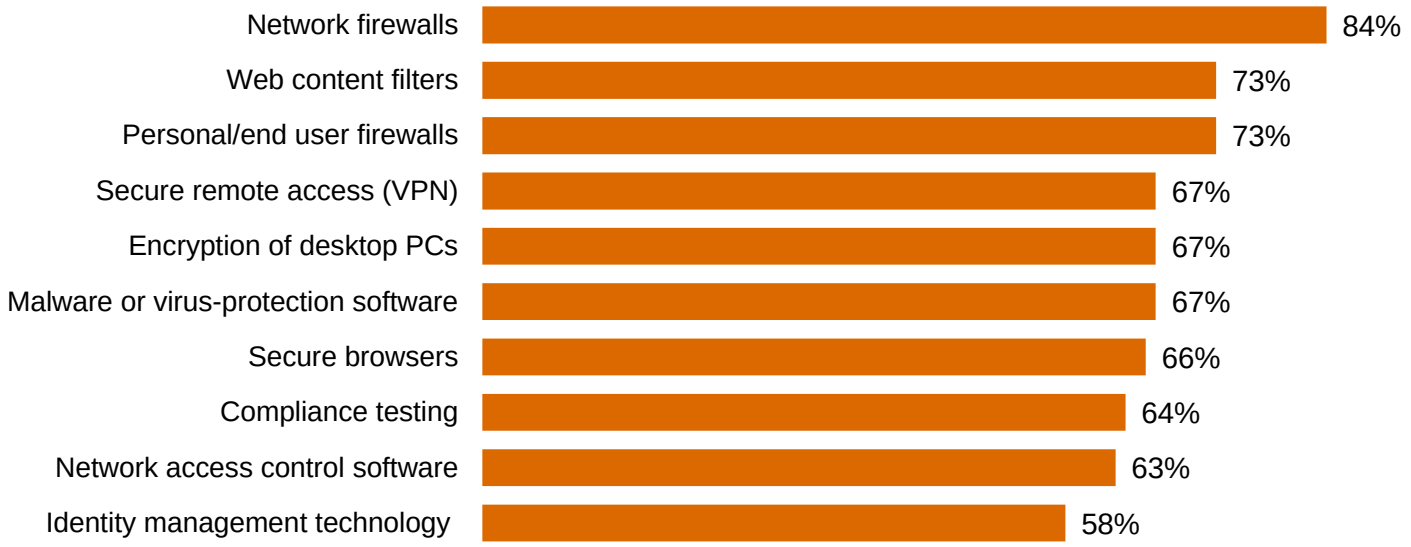


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet these technologies fail to stop today's advanced threats.

Deployment of "block and tackle" security programs is at an all-time high. But they have not effectively blocked incidents, suggesting these products and services may be ineffective because they are built on outdated security models.

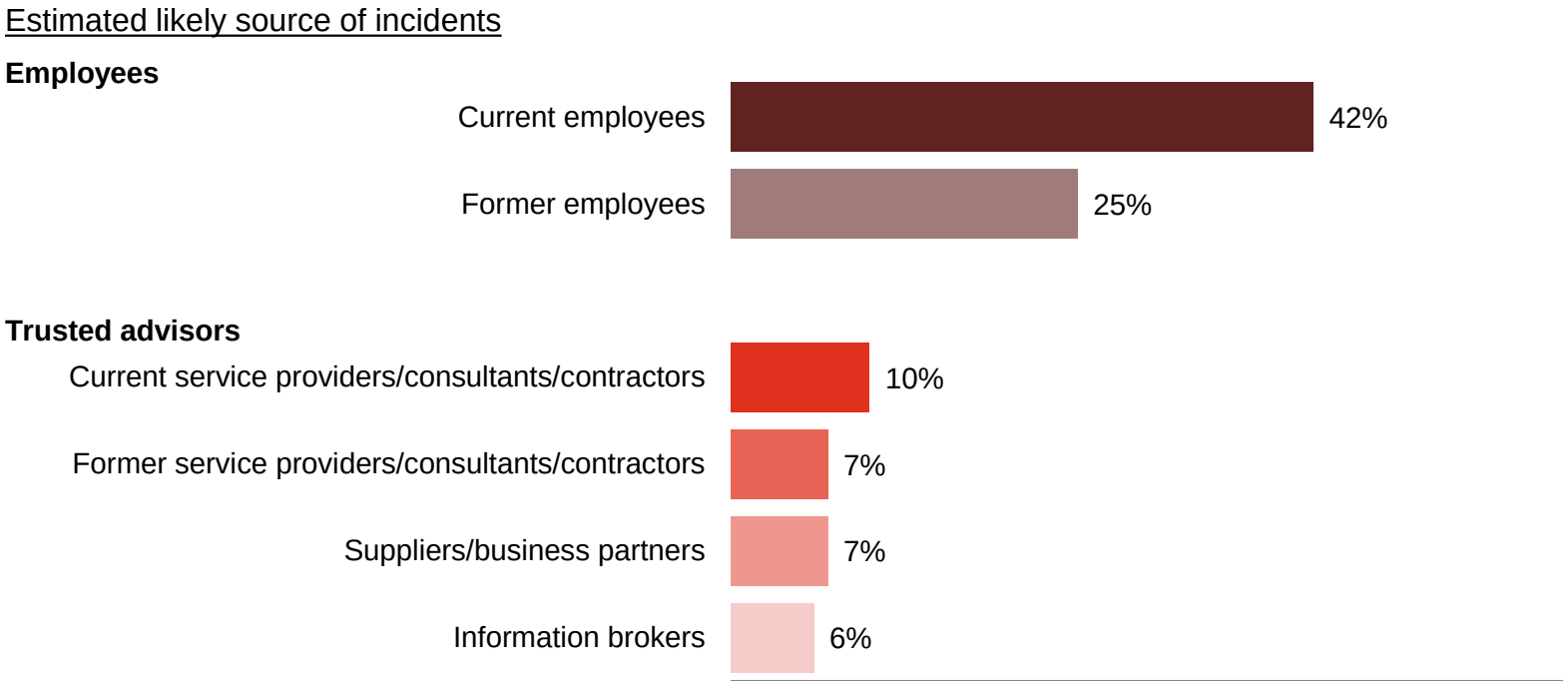
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most healthcare provider respondents.

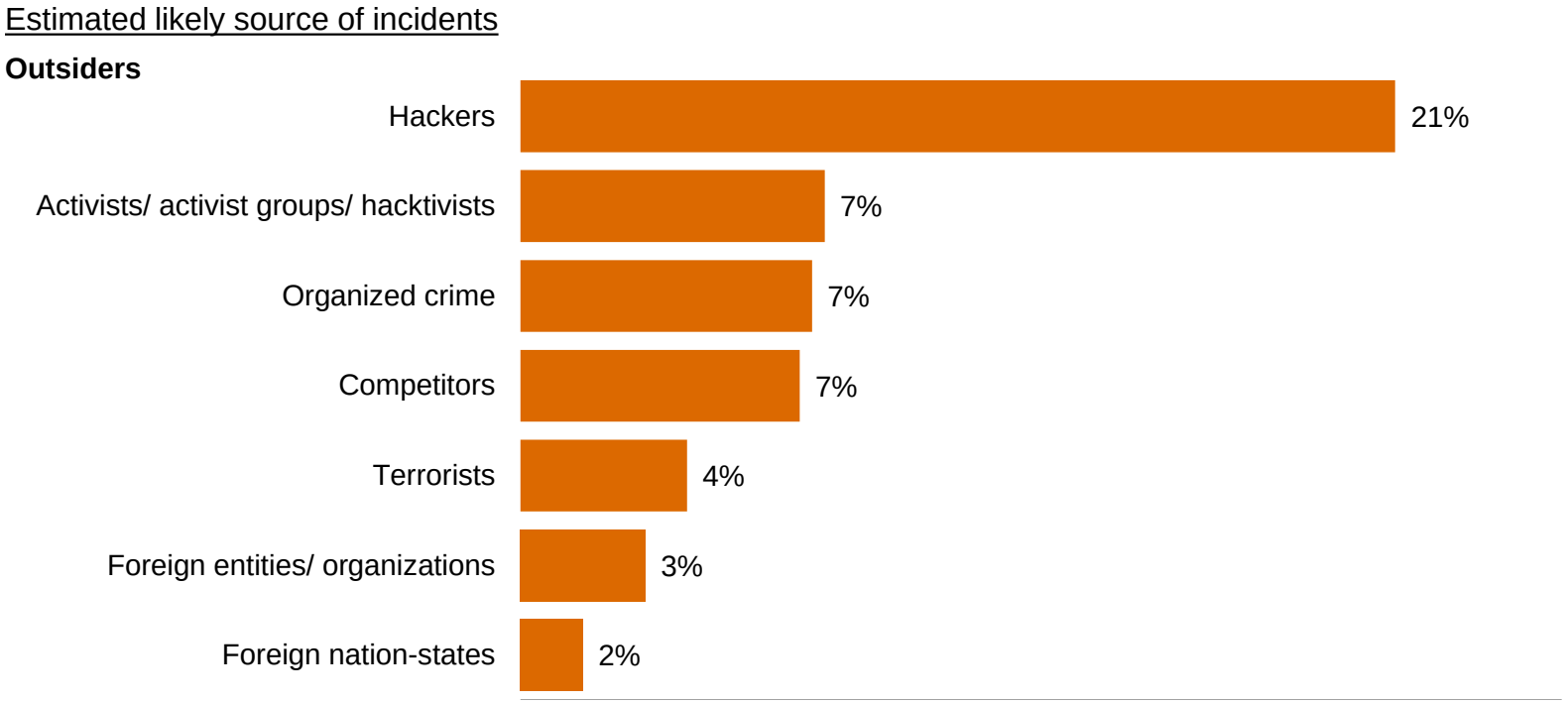
It's the people you know—primarily current and former employees—who are most likely to perpetrate security incidents.



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, organizations are more likely to be hit by other outsiders.

Only 2% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

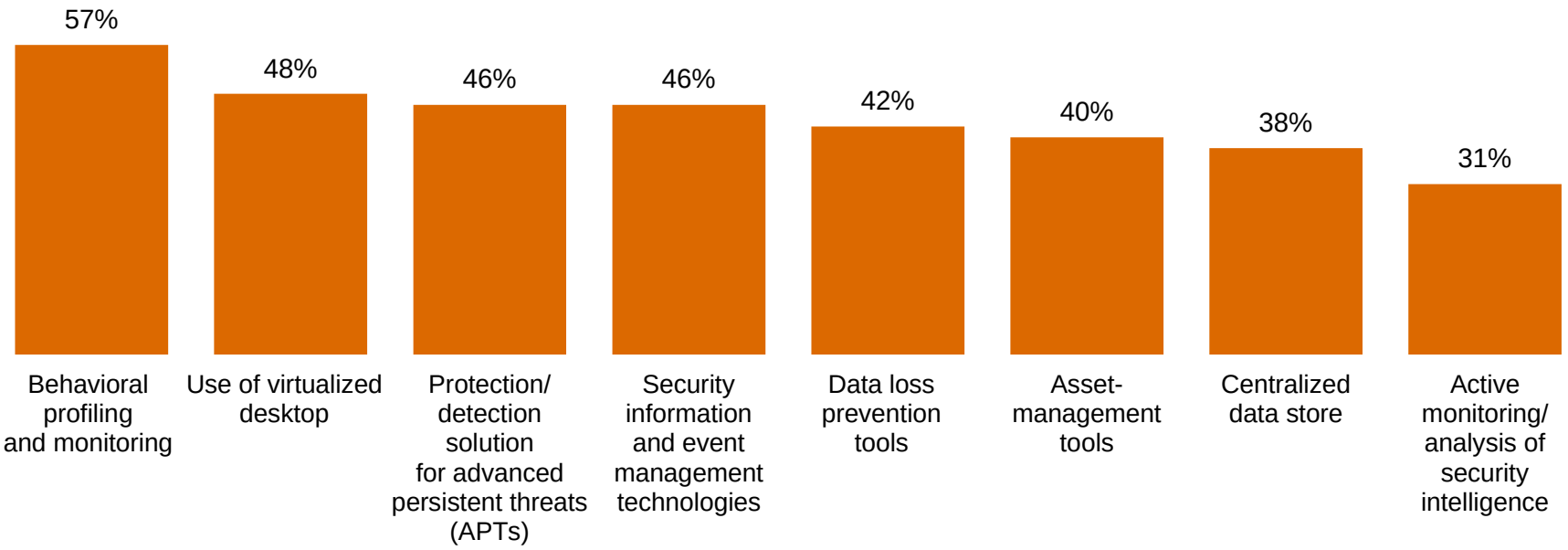
Section 4

A weak defense against adversaries

Many providers have not implemented technologies and processes that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place than traditional safeguards. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place

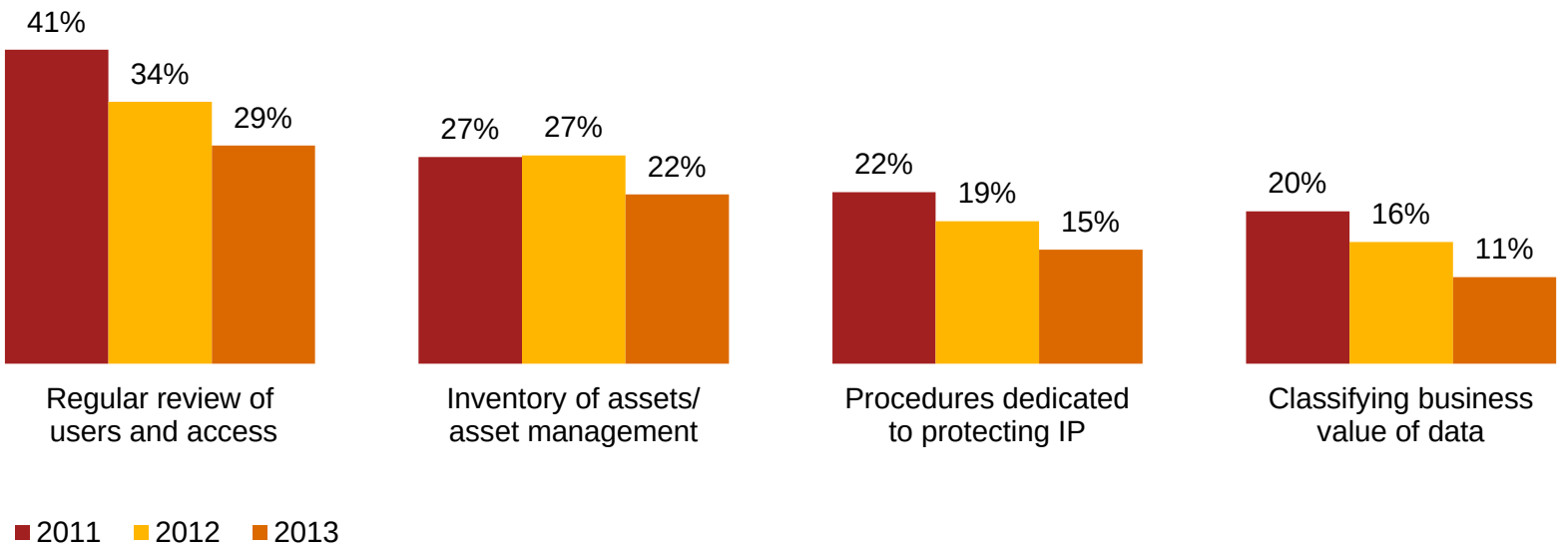


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite the potential consequences, many organizations do not adequately safeguard their high-value information.

It is imperative that organizations identify, prioritize, and protect their "crown jewels." But implementation of basic policies to safeguard intellectual property (IP) is declining among healthcare provider respondents.

Have policies to help safeguard IP and trade secrets

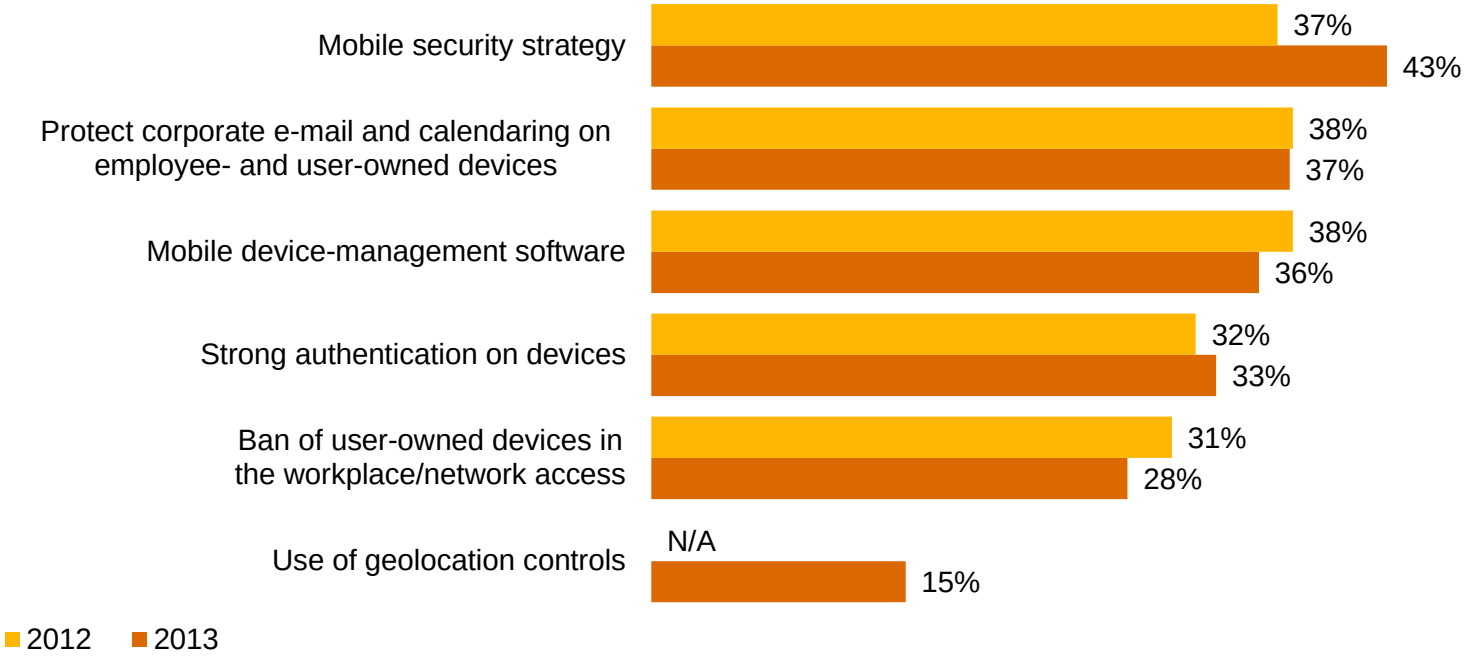


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet healthcare providers' efforts to implement mobile security programs do not show significant gains over last year, and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

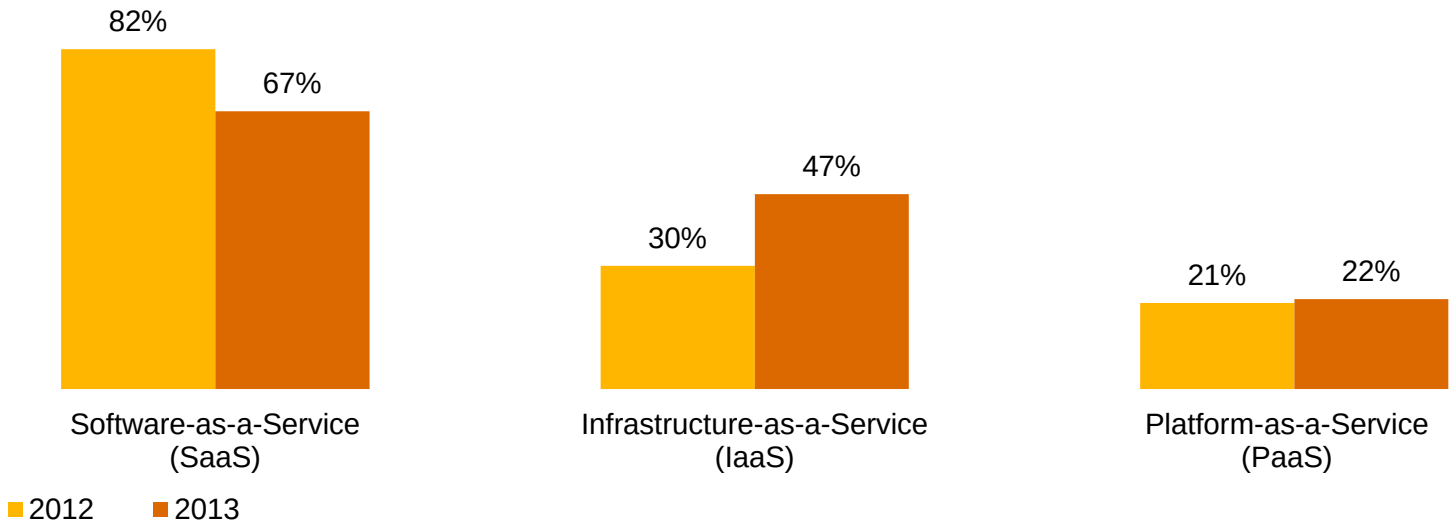


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Only 38% of respondents use cloud computing, and those that do often omit cloud from their security policy.

Adoption of cloud computing by healthcare providers lags that of other industries. While 55% of cloud users say the technology has improved information security, only 16% include cloud in their security policy. SaaS remains dominant, while IaaS shows growth.

Type of cloud service used



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

While 80% of respondents say security spending is aligned with business goals, investment in top priorities is not.

We asked healthcare provider respondents to identify their top five security challenges, then specify what percentage of their overall budgets would be applied to each challenge. The results suggest a disconnect between priorities and investments.

Top 5 security challenges	Top 5 spending priorities for challenges
1. Data leakage prevention	1. Outsourcing and vendor oversight
2. Access controls and identity management	2. Data leakage prevention
3. Monitoring of access and information use	3. Regulatory requirements
4. Identity theft and loss of patient/individual information	4. Encryption in storage and in transit
5. Regulatory requirements	5. Required software updates

Question 34: “In your opinion, how well is your company’s spending aligned with your company’s business objectives?” (Respondents who answered “Somewhat aligned” or “Completely aligned.”) (Asked only of healthcare provider respondents) Question 4: “Please identify your organization’s top five security challenges”) Question 4A: “Of your top five security challenges, what percentage of your overall budget are you spending to address each?” (Not all factors shown.)

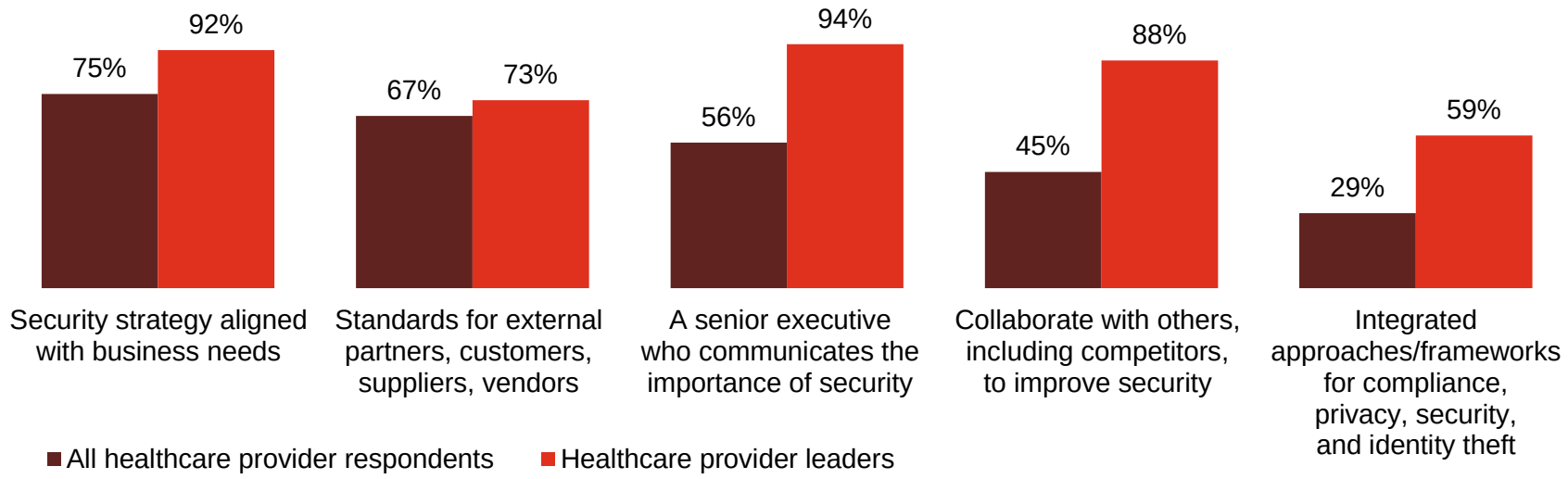
Section 5

Preparing for the threats of tomorrow

Leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT issue.

Aligning security with business needs, improving executive communications, and collaborating with others show leaders, in particular, are rethinking the basics of security.

Security policies and safeguards currently in place: All respondents vs. leaders



Question 14: “What process information security safeguards does your organization currently have in place?” (Not all factors shown.) Question 29: “Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?” Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?” (Asked only of healthcare provider respondents) Question 6: “To what extent has your organization integrated approaches/frameworks for compliance, privacy, security, and identity theft?” (Respondents who answered “To a great extent.”)

What business imperatives and processes will healthcare providers prioritize this year?

Some of the highest priorities cited by respondents include technologies that can help the organization protect its most valuable assets and safeguard the infrastructure.

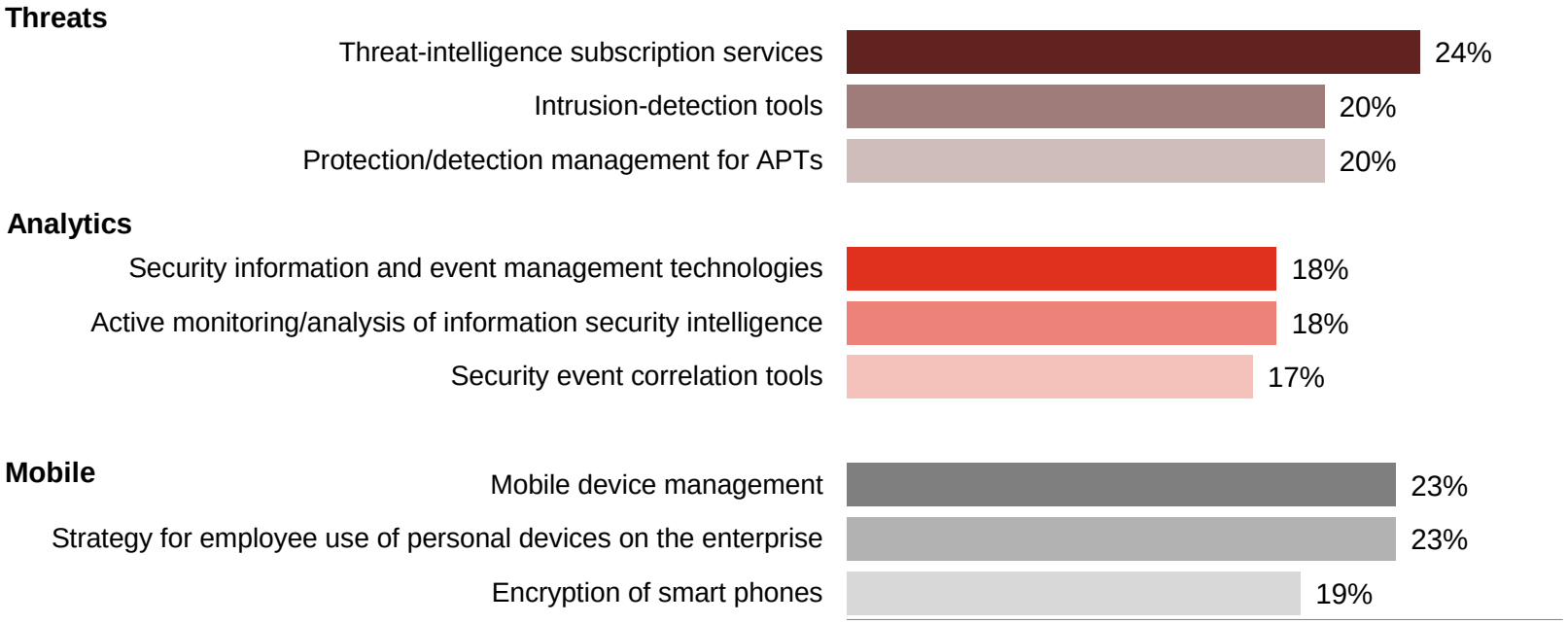
Safeguards not in place but a top priority over the next 12 months

Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and organizations are prioritizing technologies that can help them better understand threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months

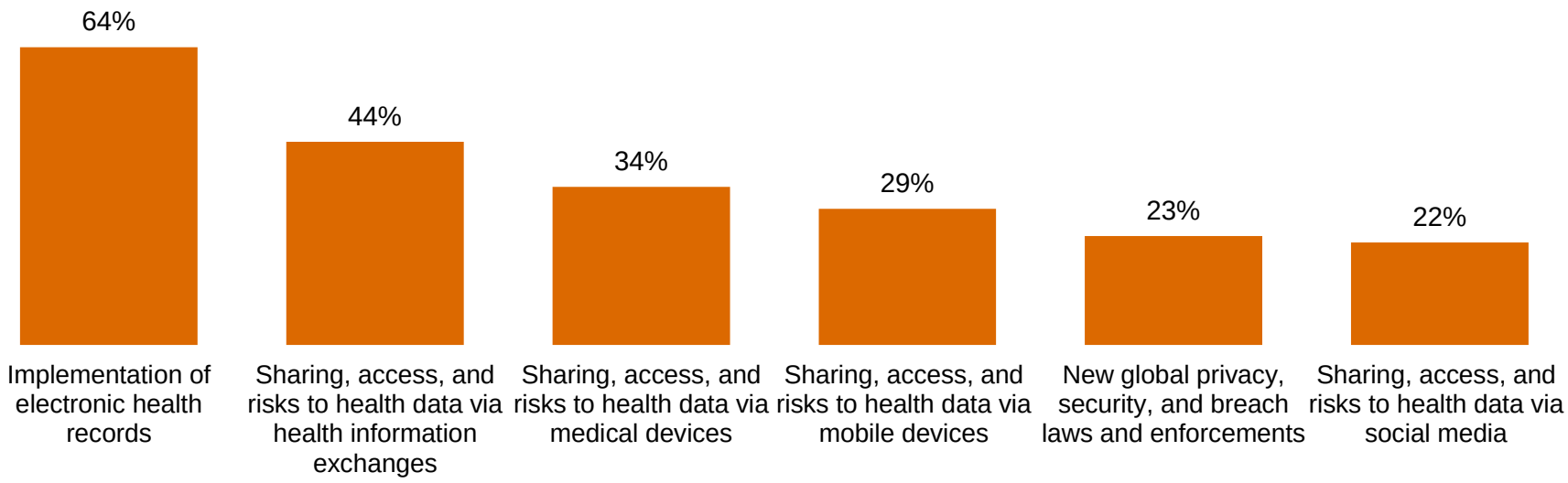


Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Healthcare provider respondents say concerns about new risks to patient health data drive security spending.

In particular, respondents say implementation of electronic health records influences security investments.

Healthcare trends driving investment in information security

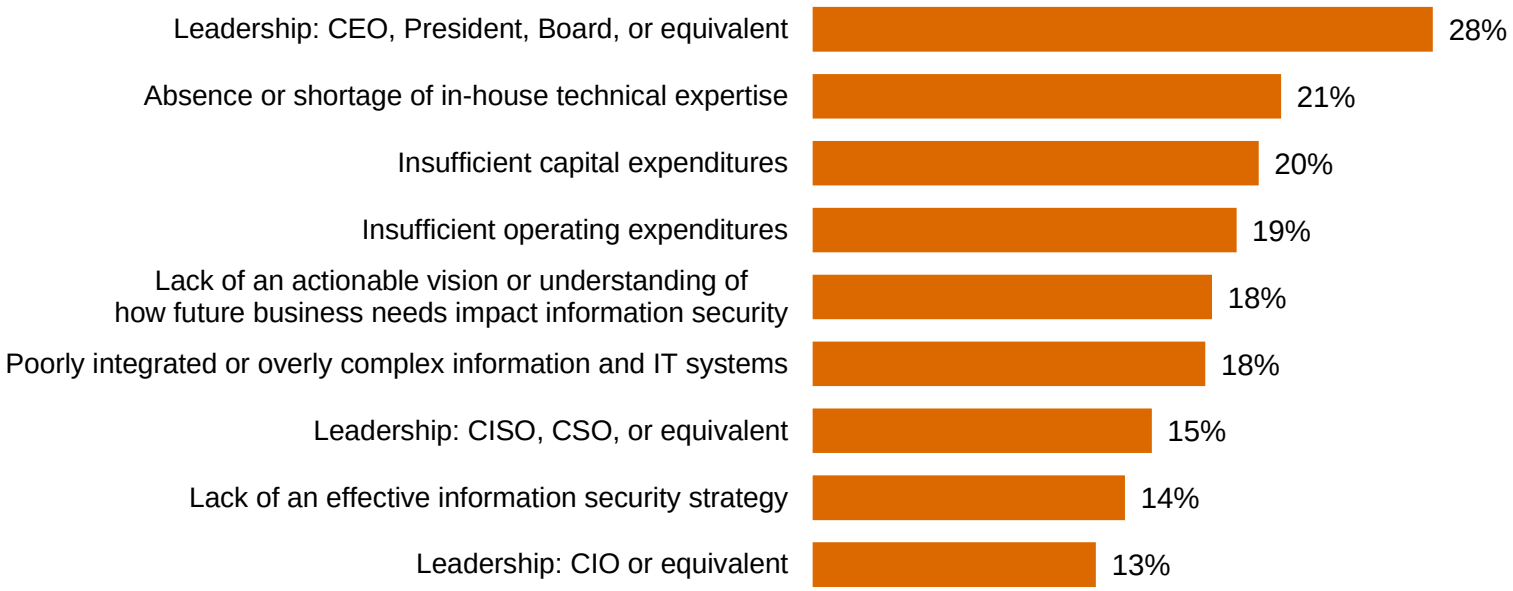


(Asked only of healthcare provider respondents) Question 3: “What healthcare trends are driving your investment in information security?” (Not all factors shown.)

Respondents say committed leadership from CEOs and other top executives is needed to improve security.

Building an effective security program for the future requires the support of top executives and a budget that is aligned with business needs.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are 10 key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
+1 949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
+1 646.471.5731
mark.a.lobel@us.pwc.com

US Healthcare Provider Contacts

Daniel Garrett
Principal
+1 267.330.8202
daniel.garrett@us.pwc.com

Mick Coady
Principal
+1 713.356.4366
mick.coady@us.pwc.com

James Koenig
Managing Director
+1 610.246.4426
james.h.koenig@us.pwc.com

Peter Harries
Principal
+1 602.750.3404
peter.harries@us.pwc.com

Dave Burg
Principal
+1 703.918.1067
david.b.burg@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

PwC

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

Industrial Products

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global industrial products industry are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising and confidence is high.

But while many companies have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased dramatically, as has the cost of breaches. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few industrial products companies have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that companies identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

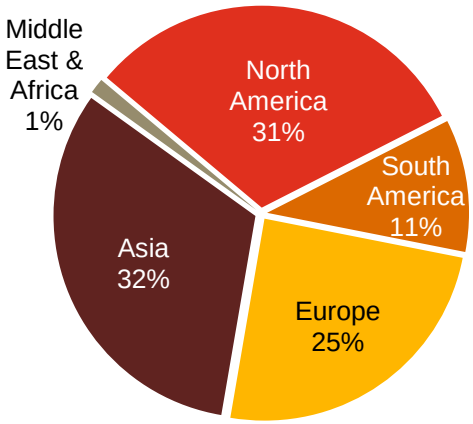
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

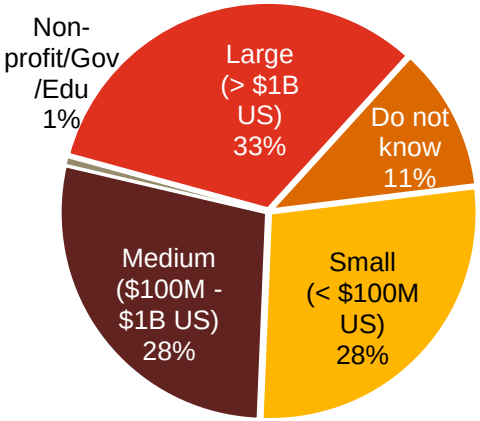
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 671 respondents from the industrial products industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

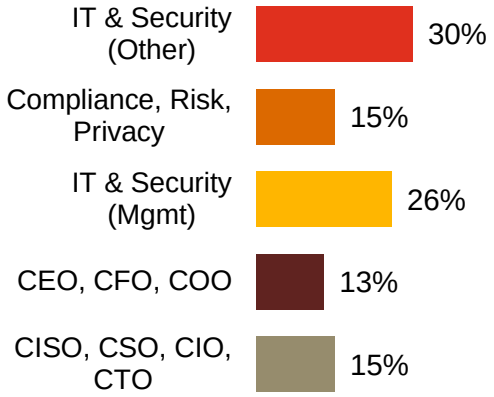
Industrial products respondents by region of employment



Industrial products respondents by company revenue size



Industrial products respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

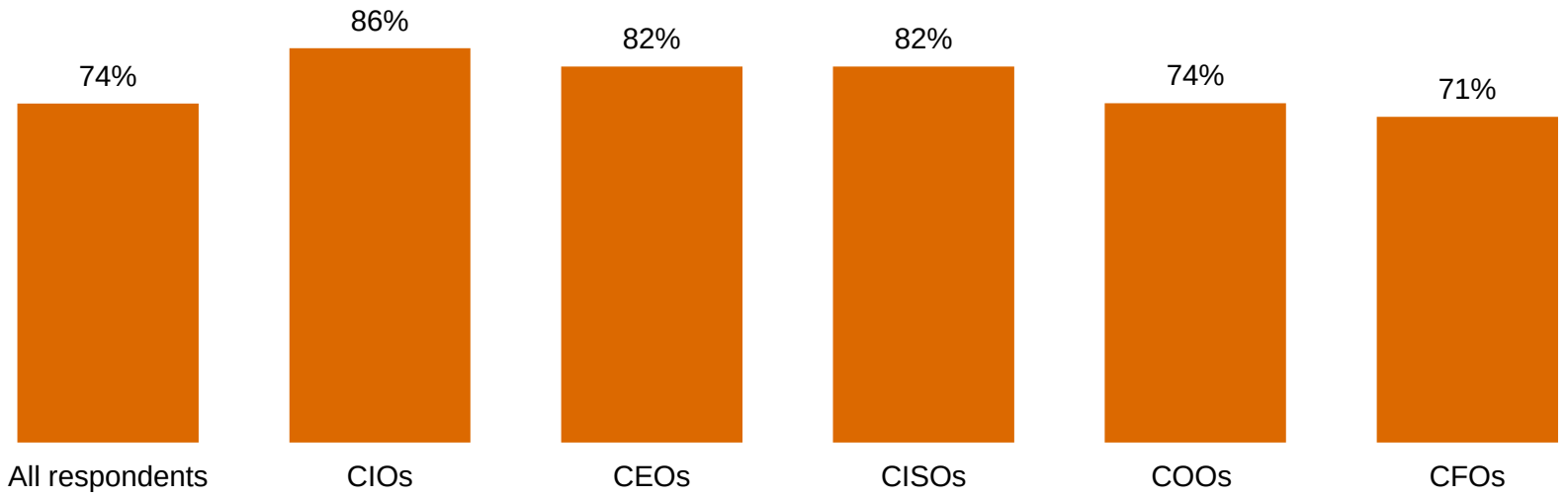
Section 2

Confidence in an era of advancing risks

Confidence is high: 74% of respondents believe their security activities are effective, with top execs even more optimistic.

In the C-suite,* 82% of industrial products CEOs say they are confident in their company's security program. Note that CFOs are the least confident among all executives.

Executive confidence in effectiveness of security activities (somewhat or very confident)

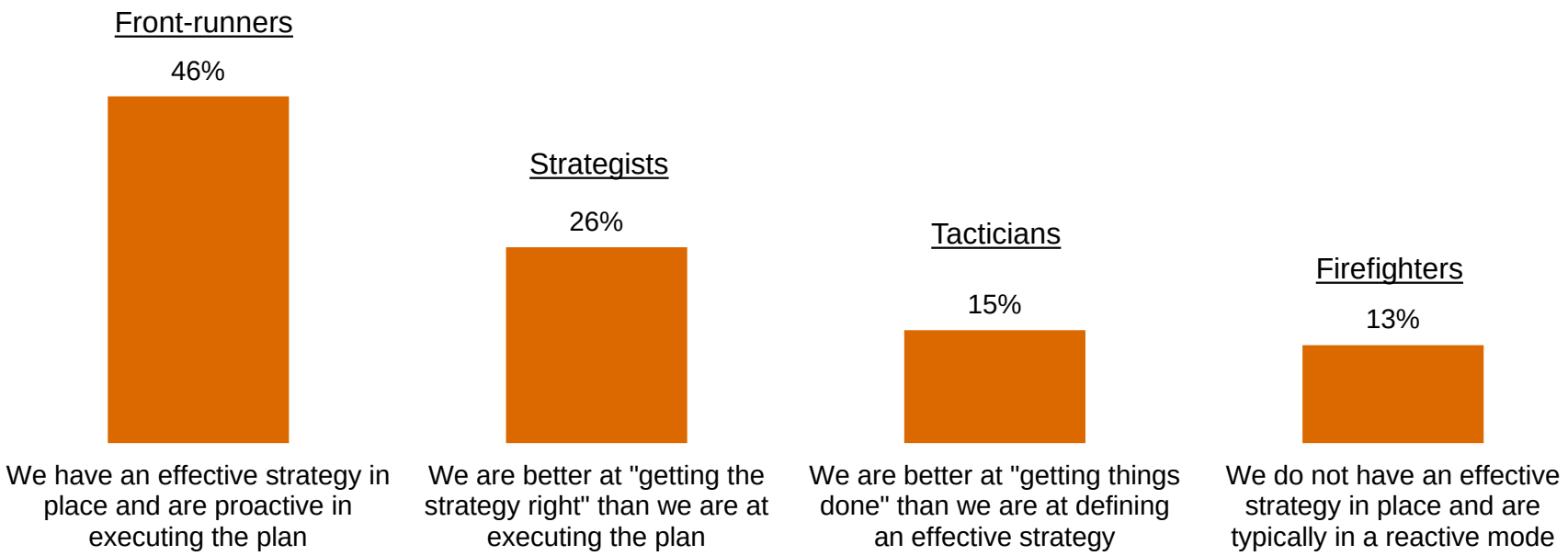


* CEOs, CFOs, and COOs

Question 39: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.") Question 1: "My job title most closely resembles"

46% of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

The number of industrial products respondents who say they have an effective strategy in place and are proactive in executing the plan increased 14% over last year. More than one in four (26%) say that they are better at getting the strategy right than executing the plan.



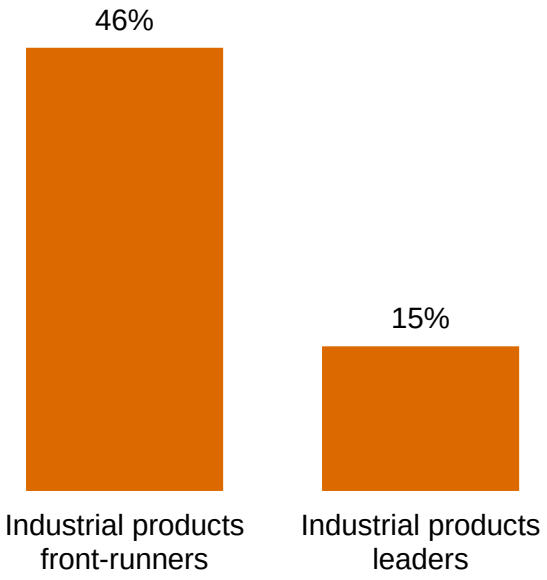
Question 27: "Which statement best characterizes your organization's approach to protecting information security?"

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured industrial products respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

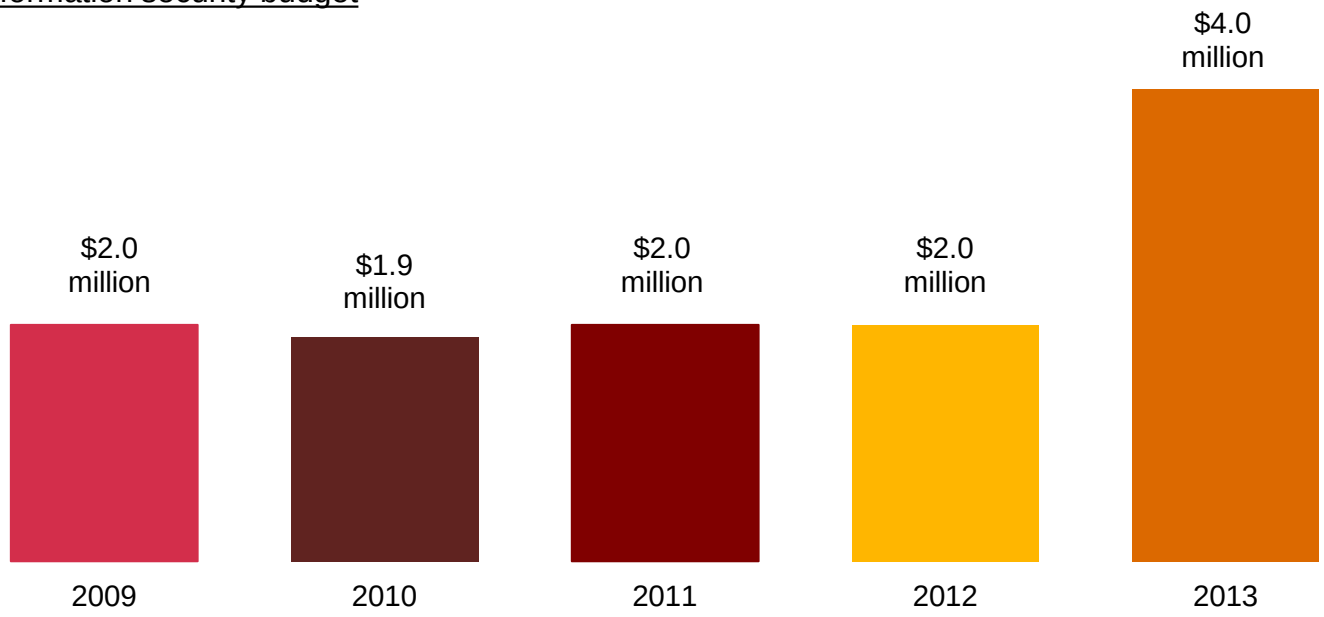


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Industrial products information security budgets increase significantly.

Industrial products security budgets average $4 million this year, a gain of nearly 100% over 2012. Organizations appear to understand that today's elevated threat landscape demands a substantial boost in security investment.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

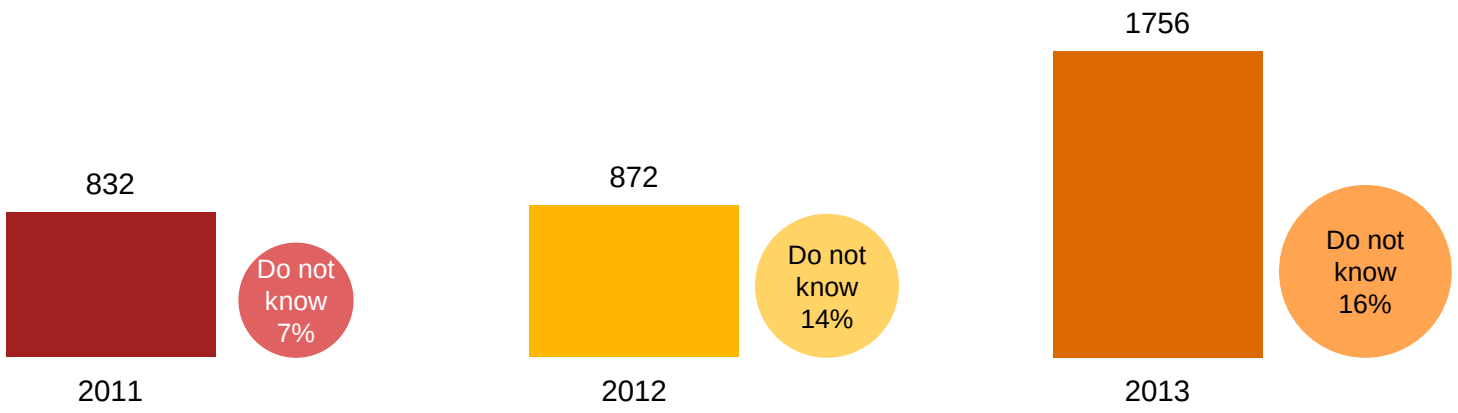
Section 3

Today's incidents, yesterday's strategies

*Industrial products companies detect more security incidents.**

Industrial products respondents detected 101% more security incidents in the past 12 months, perhaps an indication of today's elevated threat environment. It is troubling that respondents who do not know the number of incidents continues to rise.

Average number of security incidents in past 12 months



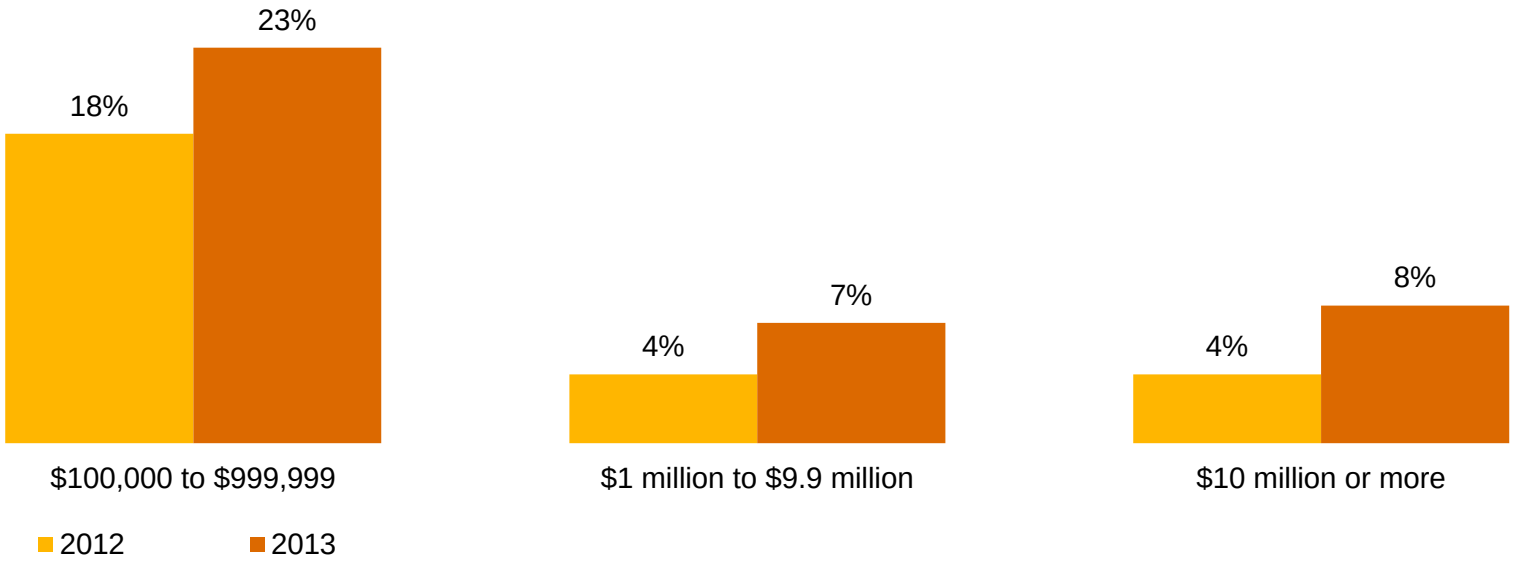
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months?

Financial costs of security incidents are rising, particularly among companies reporting high dollar-value impact.

Average financial losses reported by industrial products companies are up 64% over last year, which is not surprising given the cost and complexity of responding to threats. Big liabilities are increasing faster than smaller losses: Respondents reporting losses of $10 million or more doubled over 2012.

Financial losses of $100,000 or more

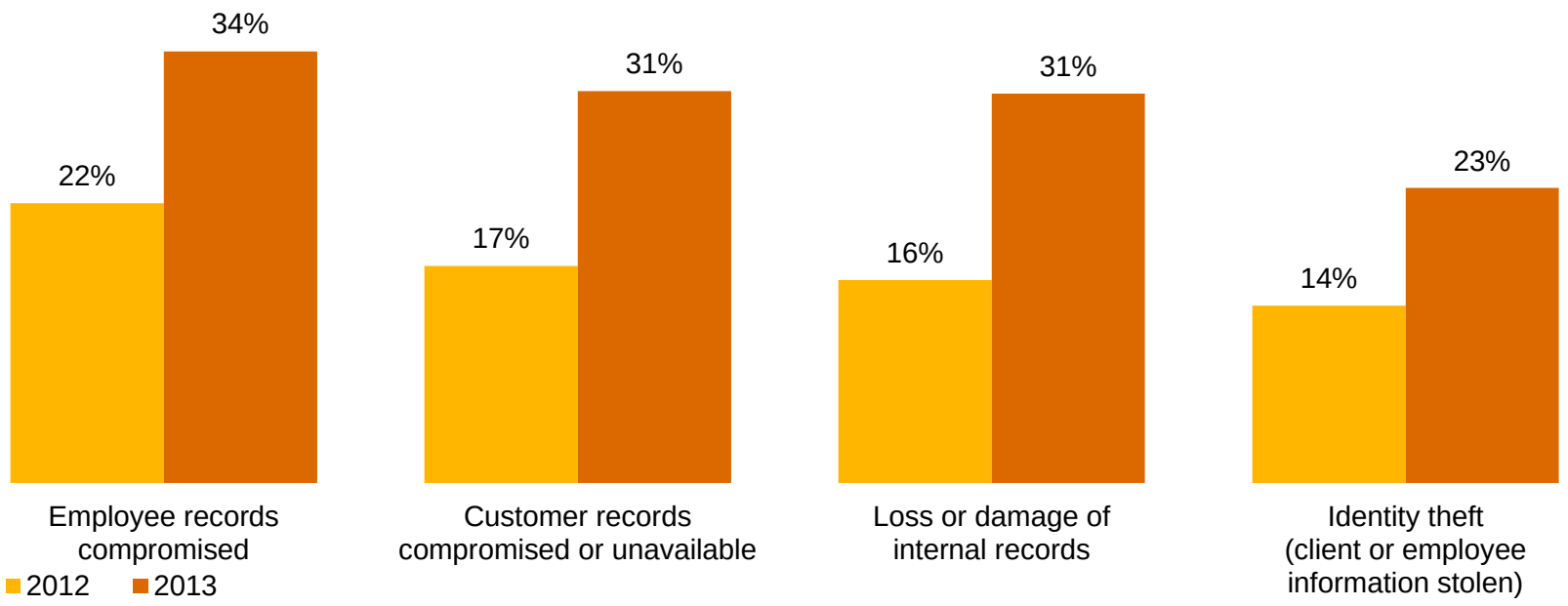


Question 22A: “Estimated total financial losses as a result of all security incidents” (Not all factors shown.)

Industrial products respondents report an increase in data loss as a result of security incidents.

Compromise of employee and customer records remain the most cited impacts, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records almost doubled over 2012.

Impact of security incidents

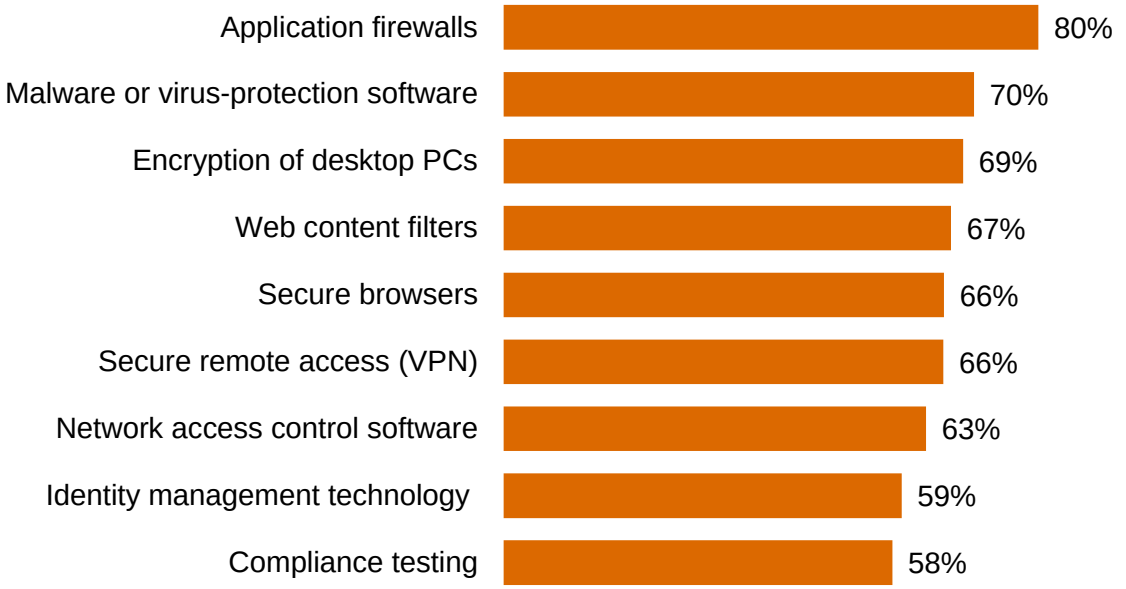


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

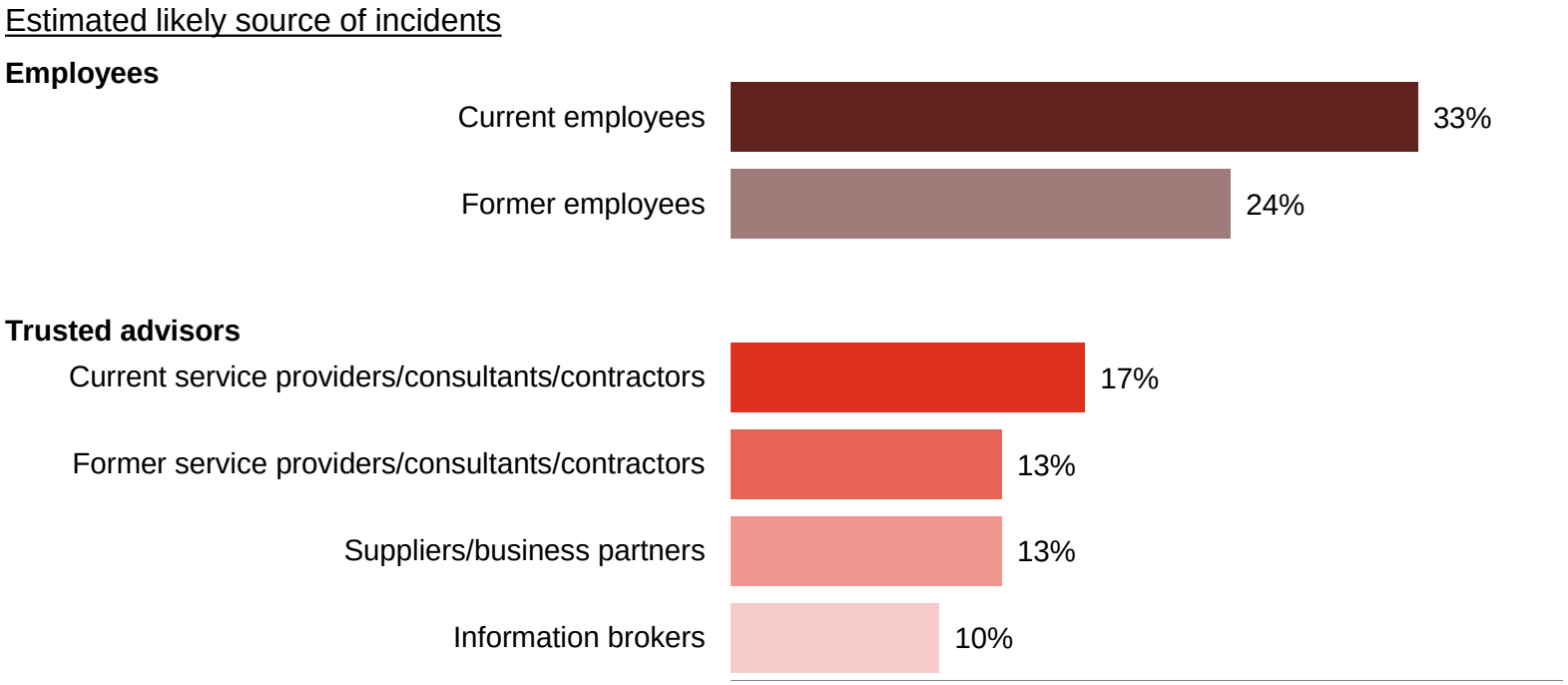
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most industrial products respondents.

It's the people you know—current and former employees, as well as other insiders—who are most likely to perpetrate security incidents.



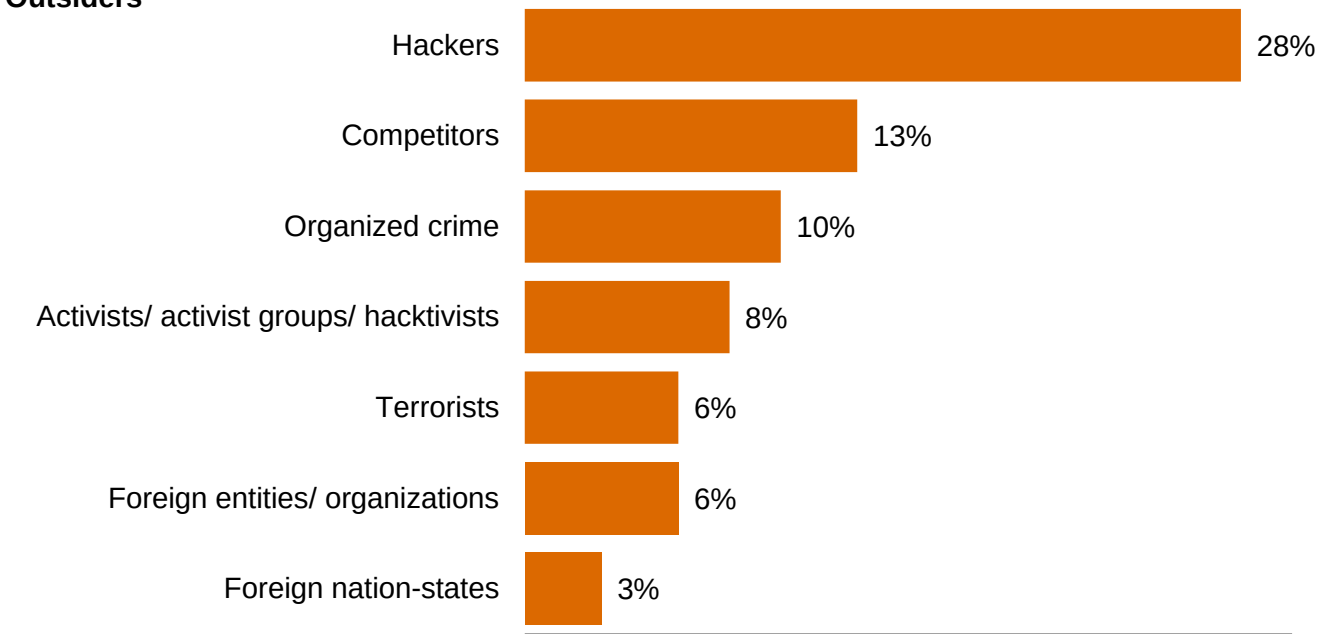
Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, companies are more likely to be hit by other outsiders.

Only 3% of industrial products respondents report that security incidents are perpetrated by foreign nation-states. Hackers represent a more likely danger, accounting for 28% of incidents.

Estimated likely source of incidents

Outsiders



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

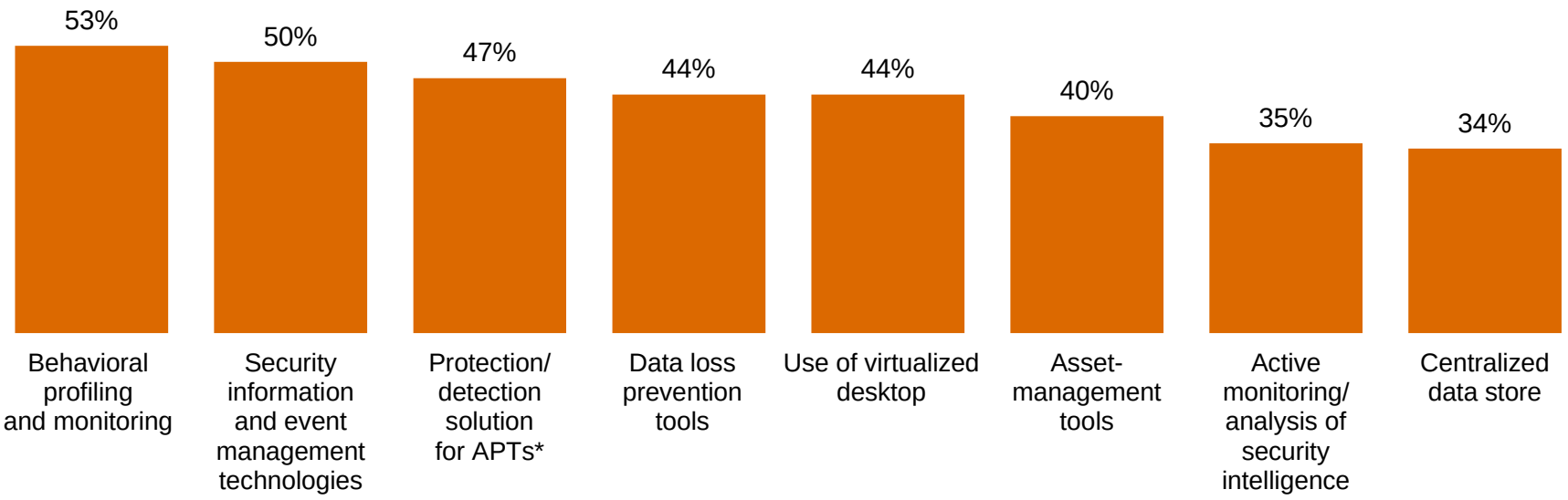
Section 4

A weak defense against adversaries

Many companies have not implemented technologies and processes that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place than traditional safeguards, according to industrial products respondents. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place



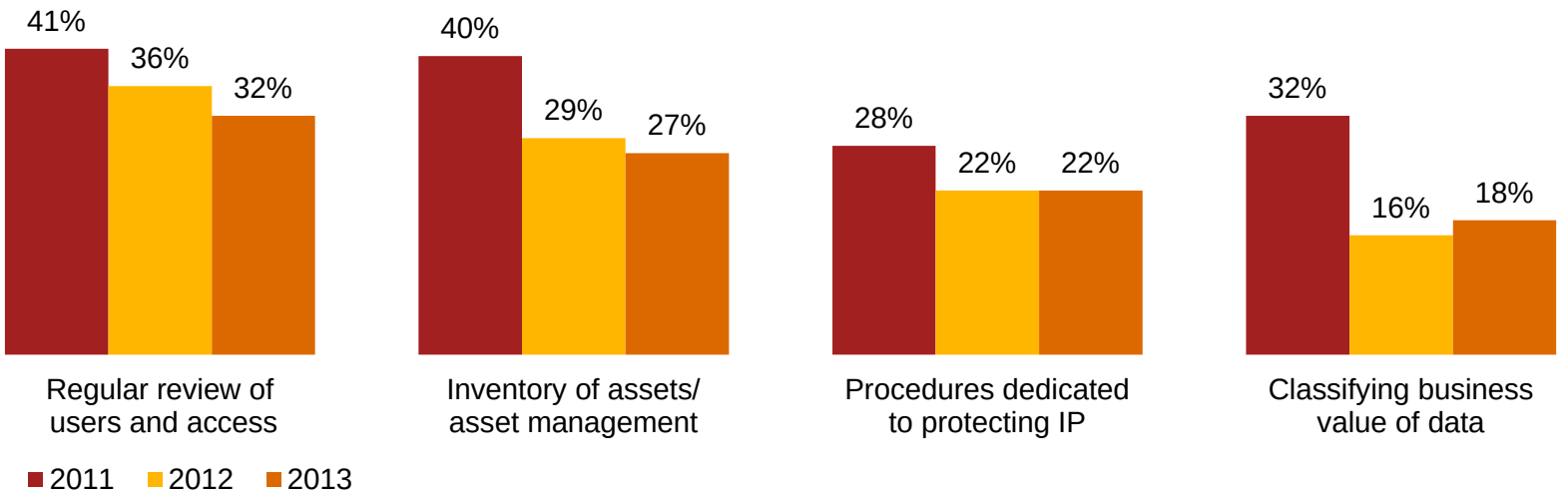
*Advanced persistent threats (APTs)

Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite the potential consequences, many companies do not adequately safeguard their high-value information.

It is imperative that companies identify, prioritize, and protect their "crown jewels." But implementation of basic policies to safeguard intellectual property (IP) is declining among industrial products respondents. Among those that have a plan to protect IP, however, 57% say they have implemented specific protection plans for emerging markets.

Have policies to help safeguard IP and trade secrets

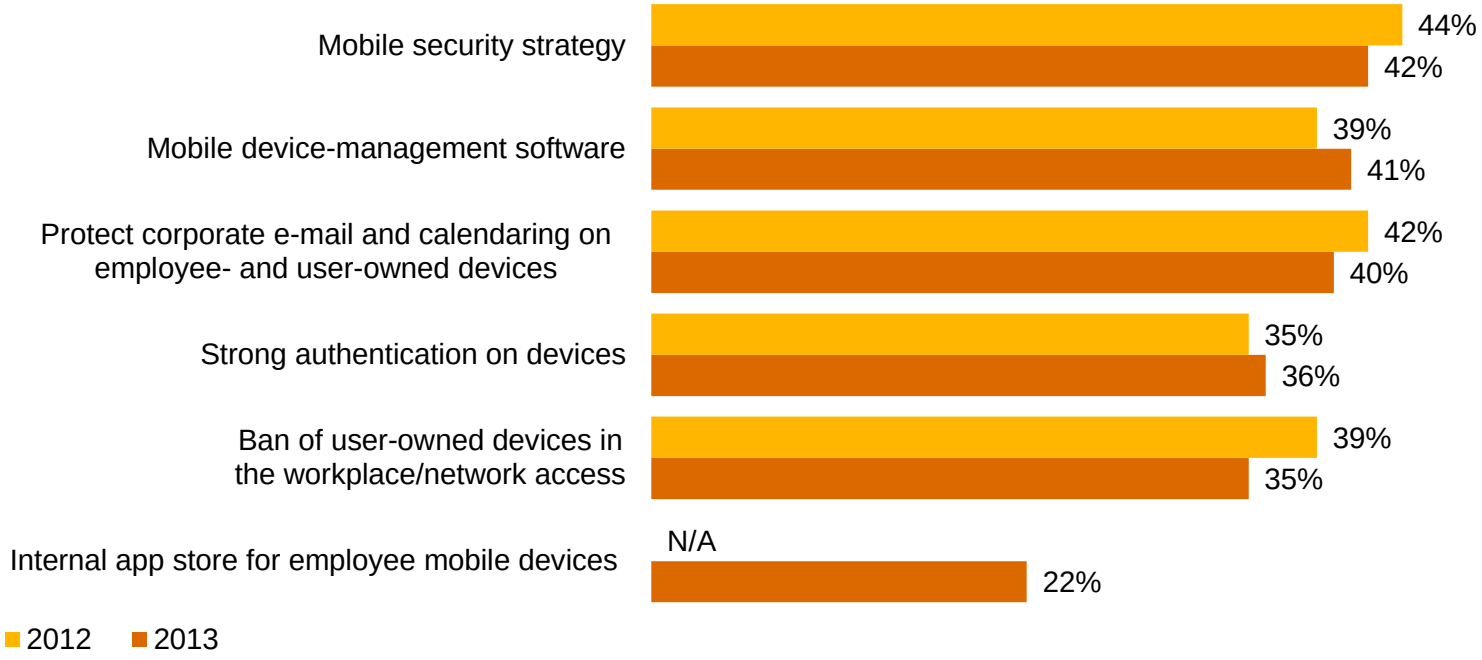


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.) (Asked only of industrial products respondents.) Question 2: "If your organization has a security plan in place to protect intellectual property, does it have specific plans for emerging markets? (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet industrial products respondents' efforts to implement mobile security do not show significant gains over last year and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

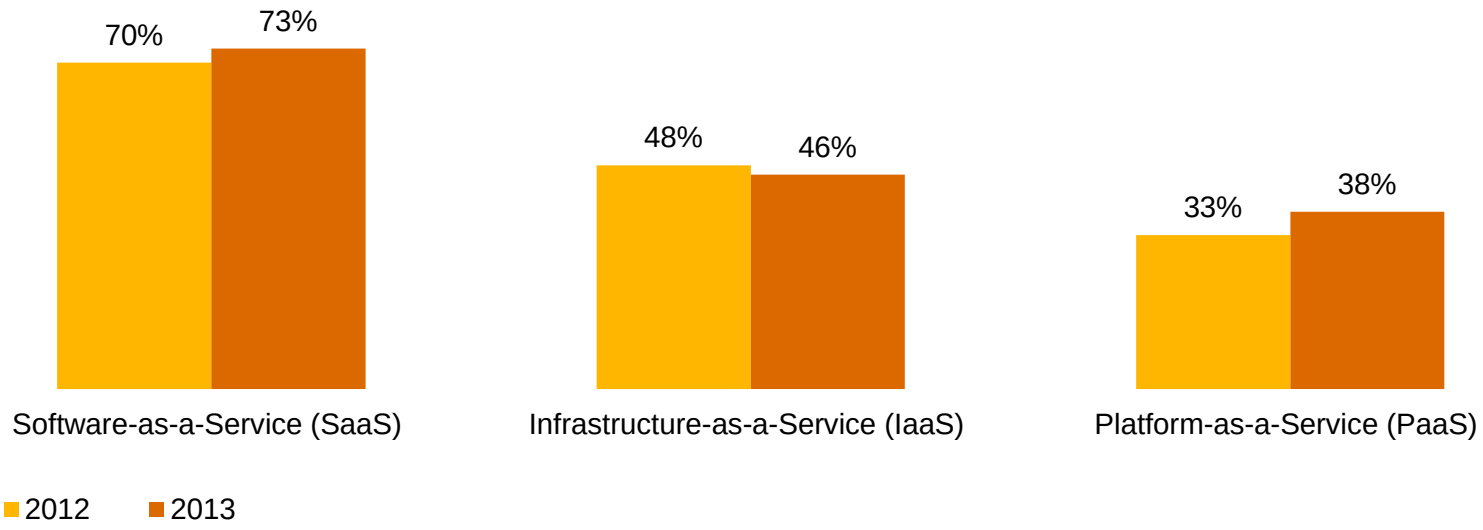


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

44% of respondents use cloud computing, but they often do not include cloud in their security policies.

Among those that use cloud services, 61% say the technology has improved security, but only 19% include provisions for cloud in their security policy. SaaS continues to be the most widely implemented type of cloud service.

Type of cloud service used

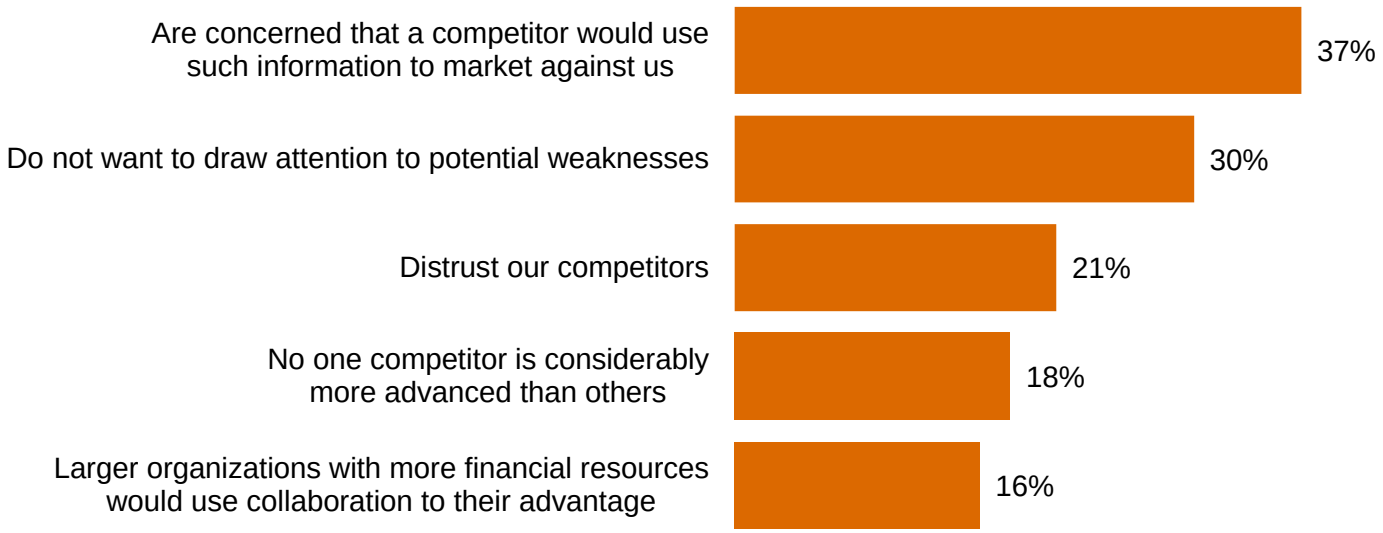


Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

33% of respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, we found that firms with collaborative C-suites intertwine business strategy and IT, which often improves performance and enables quick adaption to market changes.[1]

Reasons for not collaborating on information security



[1] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

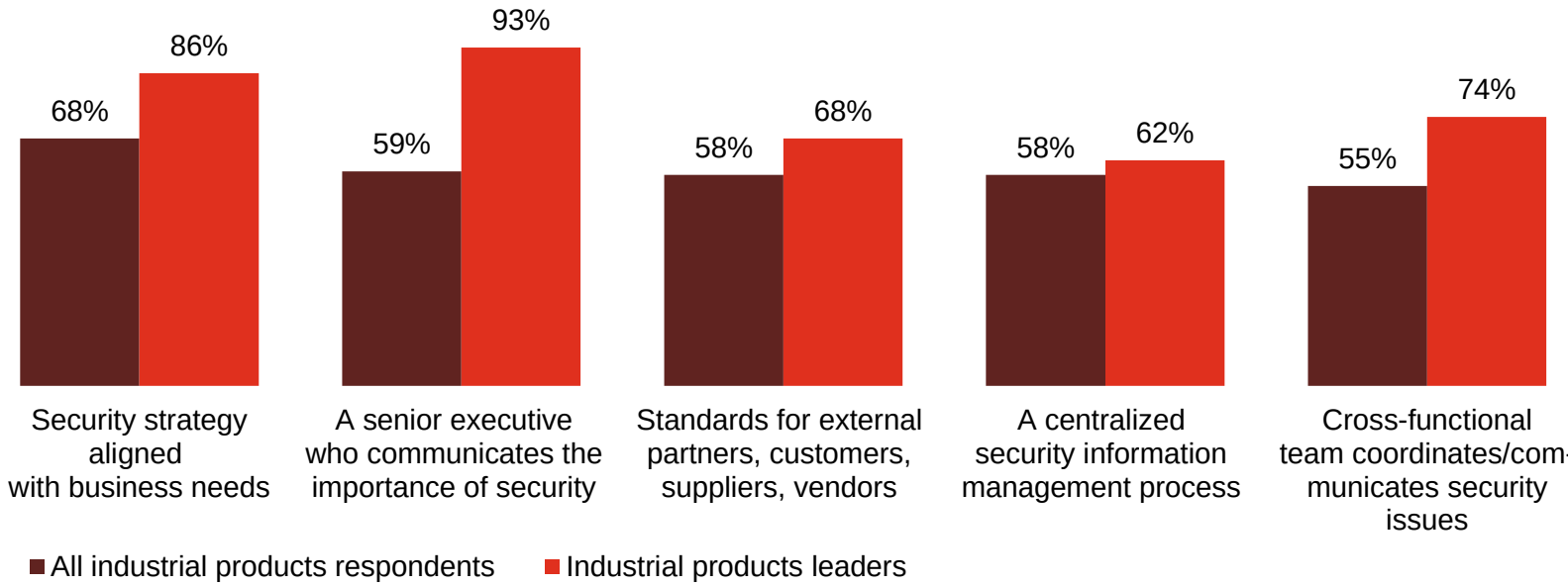
Section 5

Preparing for the threats of tomorrow

Leaders are enhancing capabilities in ways that show security is now a business imperative—not just an IT issue.

Aligning security with business needs, improving communications, and setting standards for external partners show that industrial products leaders, in particular, are rethinking the fundamentals of security.

Security policies and safeguards currently in place: All respondents vs. leaders



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?"

Many companies have invested in technology safeguards to secure their ecosystems against today's evolving threats.

Industrial products leaders are more likely to have implemented these technologies. But given today's elevated threat landscape, *all* organizations should strongly consider implementation of these safeguards.

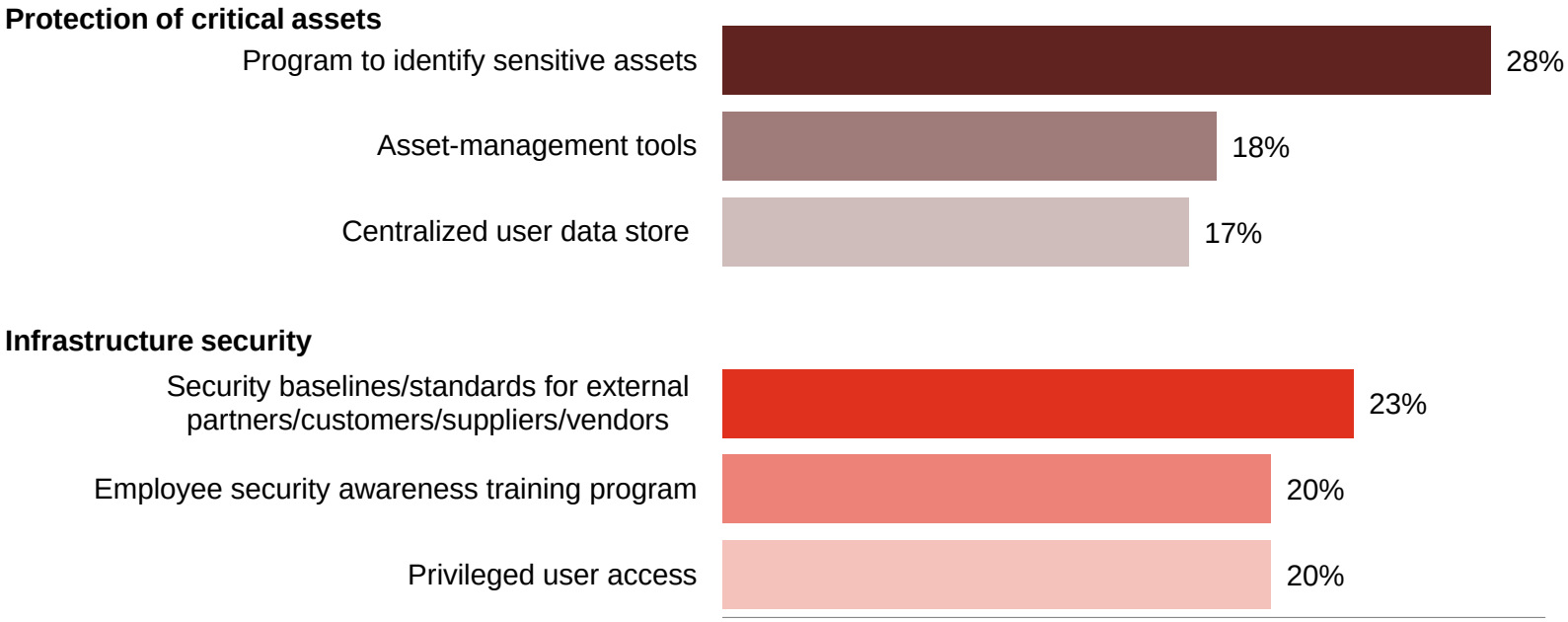
Technology safeguards currently in place	All industrial products respondents	Industrial products leaders
Malicious code detection tools	73%	92%
Intrusion prevention tools	67%	86%
Centralized user data store	66%	80%
Security plan to mitigate a breach of manufacturing control systems	62%	90%
Intrusion detection tools	60%	76%
Security event correlation tools	55%	71%
Mobile device malware detection	53%	72%
Behavioral profiling and monitoring	47%	68%
Offensive technologies	47%	66%

Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.) (Asked only of industrial products respondents) Question 1: "Does your organization have a security plan in place to mitigate a breach of manufacturing control systems?"

What business imperatives and processes will industrial products companies prioritize this year?

Some of the highest priorities cited by respondents include technologies that can help the organization protect its most valuable assets and safeguard the infrastructure.

Safeguards not in place but a top priority over the next 12 months

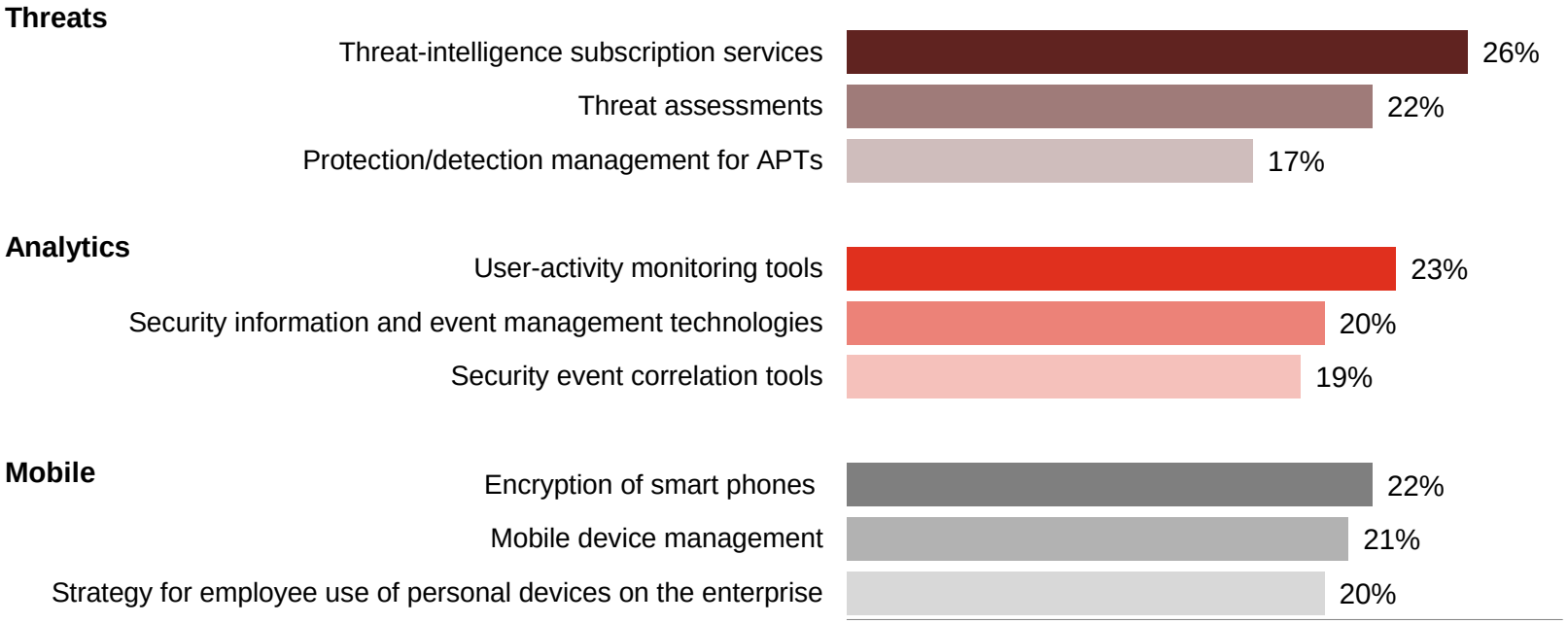


Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?"
Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and organizations are prioritizing technologies that can help them better understand threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Effective security demands that companies align security spending and policies with business objectives.

This year, more industrial products respondents say security spending is aligned with business objectives. This suggests that they understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

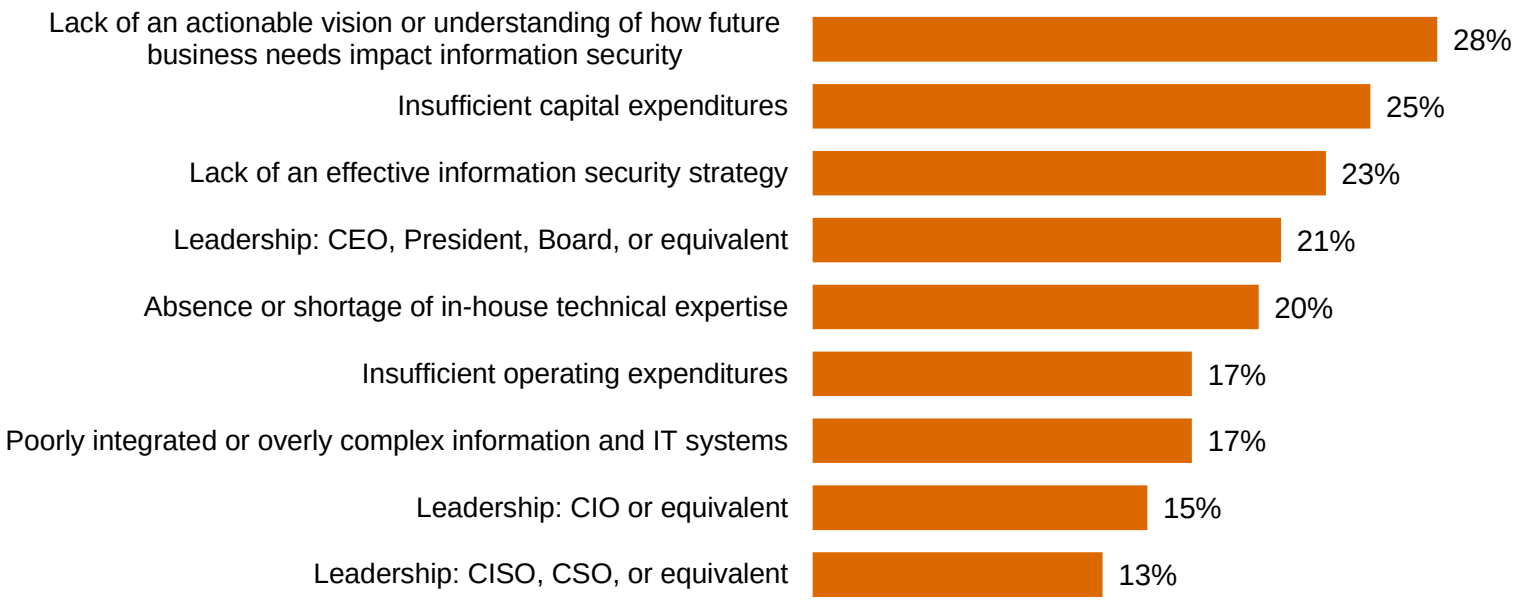
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?" Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?"

An understanding of future business needs and more money are needed to improve security.

Industrial products respondents say better security also requires a solid strategy and the support of top leadership, the CEO in particular.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
+1 949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
+1 646.471.5731
mark.a.lobel@us.pwc.com

US Industrial Products Contacts

Robert McCutcheon
Partner
+1 412.355.2935
robert.w.mccutcheon@us.pwc.com

Quentin Orr
Managing Director
+1 267.330.2699
e.quentin.orr@us.pwc.com

John Pearce
Director
+1 703.346.9071
john.pearce@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

Oil & Gas

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global oil & gas (O&G) industry are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising and confidence is high.

But while many companies have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased dramatically, as has the cost of breaches. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few oil & gas companies have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that O&G companies identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

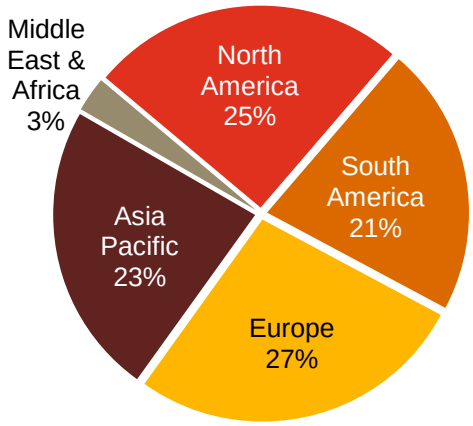
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

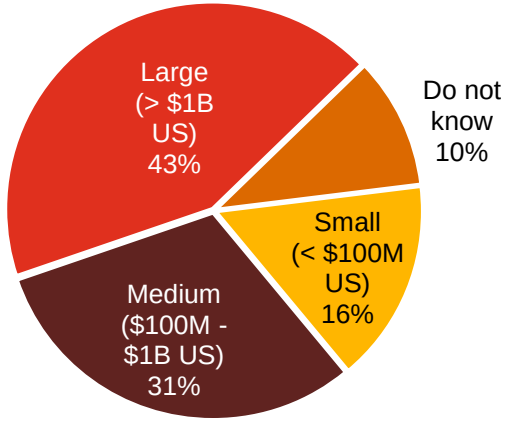
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 107 respondents from the oil & gas industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

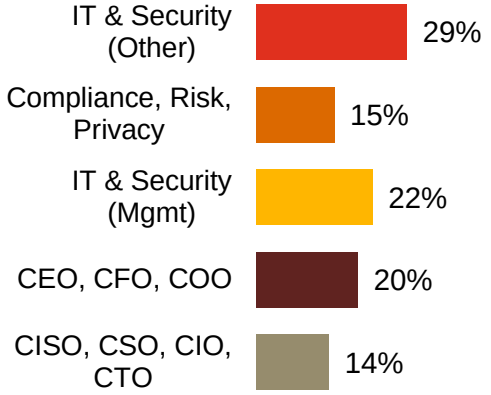
O&G respondents by region of employment



O&G respondents by company revenue size



O&G respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

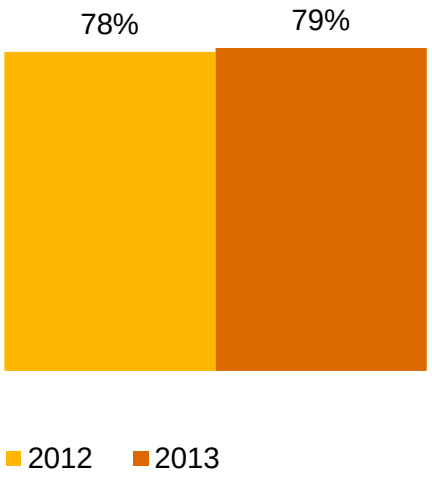
Section 2

Confidence in an era of advancing risks

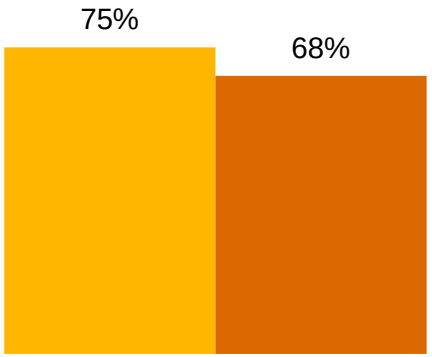
Confidence is high: 79% of O&G respondents believe their security activities are effective.

Confidence in the security programs of partners and suppliers decreased over last year, however.

Confidence in effectiveness of security activities



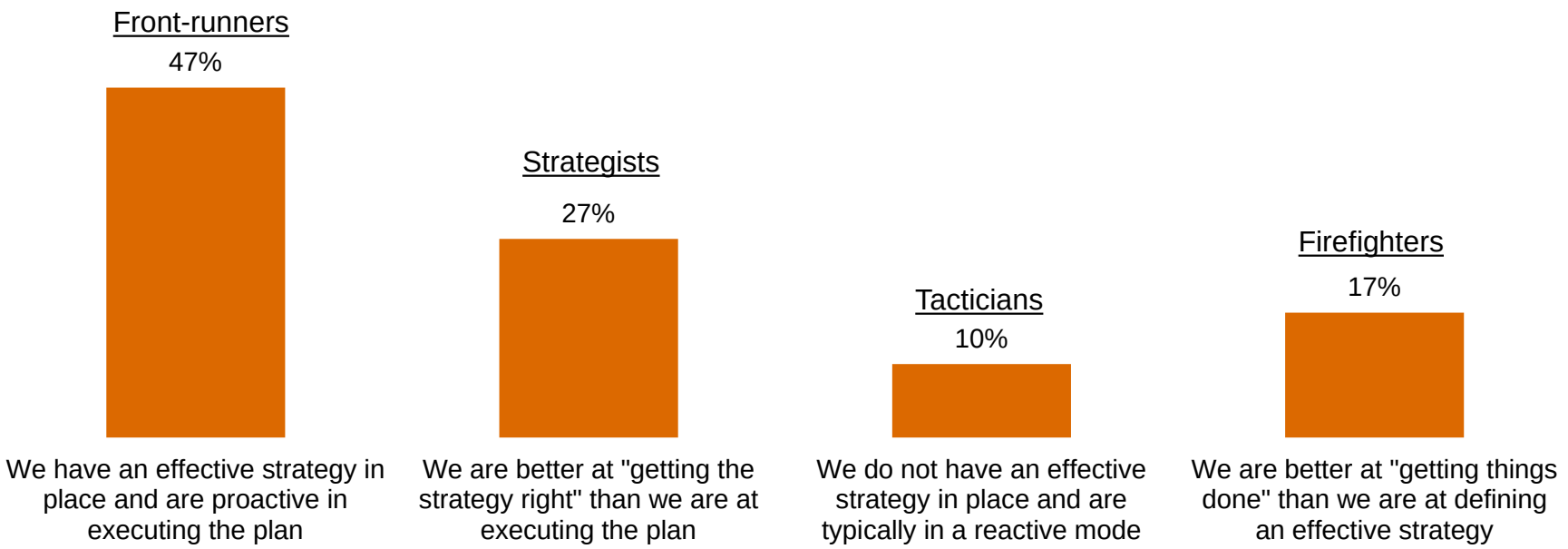
Confidence in effectiveness of partners'/suppliers' security activities



Question 39: "How confident are you that your organization's information security activities are effective?" Question 40: "How confident are you that your partners'/suppliers' information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.")

47% of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

Almost half of O&G respondents say they have an effective strategy in place and are proactive in executing the plan, a 10% increase over last year. More than one in four (27%) say they are better at getting the strategy right than executing the plan.



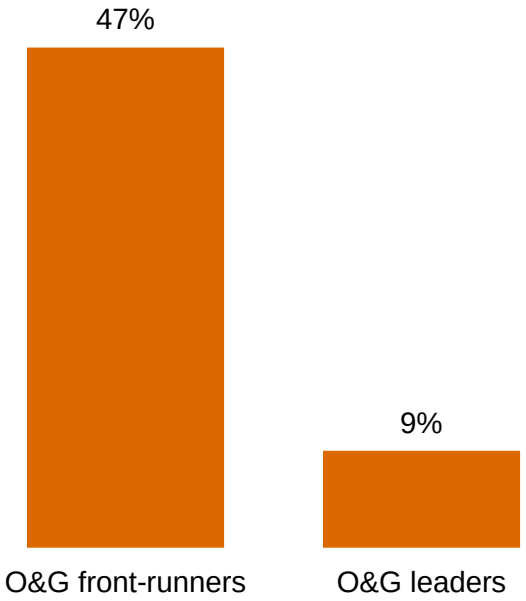
Question 27: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding.)

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured O&G respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

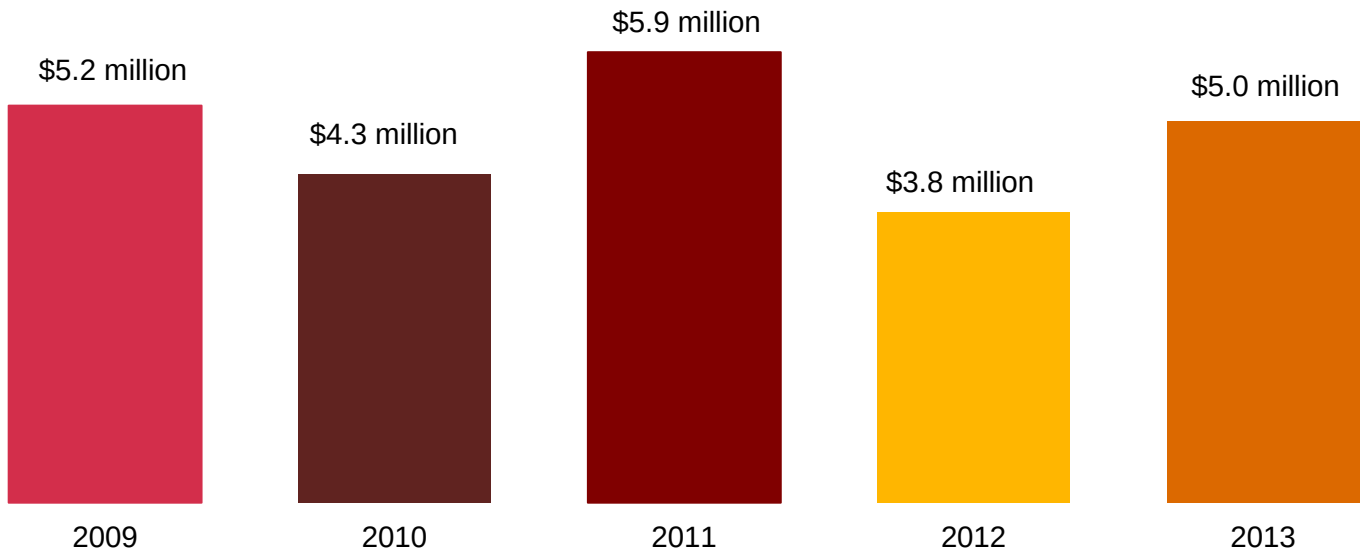


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

O&G information security budgets increase significantly.

Information security budgets average $5 million this year, a 32% increase over 2012. O&G companies appear to understand that today's elevated threat landscape demands a substantial boost in security investment.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

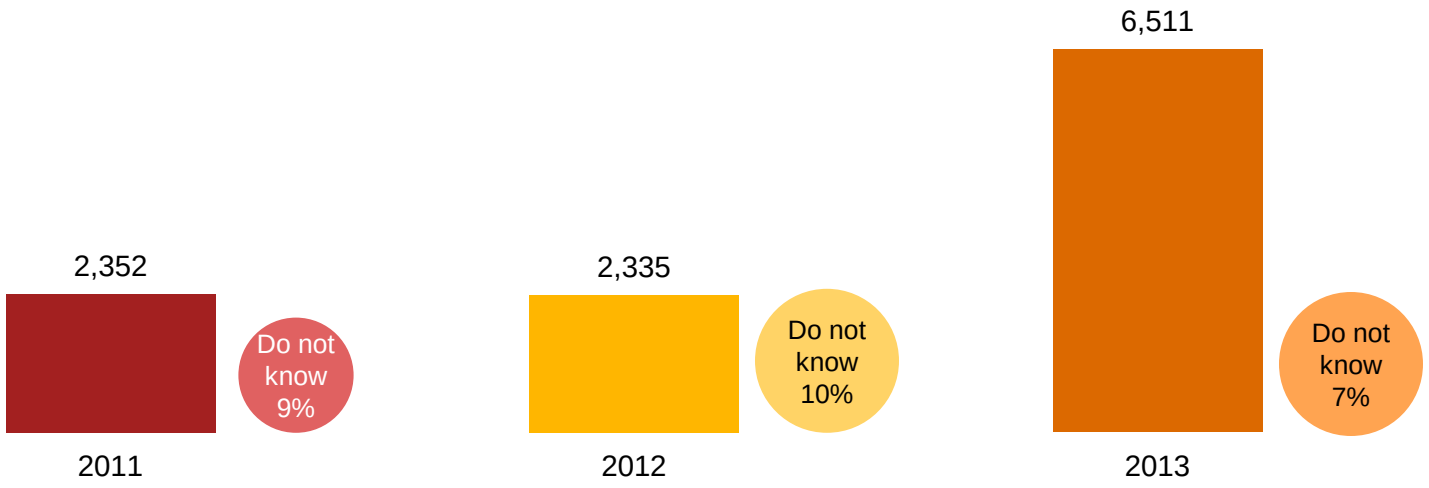
Section 3

Today's incidents, yesterday's strategies

*O&G respondents are detecting significantly more security incidents.**

O&G respondents detected 179% more security incidents in the past 12 months compared with 2012, perhaps an indication of today's elevated threat environment. Average financial losses as a result of incidents soared 470% over last year, which is not surprising given the cost and complexity of responding to incidents.

Average number of security incidents in past 12 months



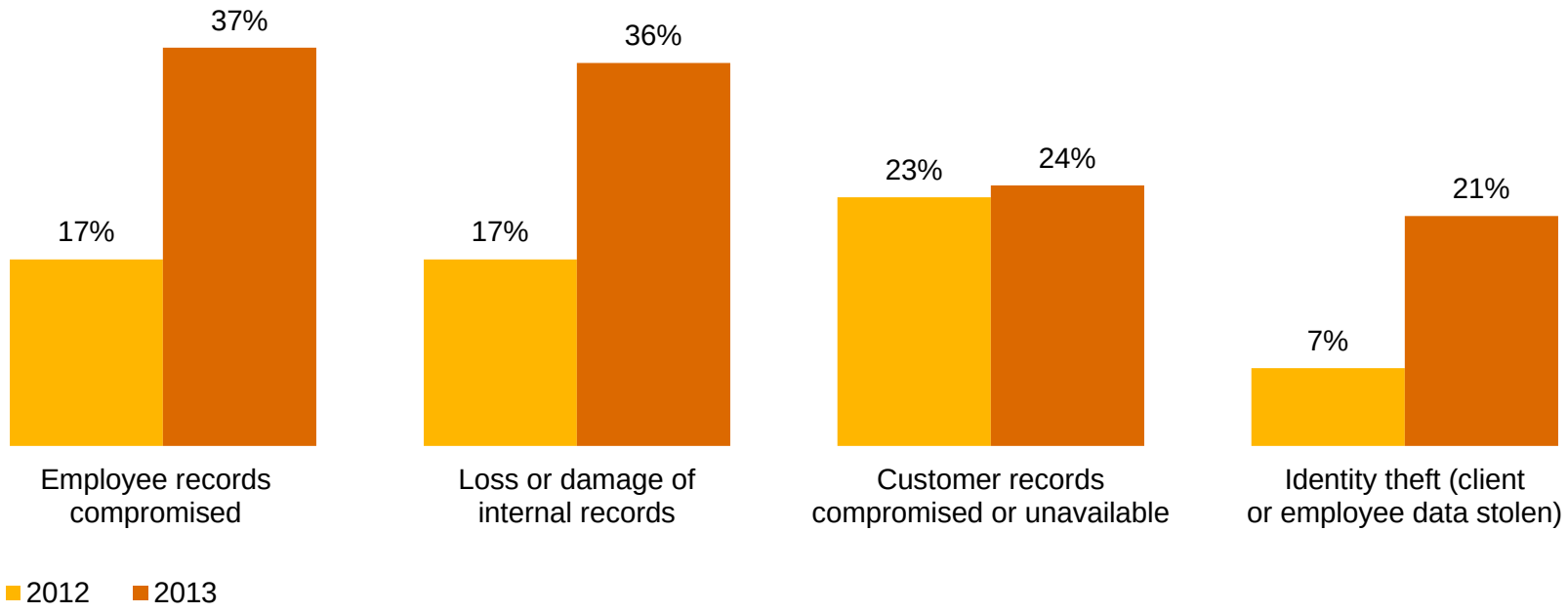
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

O&G respondents report significant increases in data loss as a result of security incidents.

Compromise of employee records more than doubled over last year, potentially jeopardizing an organization's most valuable relationships. Also significant: Theft of client or employee data tripled over 2012.

Impact of security incidents

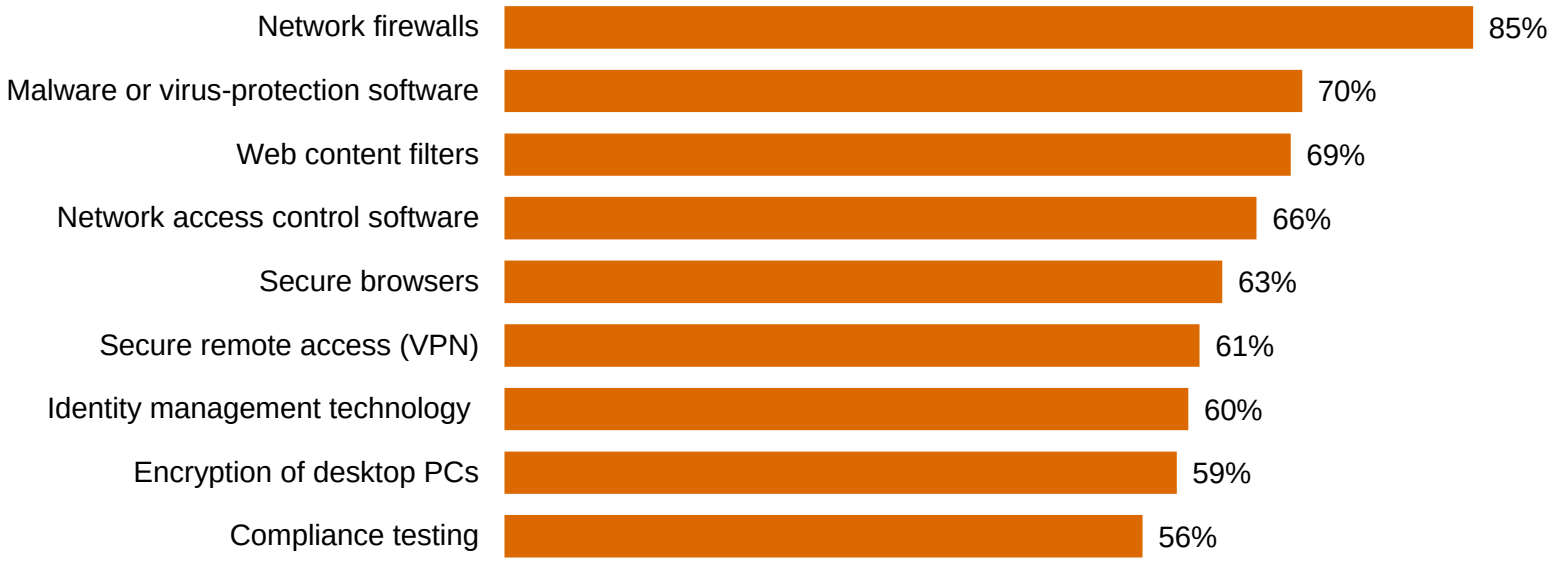


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

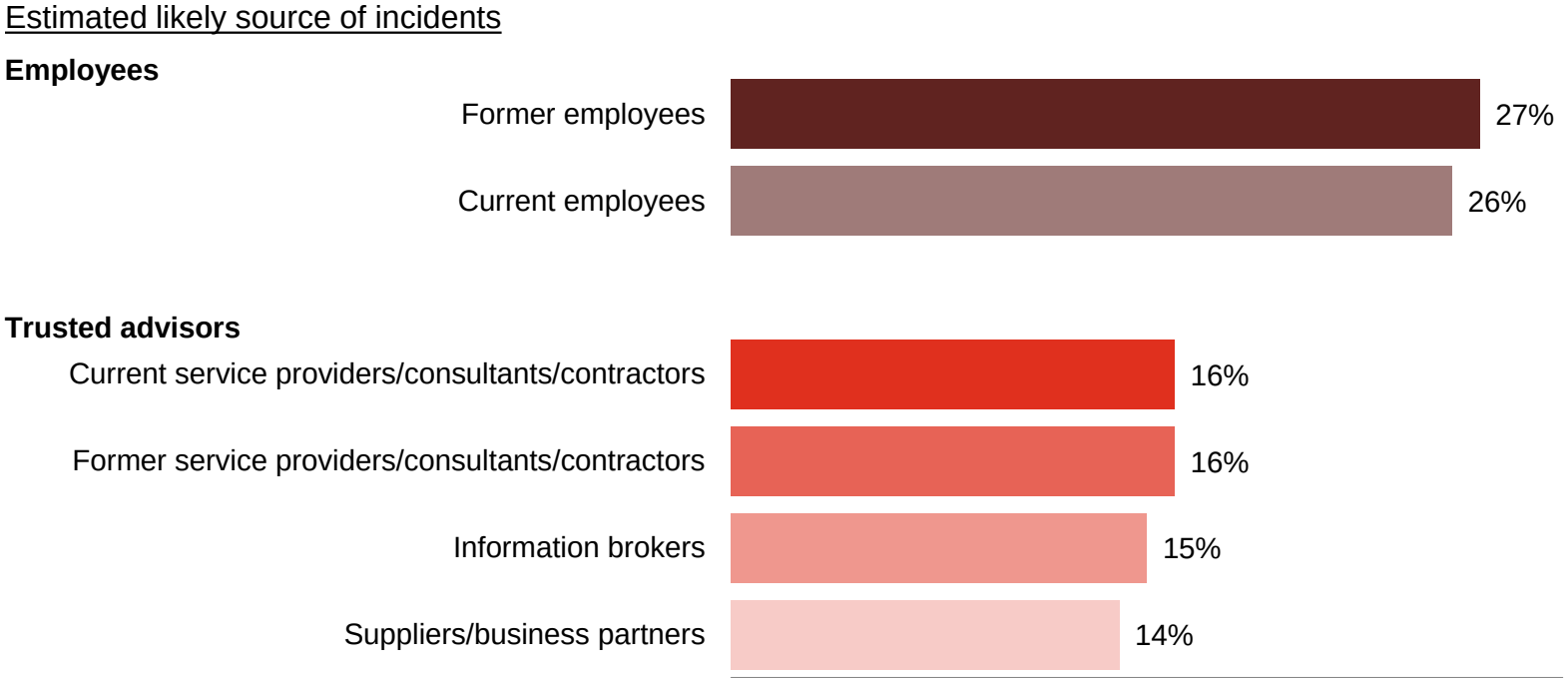
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most O&G respondents.

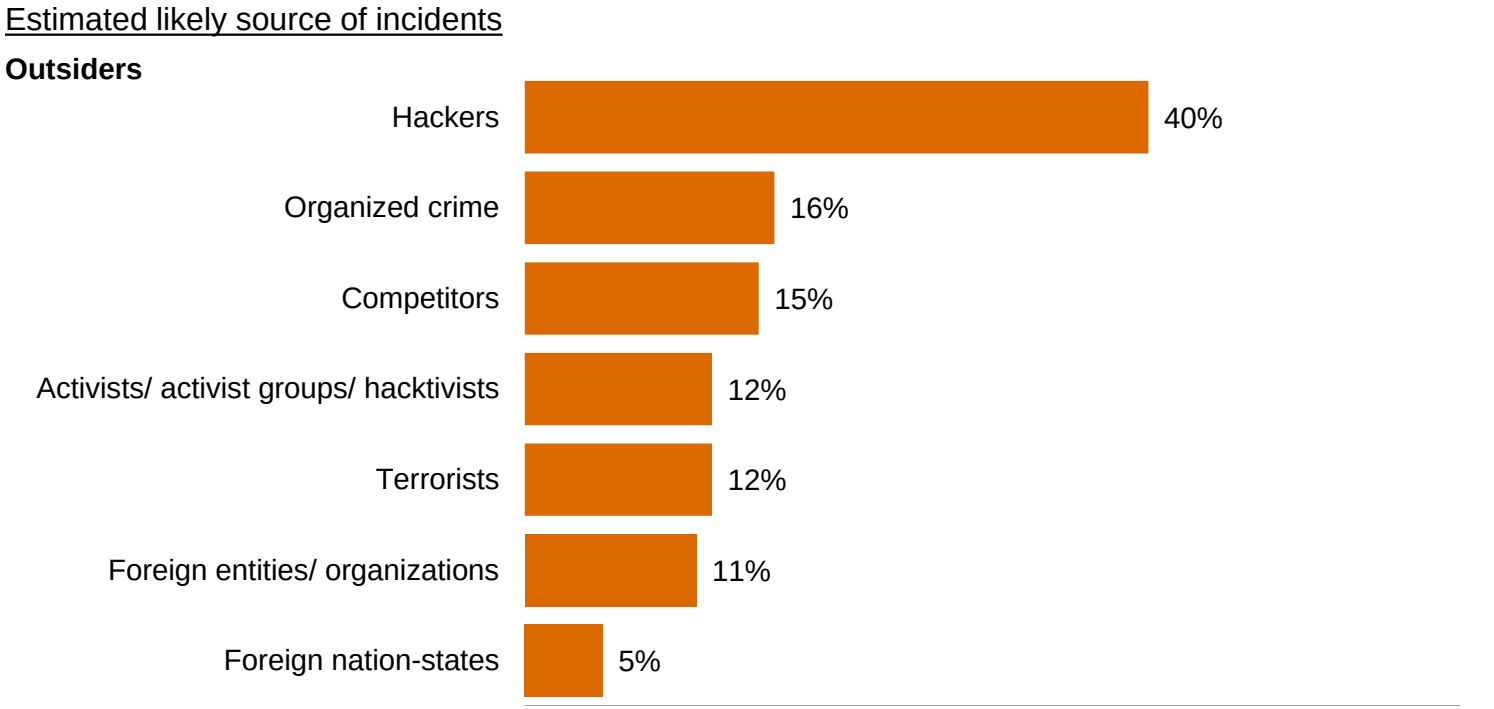
The people you know—particularly current and former employees—are most likely to perpetrate security incidents.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

While attacks backed by nation-states make headlines, O&G companies are more likely to be hit by other outsiders.

Only 5% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

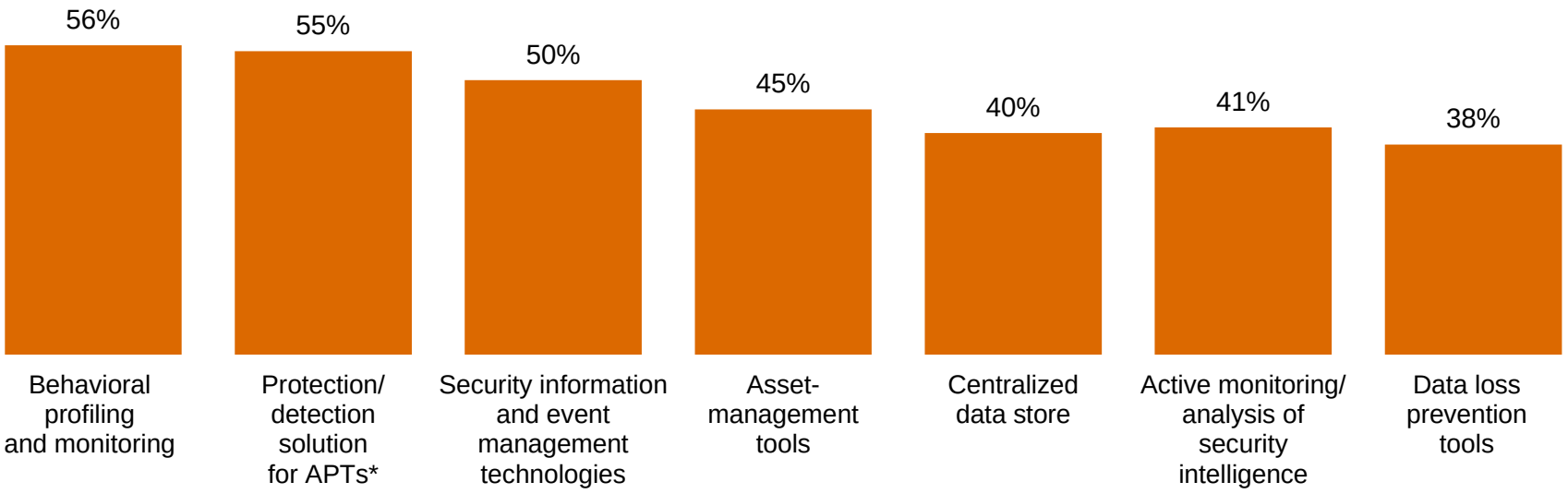
Section 4

A weak defense against adversaries

Many O&G companies have not implemented technologies and processes that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place than traditional technologies. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place



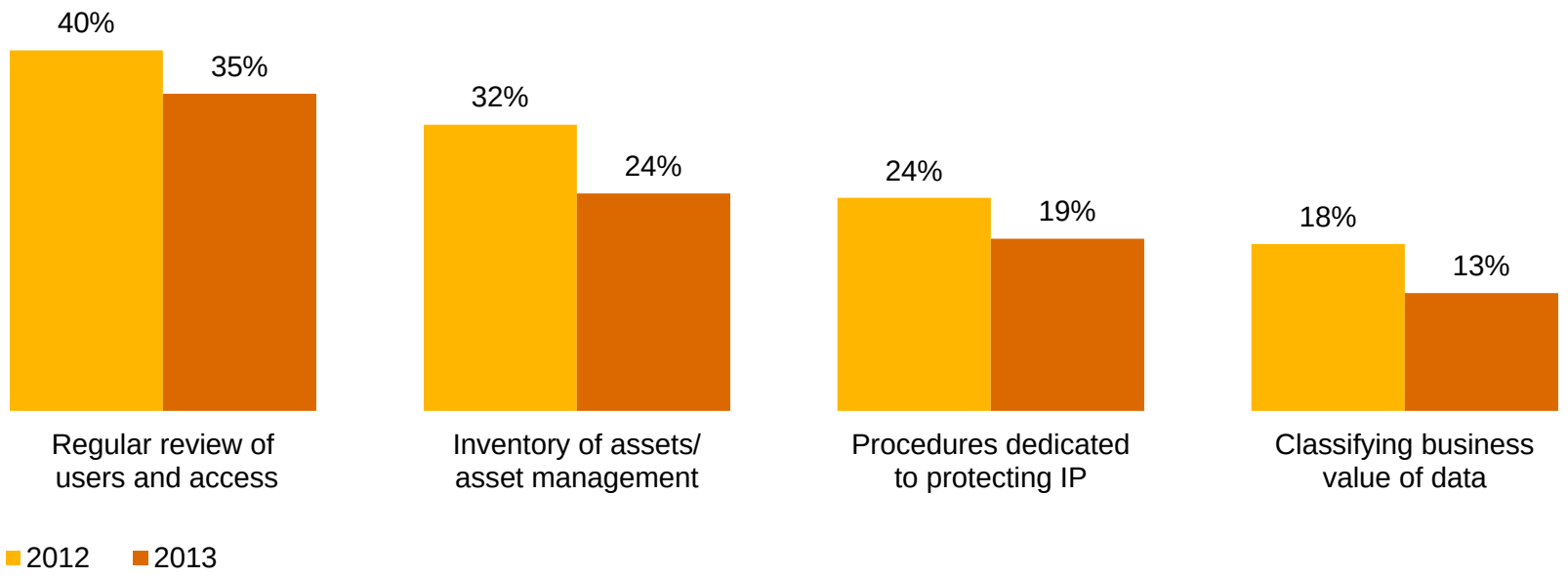
*Advanced persistent threats (APTs)

Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite the potential consequences, many O&G companies do not adequately safeguard high-value information.

It is imperative that organizations identify, prioritize, and protect their "crown jewels." O&G respondents, however, report a decline in implementation of basic policies to safeguard intellectual property (IP).

Have policies to help safeguard IP and trade secrets

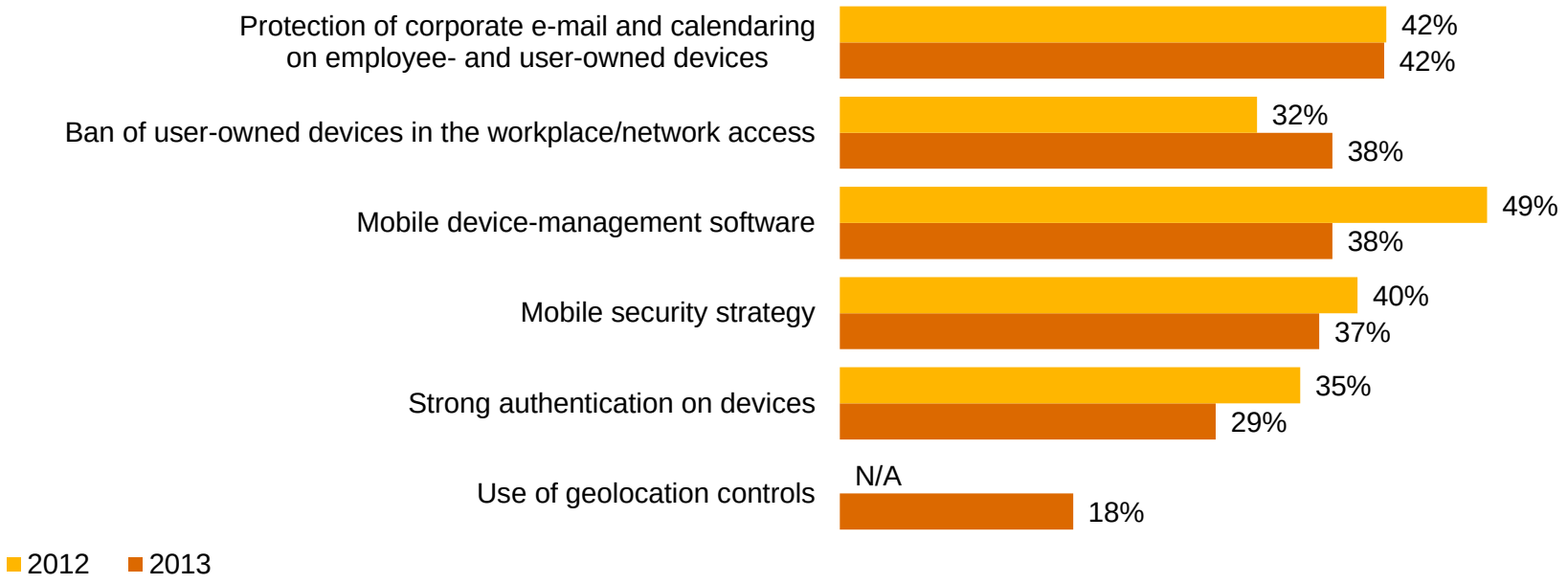


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security is declining.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet O&G respondents' efforts to implement most mobile security programs have diminished over last year and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

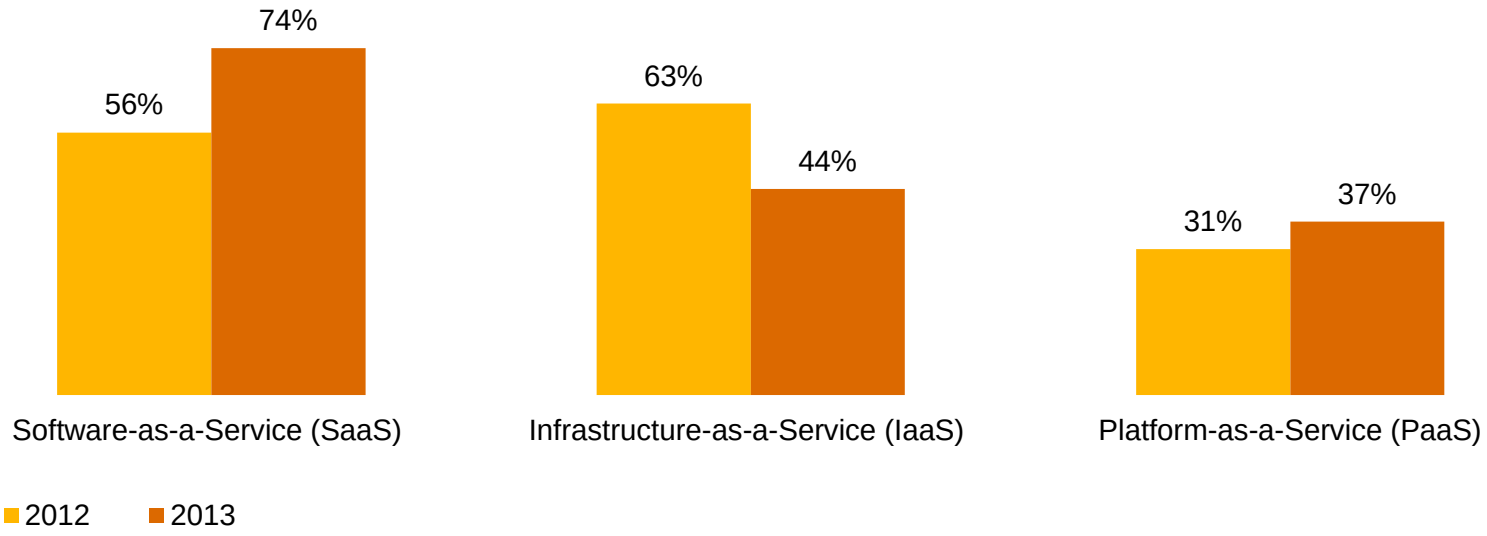


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Many O&G respondents use cloud computing, but they often do not include cloud in their security policies.

While 43% of O&G respondents report using cloud computing—and 56% say the technology has improved security—only 25% include provisions for cloud in their security policy. SaaS deployments increased 32% over the year before.

Type of cloud service used

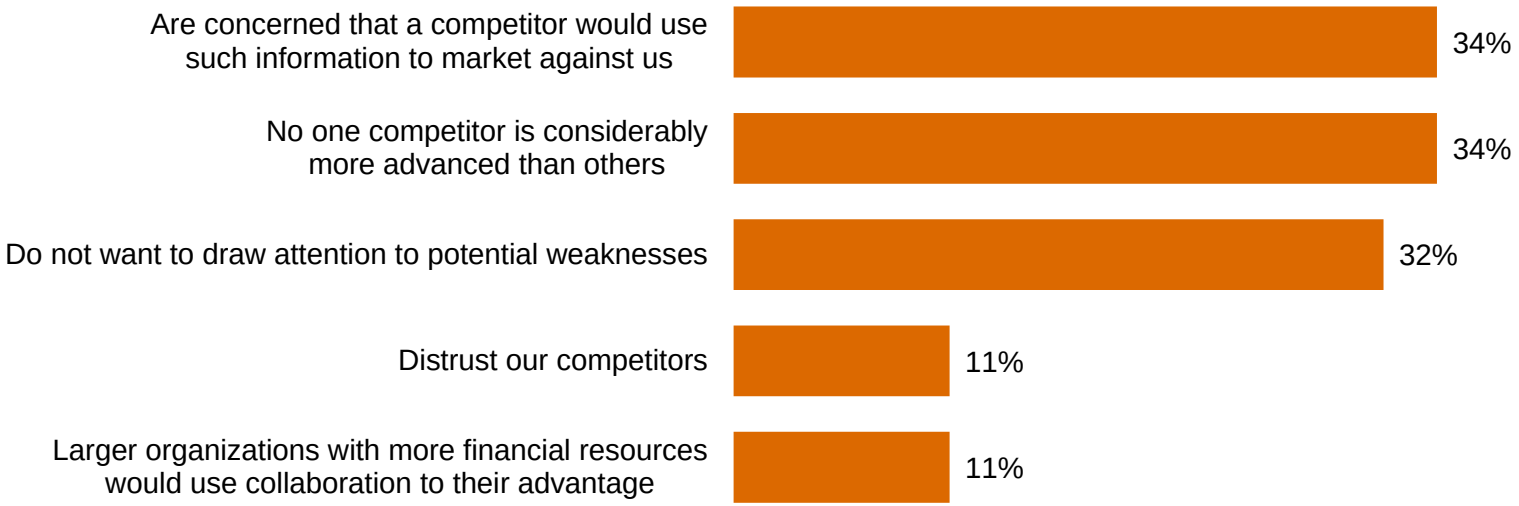


Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

38% of O&G respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.[1]

Reasons for not collaborating on information security



[1]PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

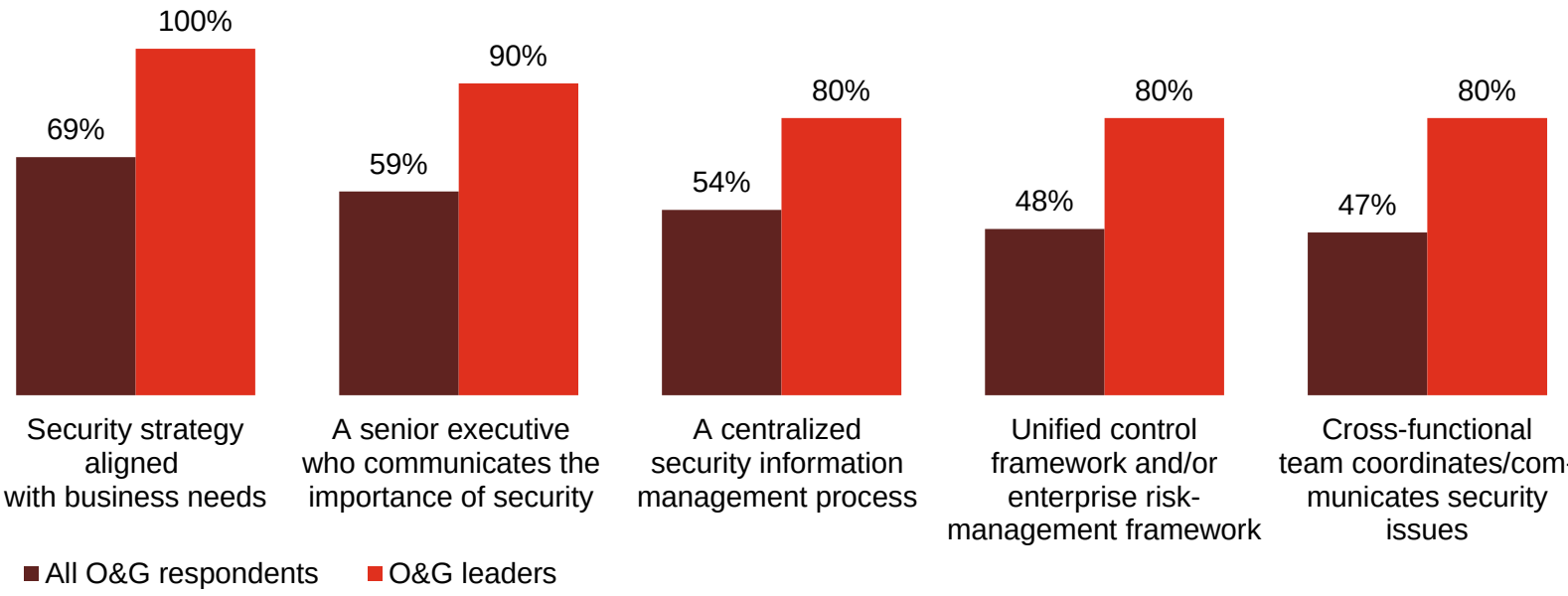
Section 5

Preparing for the threats of tomorrow

O&G leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT challenge.

Aligning security with business needs, improving communications, and centralizing security processes show leaders, in particular, are rethinking the fundamentals of security.

Security policies and safeguards currently in place: All respondents vs. leaders



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?" (Asked only of O&G respondents) Question 2: "Does your company employ a unified control framework and/or enterprise risk management framework for addressing cyber security risks?"

Many respondents have invested in technology safeguards to secure their ecosystems against today's evolving threats.

O&G leaders are more likely to have implemented these technologies. But given today's elevated threat landscape, *all* organizations should strongly consider implementation of these safeguards.

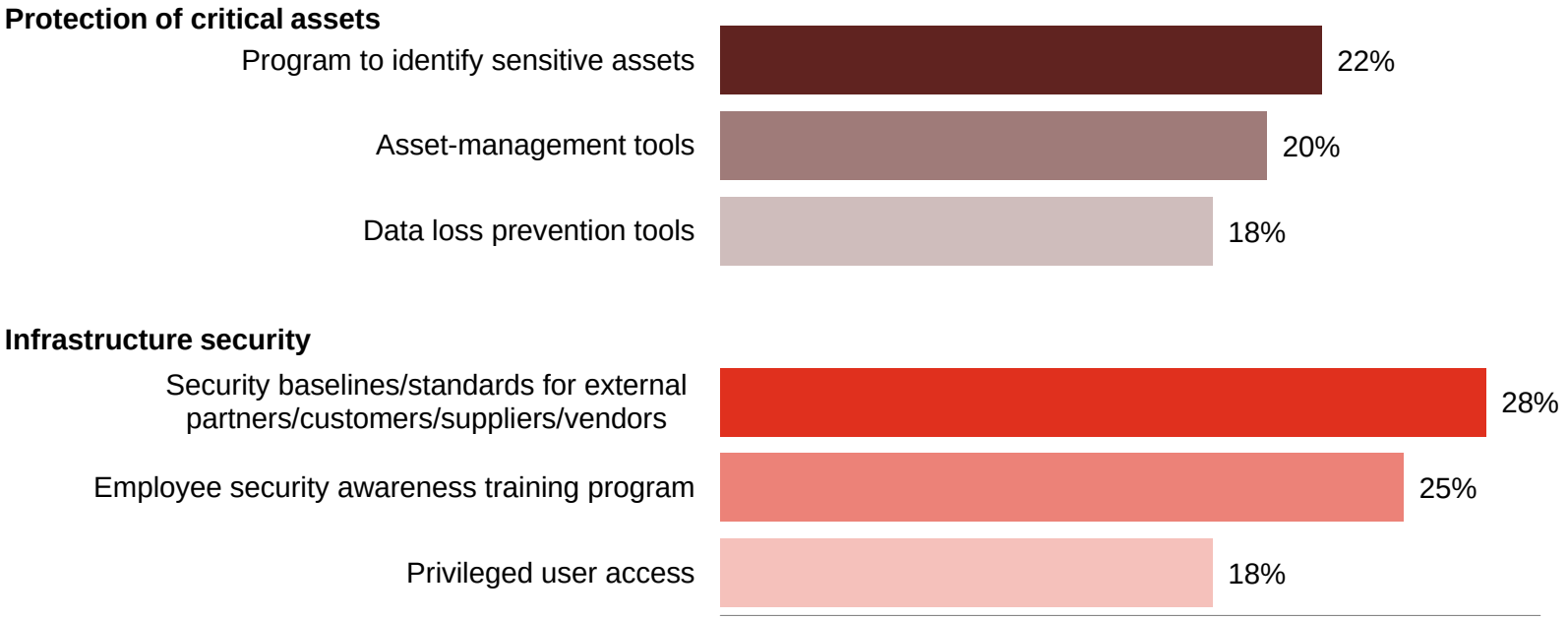
Technology safeguards currently in place	All O&G respondents	O&G leaders
Privileged user access	70%	80%
Malicious code detection tools	66%	80%
Intrusion prevention tools	65%	90%
Vulnerability scanning tools	63%	80%
Patch management tools	59%	80%
Security event correlation tools	56%	70%
Mobile device management	51%	70%
Code analysis tools	49%	70%
Encryption of smartphones	49%	70%

Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

What business imperatives and processes will O&G respondents prioritize this year?

Some of the highest priorities cited by respondents include technologies that can help the organization safeguard its most valuable assets and protect the infrastructure.

Safeguards not in place but a top priority over the next 12 months

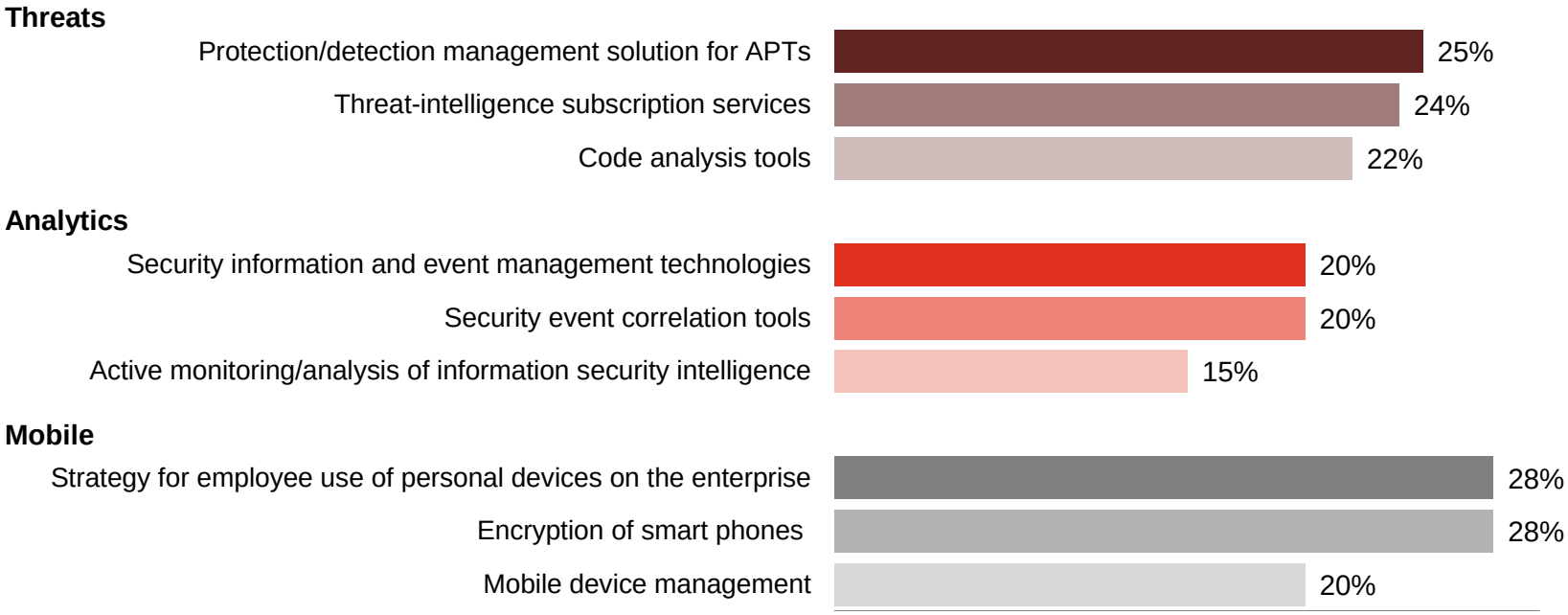


Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?"
Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and O&G companies are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months

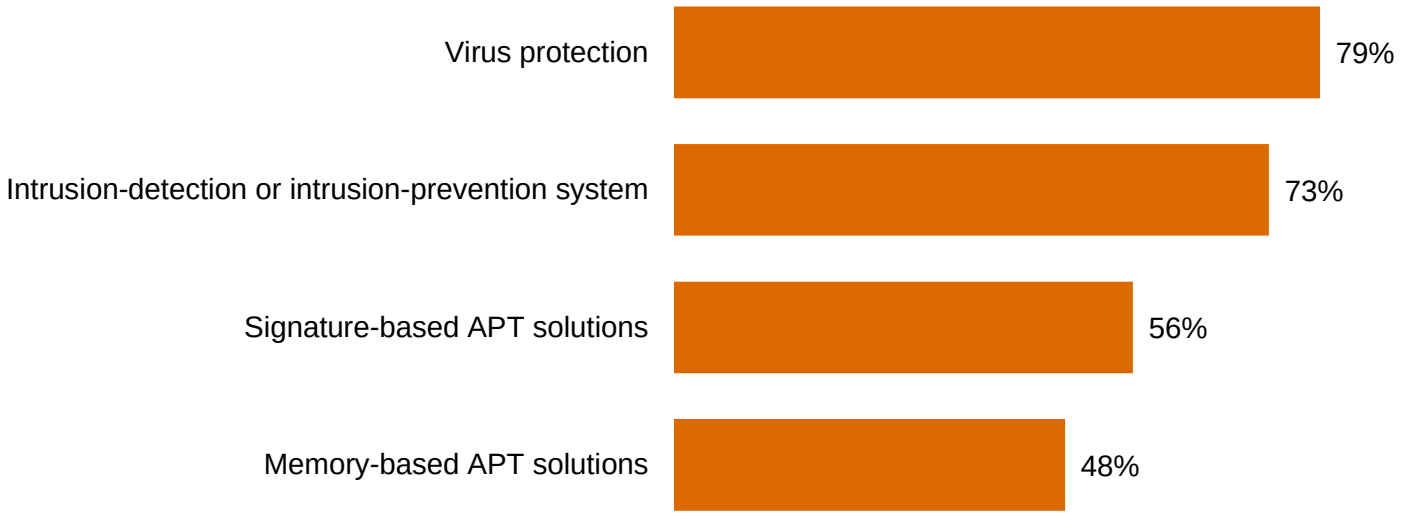


Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?"
Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Many O&G companies are beginning to address the risks of advanced persistent threats.

53% of O&G respondents say they have deployed technologies to prevent APTs, an increase of 13% over last year. Most rely on anti-virus and intrusion detection and prevention tools.

Technologies for protecting against APTs



(Asked only of O&G respondents) Question 3: "Does your company have a program in place to monitor for and respond to advanced persistent threats (APTs)?" Question 3A: "What technologies does your organization employ to protect against APTs?'' (Not all factors shown.)

Effective security demands that O&G companies align policies and spending with business objectives.

A high level of O&G respondents say security policies and spending are aligned with business objectives. This suggests they understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

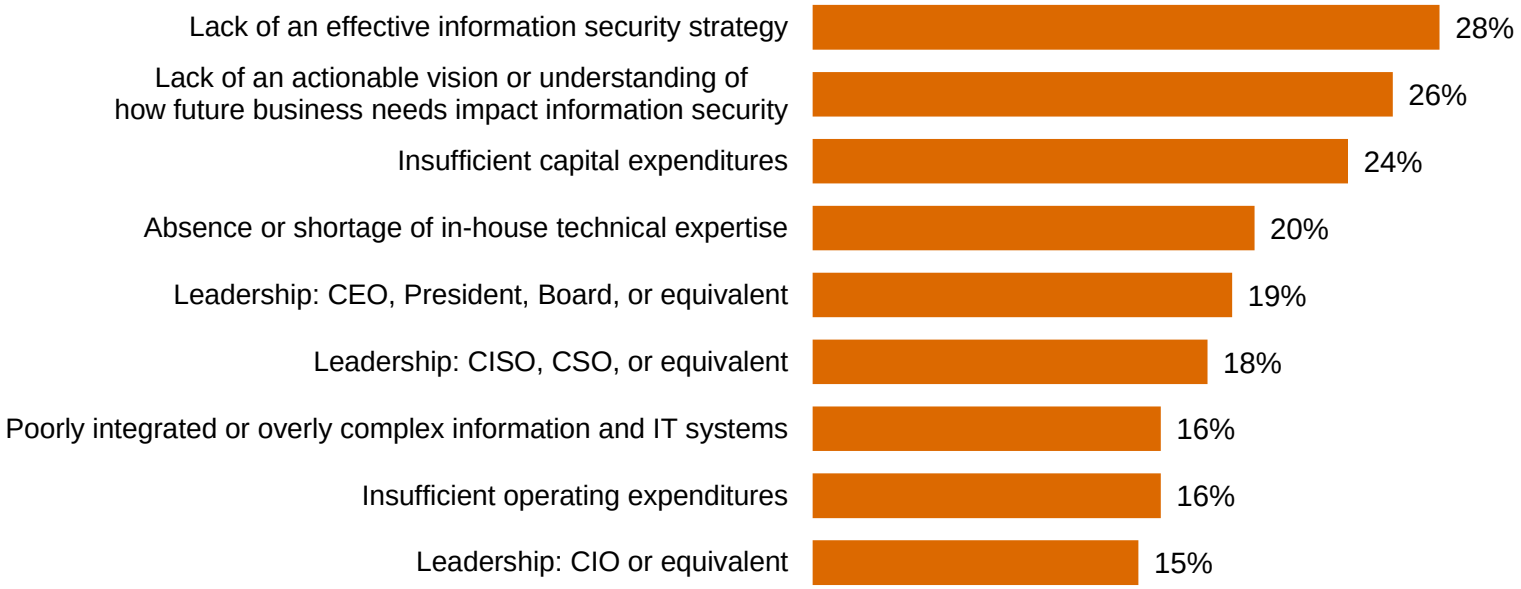
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

An effective strategy, informed vision, and capital funding are needed to advance security.

These are critical because an evolved approach to security requires an understanding of future business needs and an adequate budget. C-level commitment is also key.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
+1 949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
+1 646.471.5731
mark.a.lobel@us.pwc.com

US Oil & Gas Contacts

Brad Bauch
Principal
+1 713.356.4536
brad.bauch@us.pwc.com

Jim Guinn, II
Managing Director
+1 832.656.8242
jim.guinn@us.pwc.com

Jamie Bass
Director
+1 281.788.8263
james.bass@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

PwC

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

Pharmaceuticals

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global pharmaceuticals industry are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising and confidence is high.

But while many pharma companies have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased dramatically, as has the cost of breaches. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few pharma companies have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that pharma companies identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

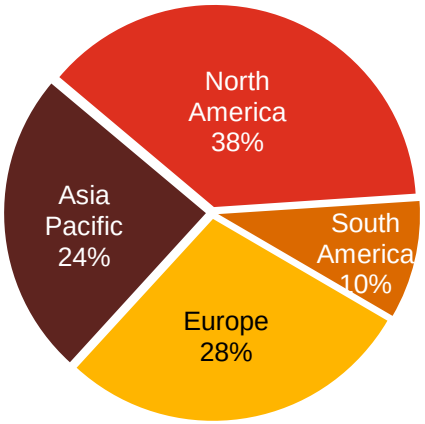
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

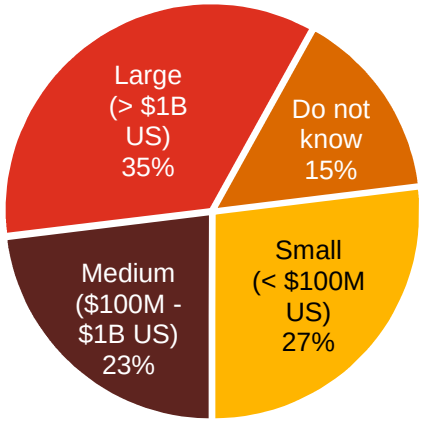
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 74 respondents from the pharmaceuticals industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

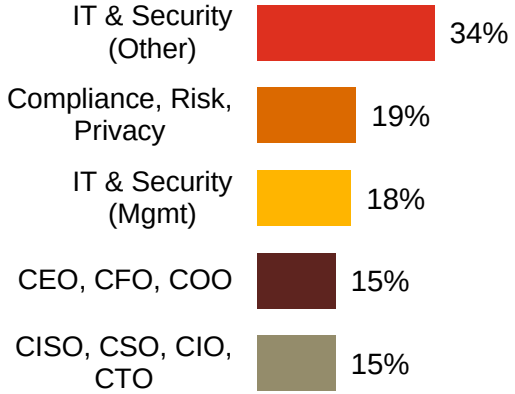
Pharma respondents by region of employment



Pharma respondents by revenue size



Pharma respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

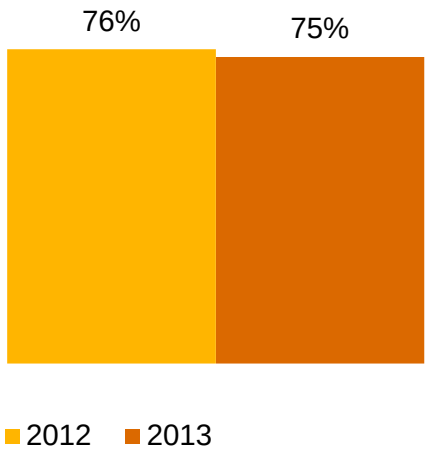
Section 2

Confidence in an era of advancing risks

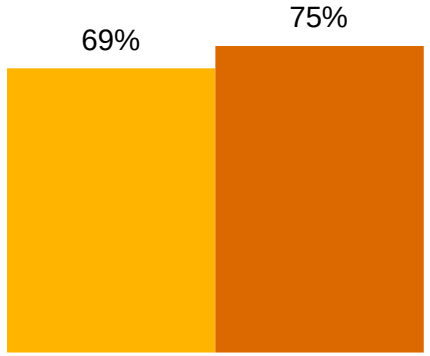
Confidence is high: 75% of pharma respondents believe their security activities are effective.

The same number of respondents also report confidence in their partners' and suppliers' security programs, an increase over last year.

Confidence in effectiveness of security activities (somewhat or very confident)



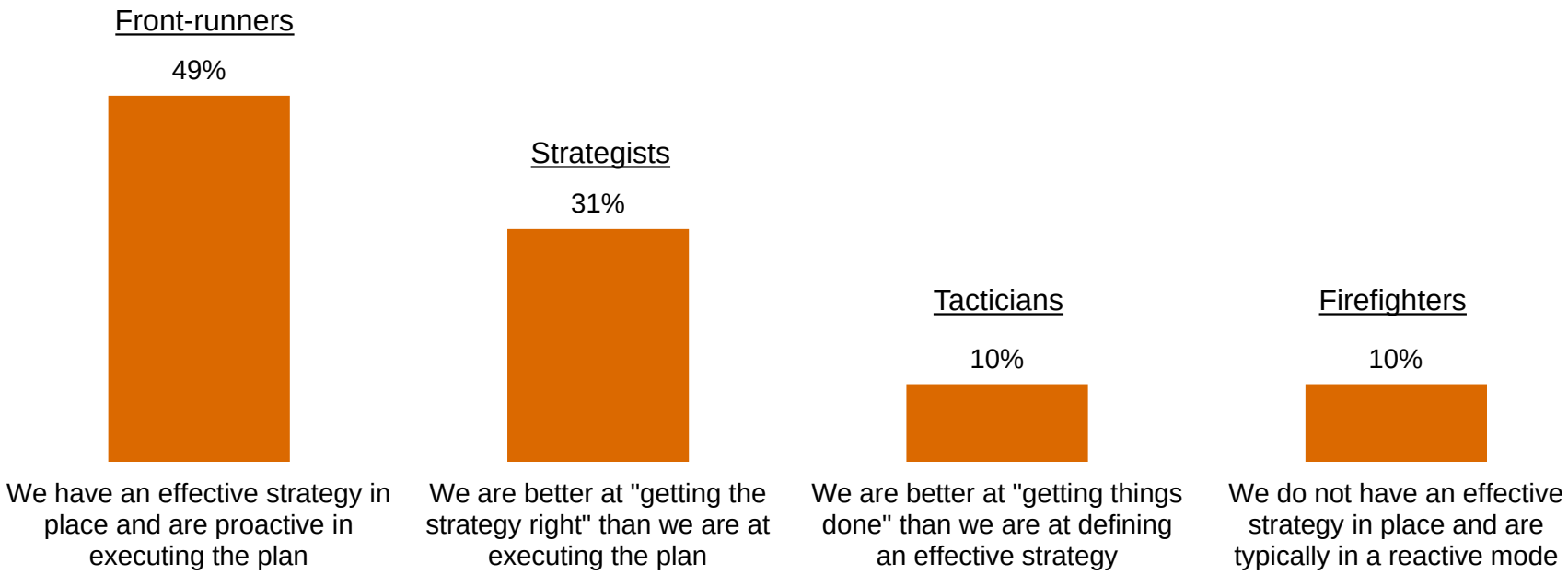
Confidence in effectiveness of partners'/suppliers' security activities



Question 39: "How confident are you that your organization's information security activities are effective?" Question 40: "How confident are you that your partners'/suppliers' information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.")

49% of respondents consider themselves "front-runners," ahead of the pack in security strategy and practices.

Almost half of pharma respondents say they have an effective strategy in place and are proactive in executing the plan, a sign of increasing confidence. About one in three (31%) admit that they are better at getting the strategy right than executing the plan, a sharp increase over last year.



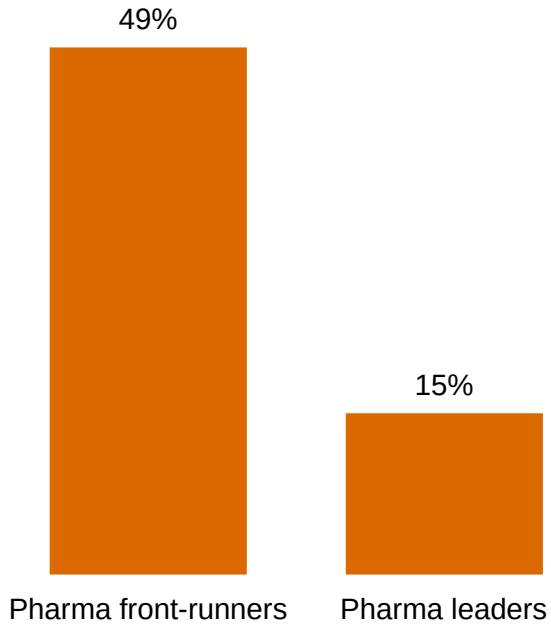
Question 27: "Which statement best characterizes your organization's approach to protecting information security?"

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured pharma respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

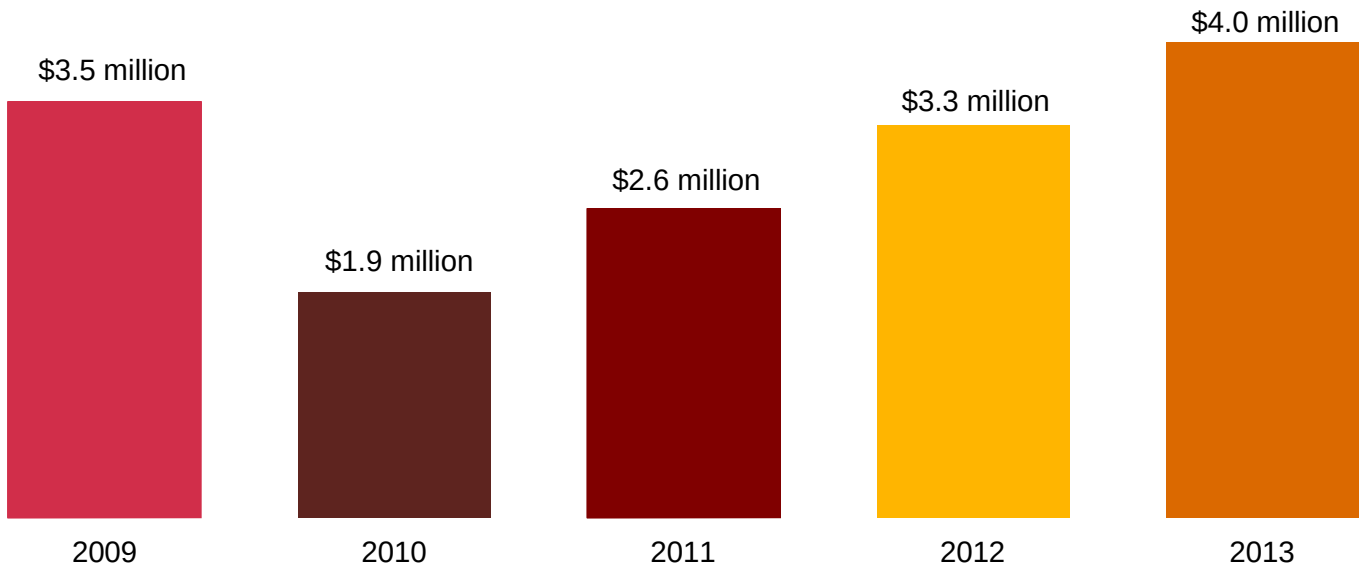


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Pharma information security budgets increase significantly.

Pharma security budgets average $4 million this year, a gain of 19% over 2012. This suggests that organizations understand that today's sophisticated threats demand a substantial boost in security investment.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

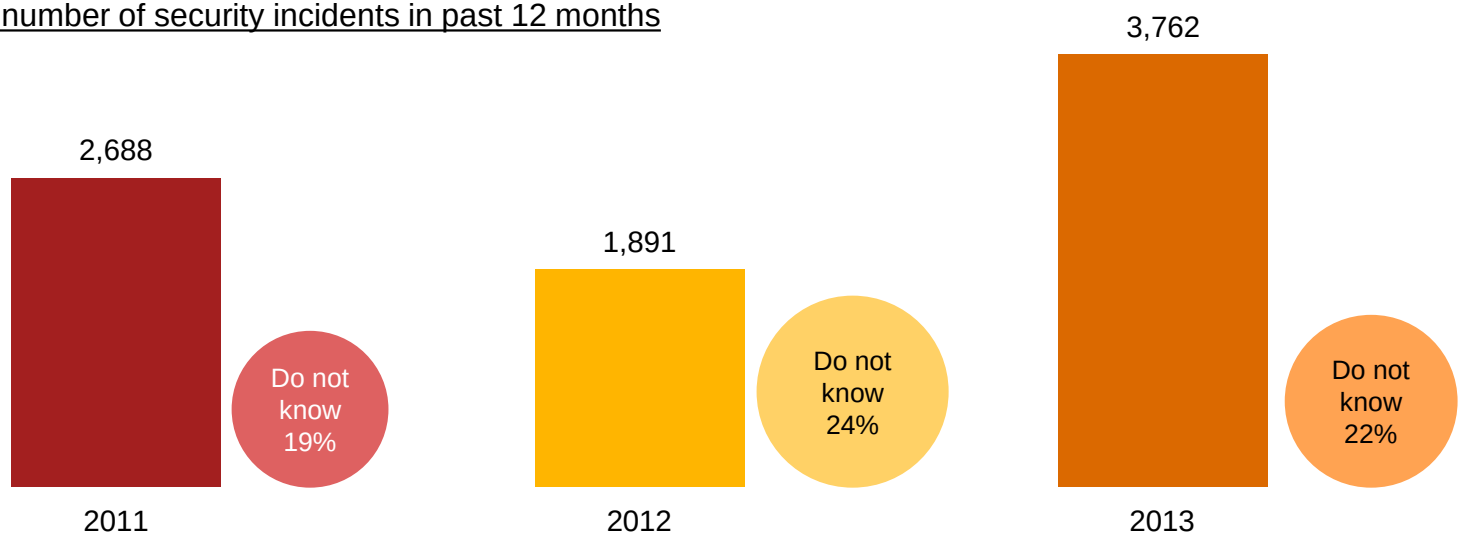
Section 3

Today's incidents, yesterday's strategies

*Pharma companies are detecting more security incidents.**

The number of incidents detected by pharma companies in the past 12 months increased 99% over 2012, perhaps an indication of today's elevated threat environment. Given the cost and complexity of responding to incidents, it's not surprising that financial losses as a result of incidents jumped 49%.

Average number of security incidents in past 12 months



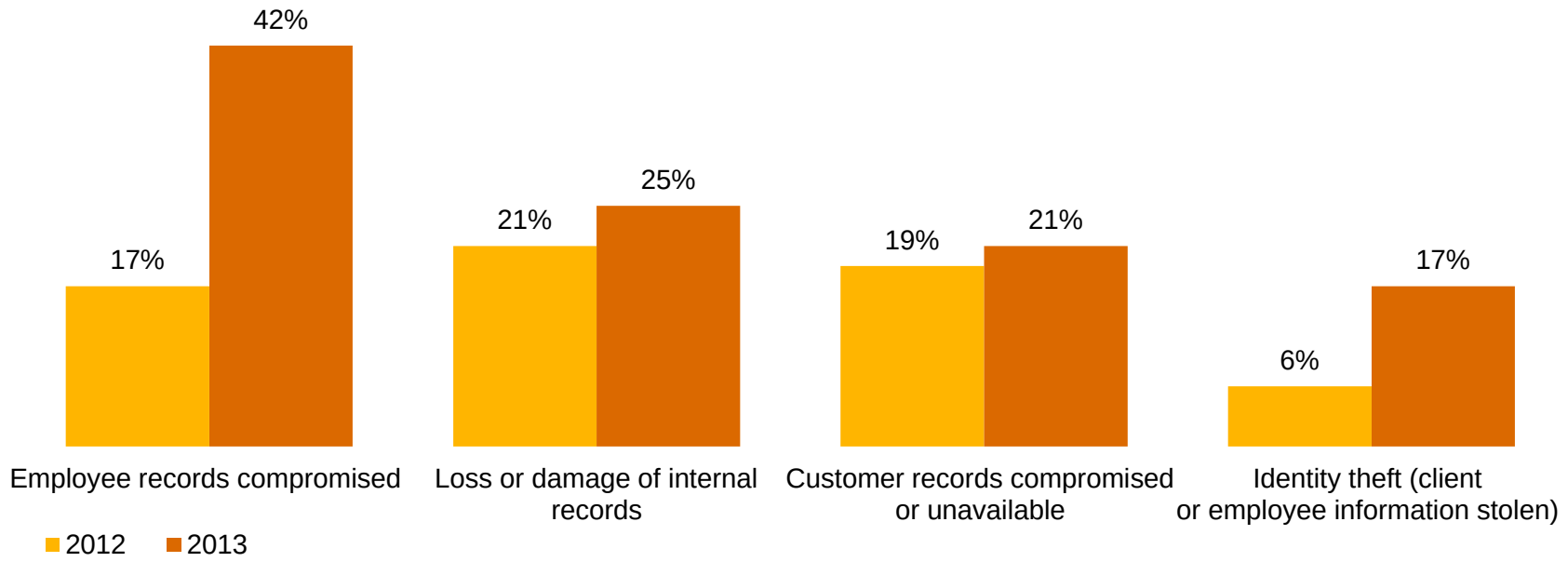
*A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

Pharma companies report an increase in data loss as a result of security incidents.

Compromise of employee records and identity theft are up sharply this year, potentially jeopardizing an organization's most valuable relationships.

Impact of security incidents

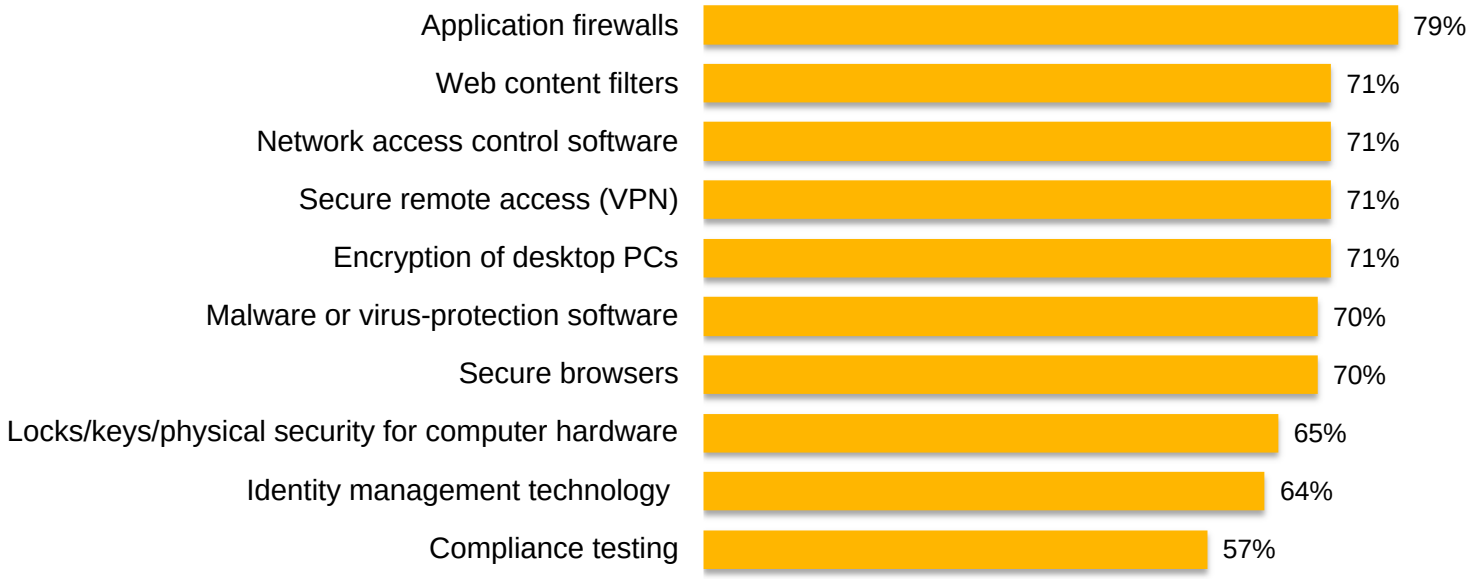


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

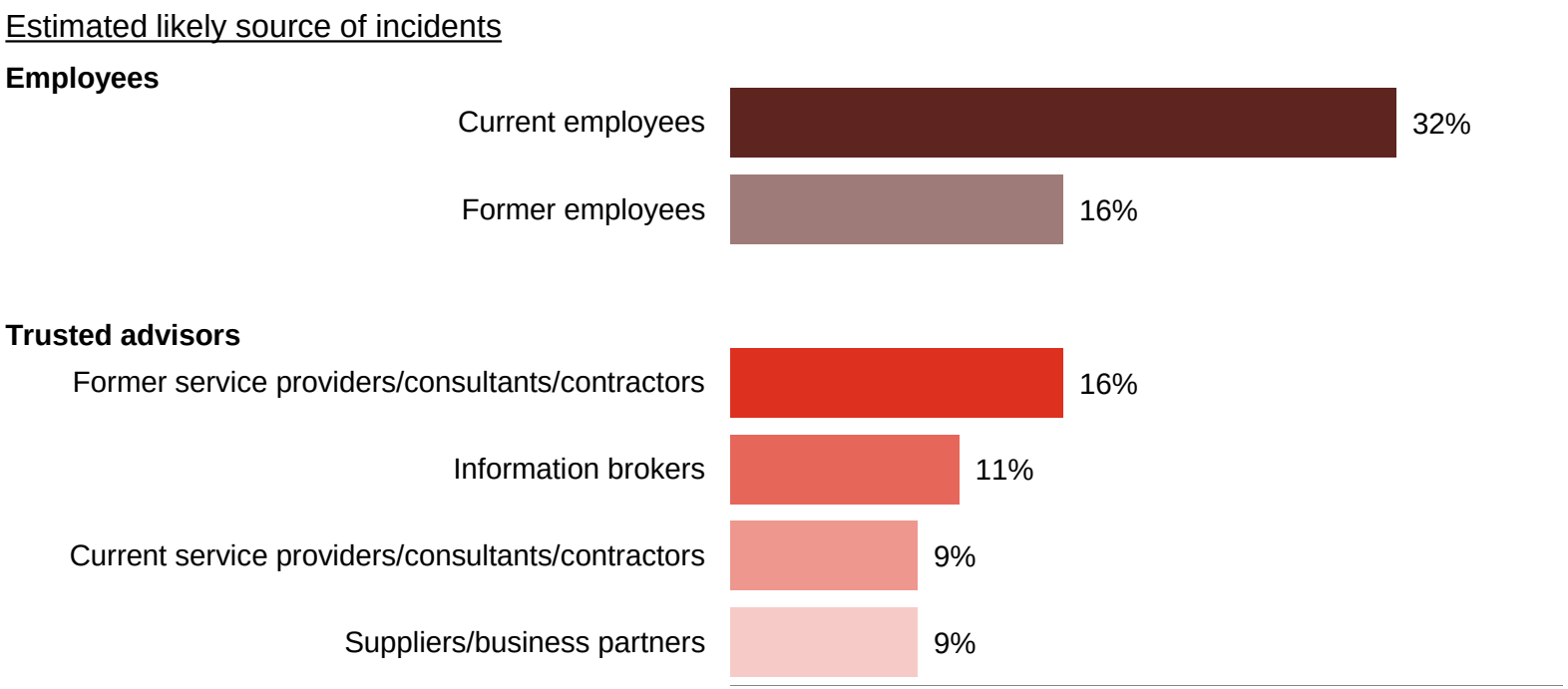
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most Pharma respondents.

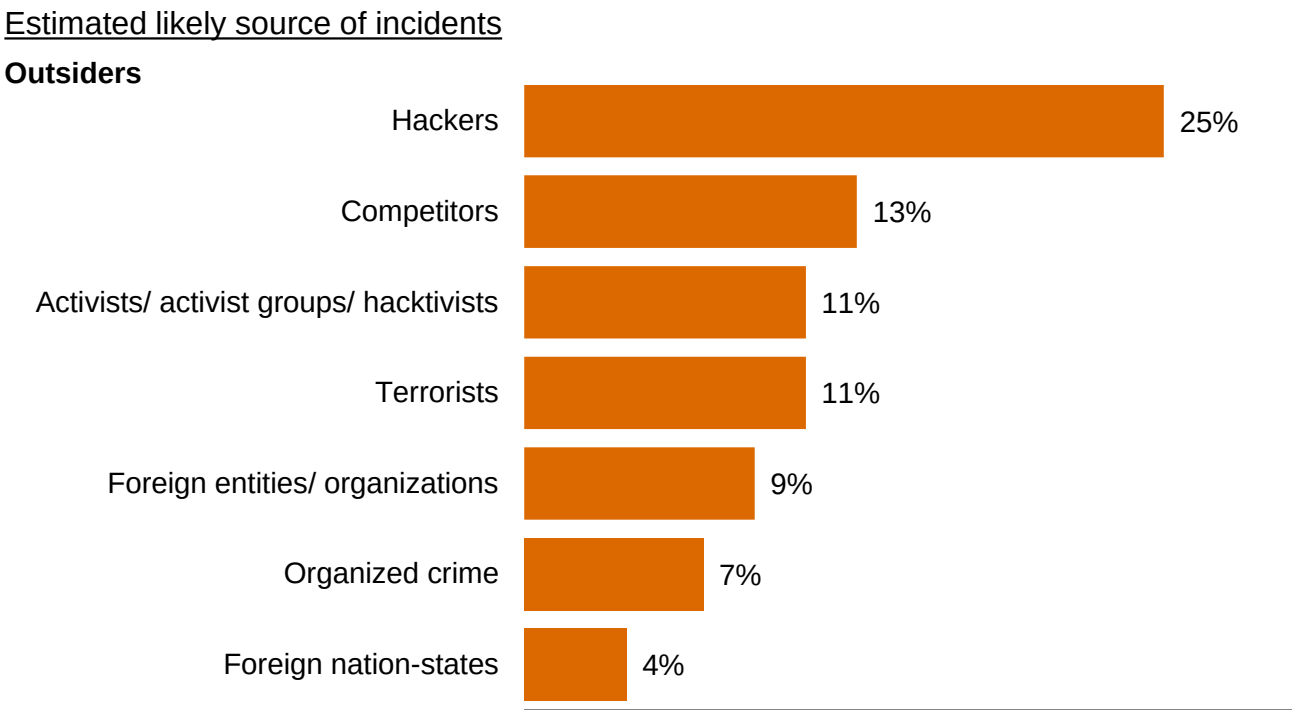
It's the people you know—current and former employees, as well as former service providers and contractors—who are most likely to perpetrate security incidents.



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, pharma firms are more likely to be hit by other outsiders.

Only 4% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a more likely danger.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

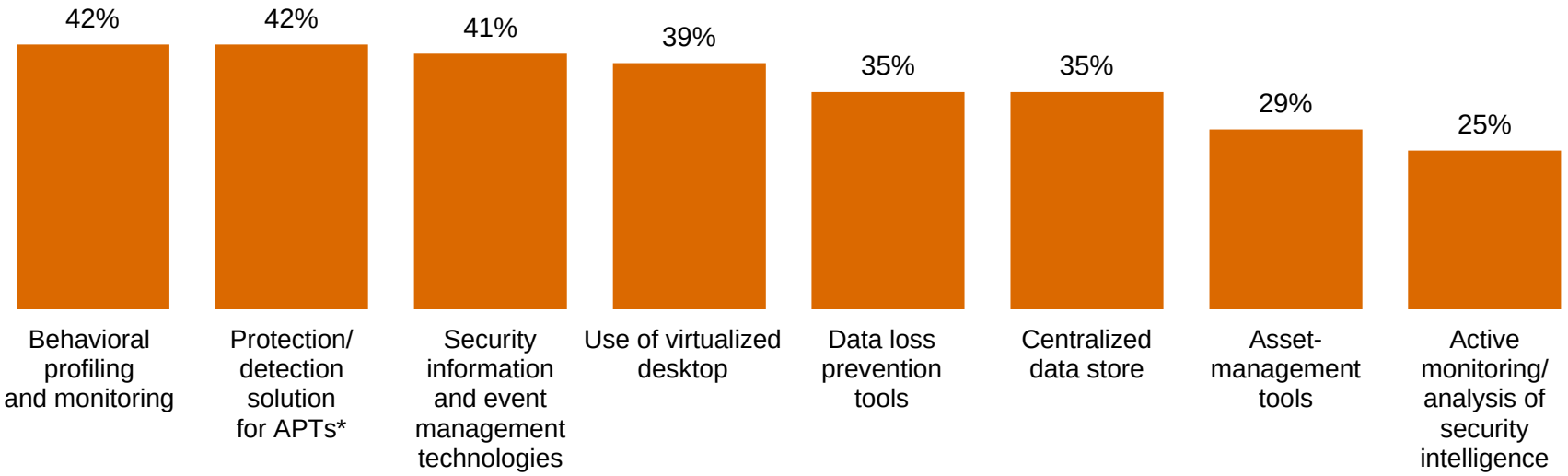
Section 4

A weak defense against adversaries

Many pharma companies have not implemented technologies that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place



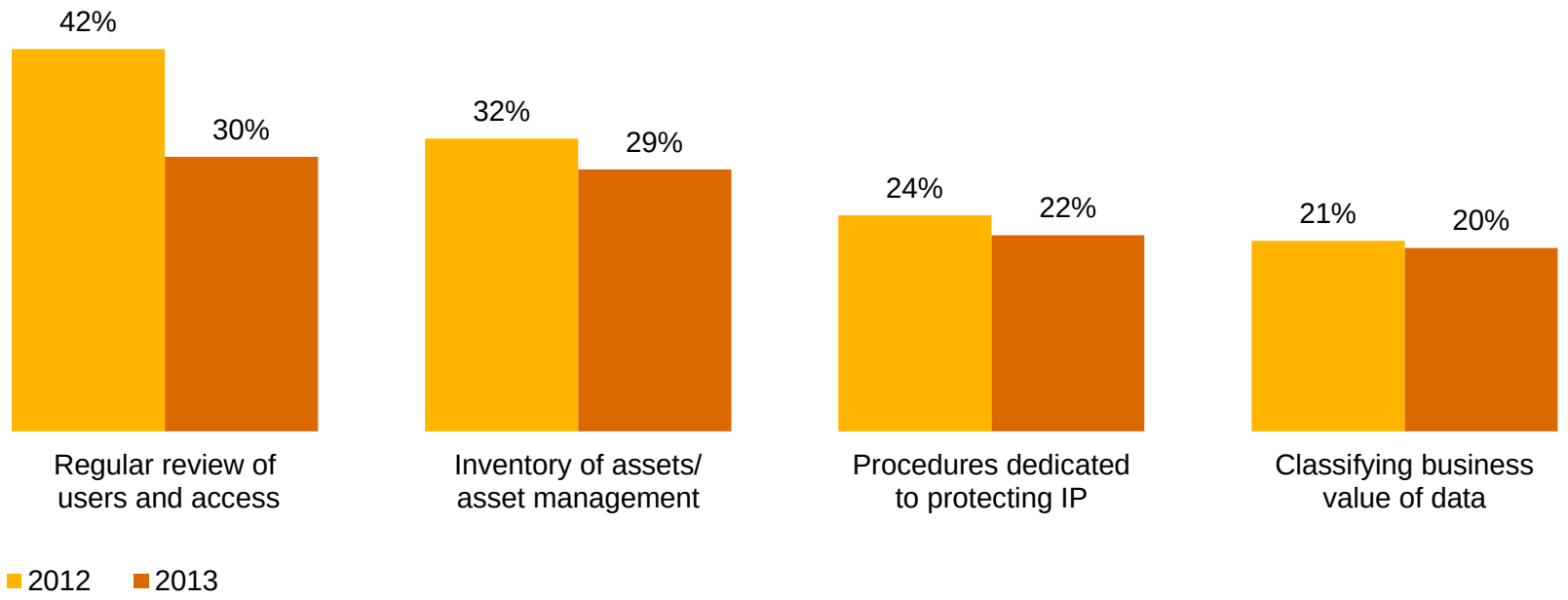
*Advanced persistent threats (APTs)

Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite potential consequences, many pharma companies do not adequately safeguard their high-value information.

It is imperative that companies identify, prioritize, and protect their "crown jewels." But pharma respondents report a decline in implementation of basic policies to safeguard intellectual property (IP).

Have policies to help safeguard IP and trade secrets

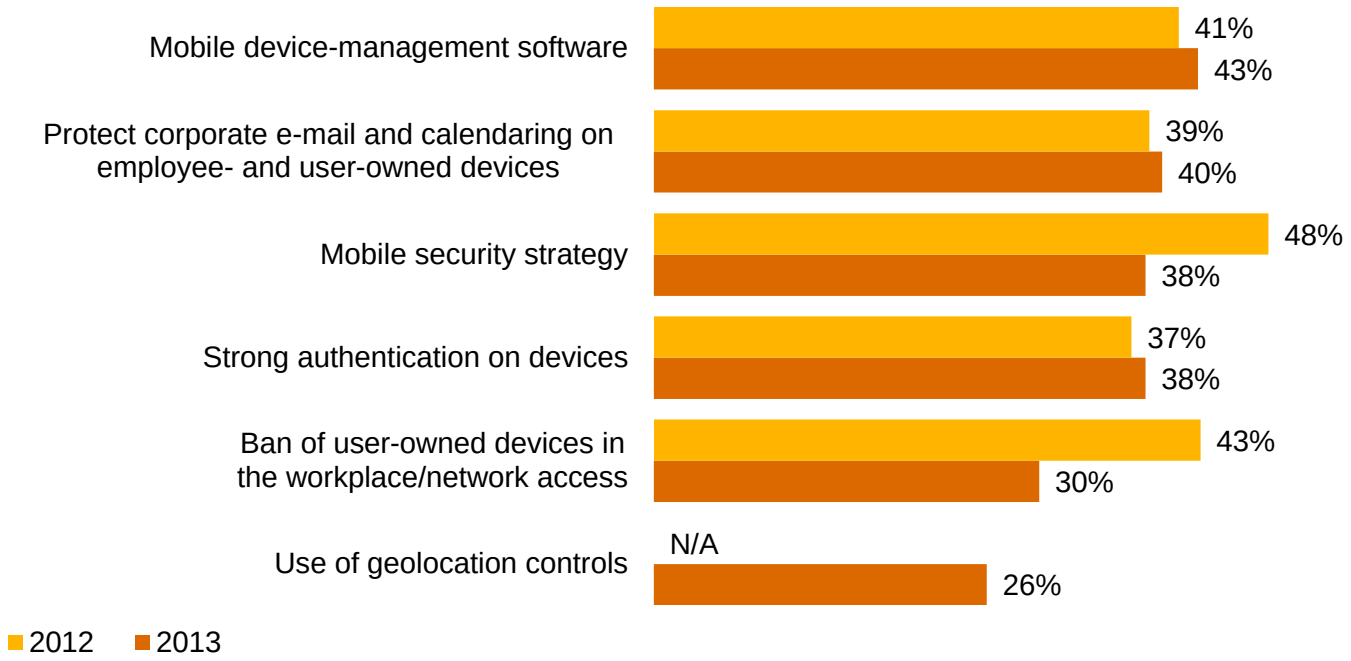


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet pharma companies' efforts to implement mobile security programs do not show significant gains over last year, and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

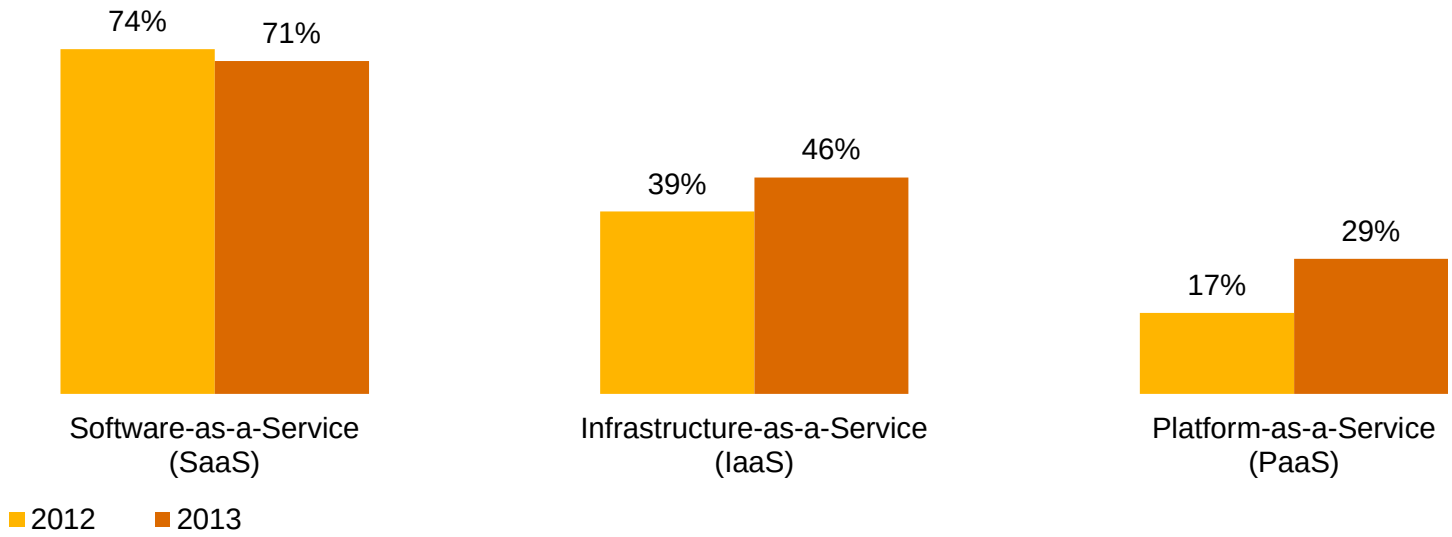


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

42% of pharma companies use cloud computing, but they often do not include cloud in their security policies.

Among pharma companies that use cloud computing, 57% say security has improved—but only 16% include provisions for cloud in their security policy. SaaS is the most widely adopted cloud service, but PaaS shows solid growth.

Type of cloud service used

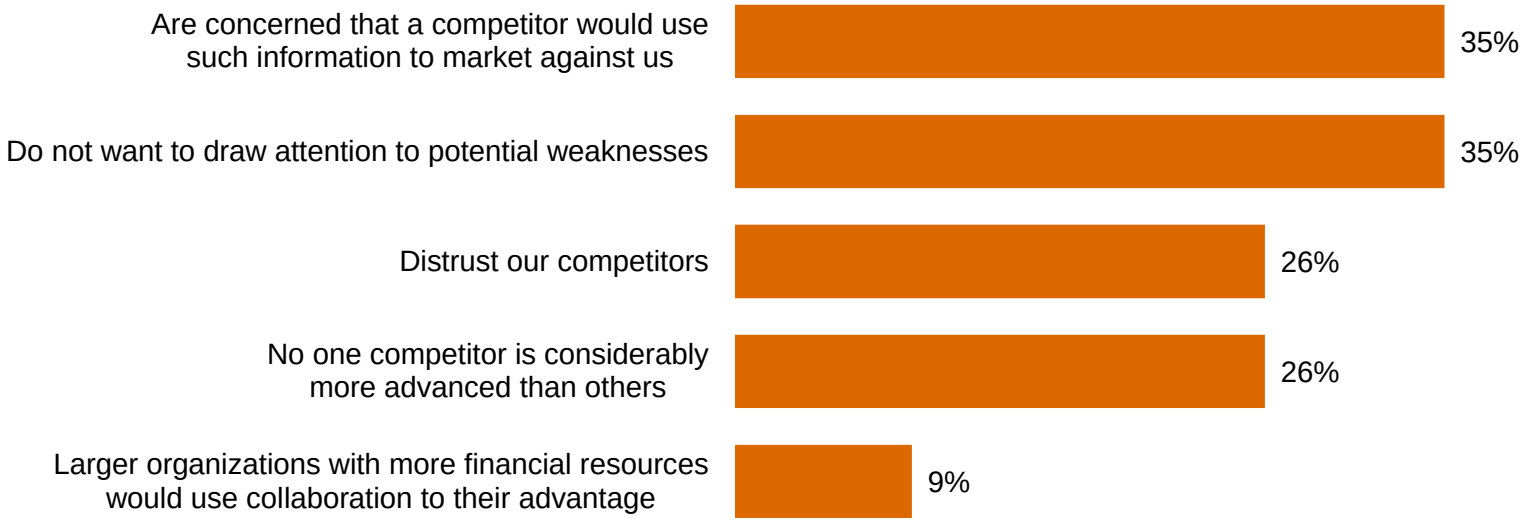


Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

34% of respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.[1]

Reasons for not collaborating on information security



[1] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

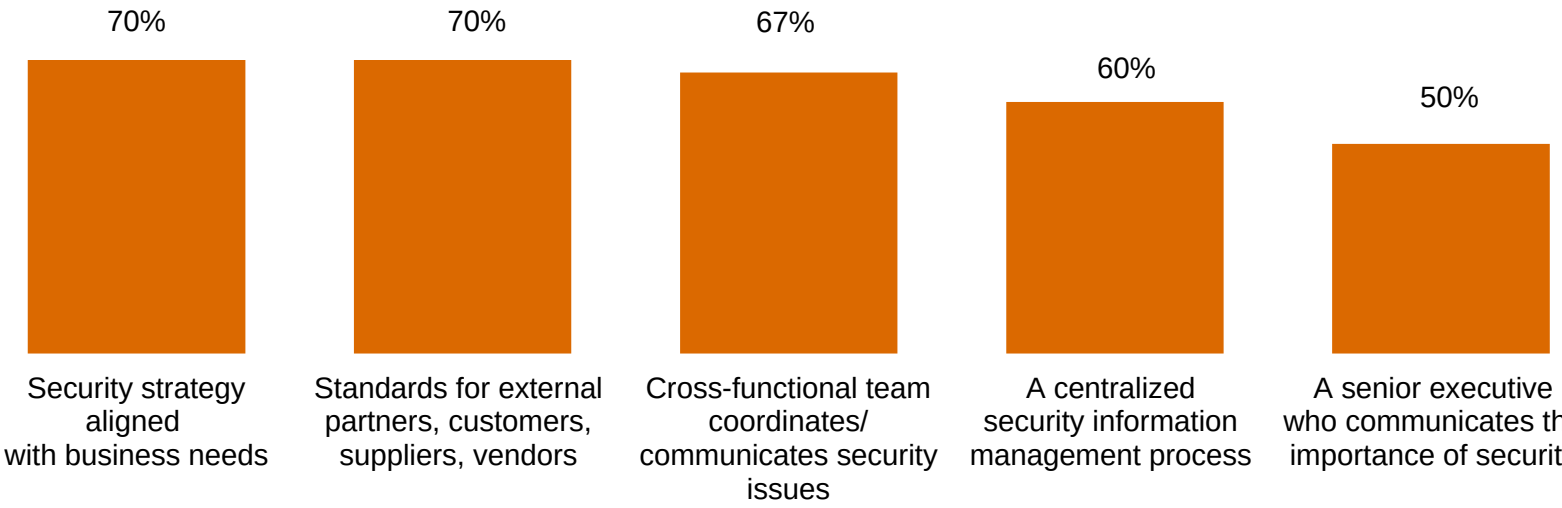
Section 5

Preparing for the threats of tomorrow

Pharma respondents are enhancing capabilities in ways that show security is a business imperative—not an IT challenge.

Aligning security with business needs, setting standards for external partners, and improving communications show pharma respondents are rethinking the fundamentals of security.

Security policies and safeguards currently in place

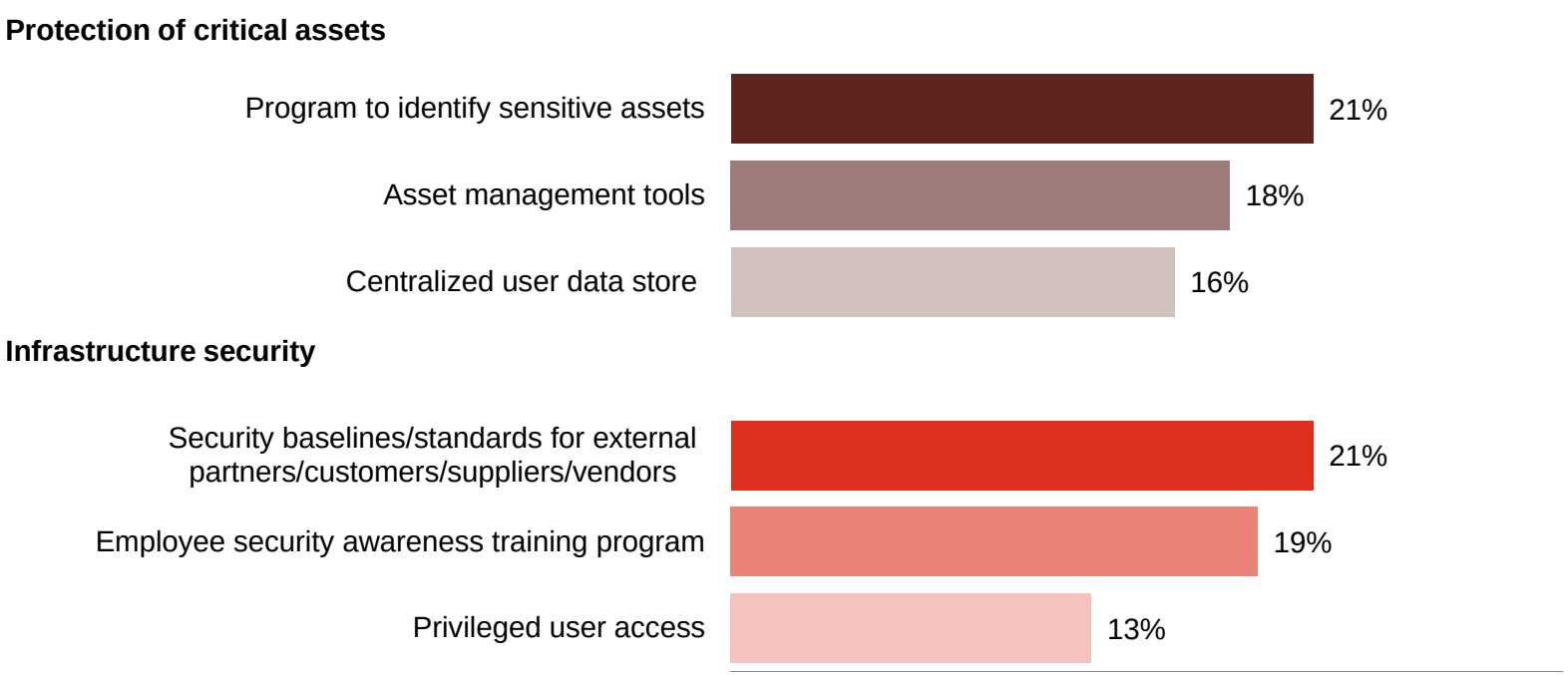


Question 14: “What process information security safeguards does your organization currently have in place?” (Not all factors shown.) Question 29: “Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?”

What business imperatives and processes will pharma companies prioritize this year?

Some of the highest priorities cited by respondents include technologies that can help the organization protect its most valuable assets and protect the infrastructure.

Safeguards not in place but a top priority over the next 12 months

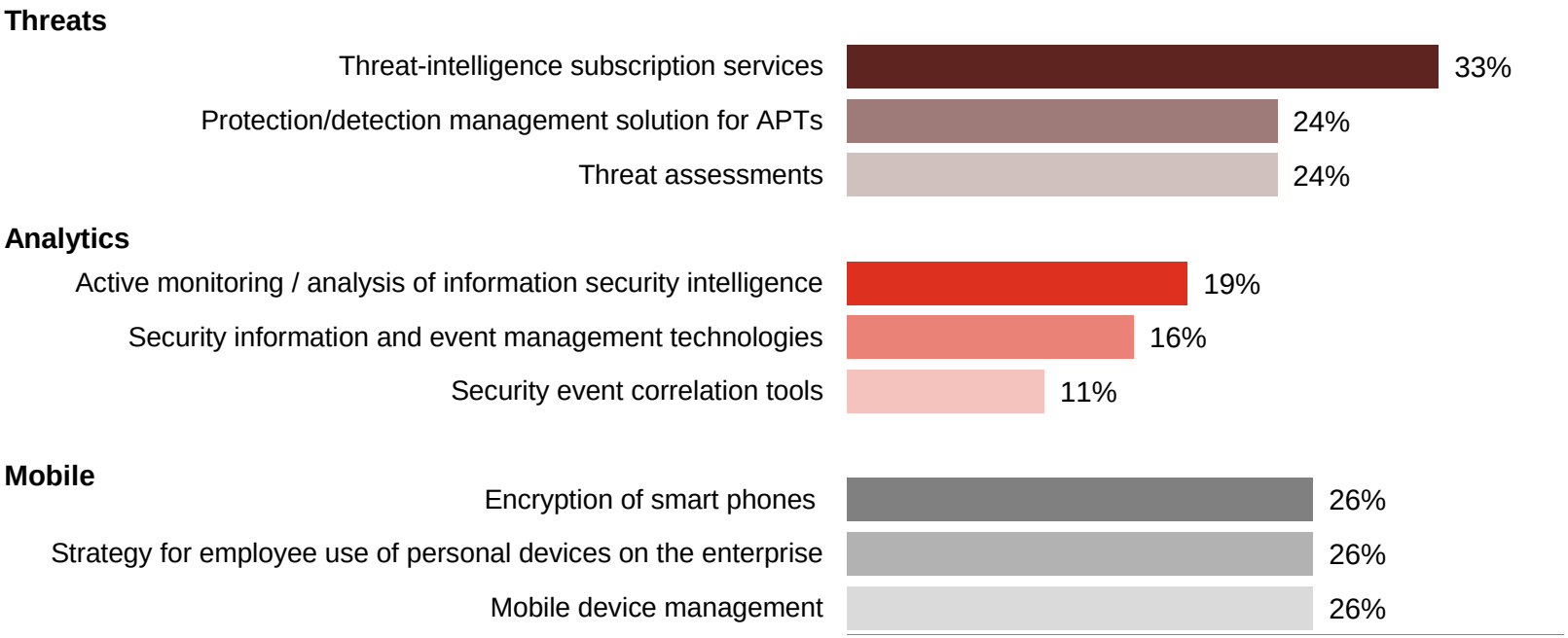


Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?"
Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and pharma companies are prioritizing technologies that can help better understand threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Effective security demands that pharma companies align security policies and spending with business objectives.

Compared with last year, fewer respondents say security policies and spending are aligned with business objectives. It is important to understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

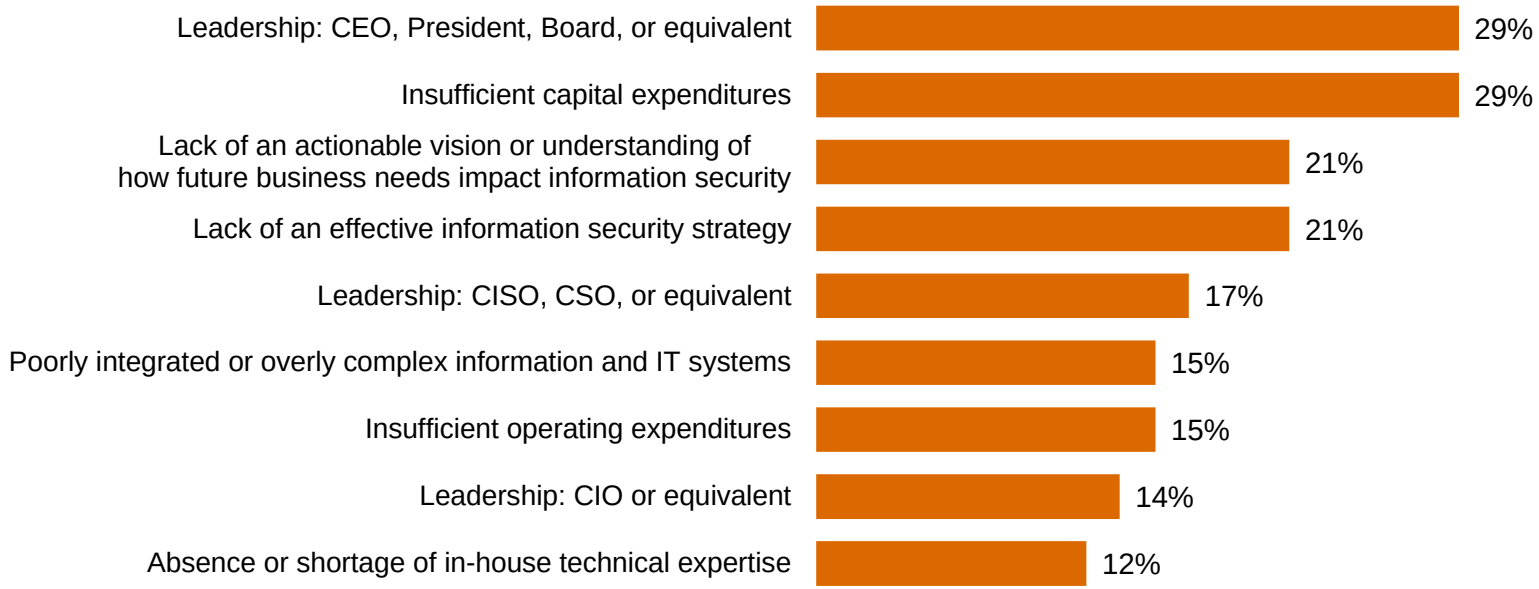
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

Committed leadership and more money are needed to advance security.

This is critical because an evolved approach to security requires the support of top executives and an adequate budget that is aligned with business needs.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

US Pharmaceuticals Contacts

Daniel Garrett
Principal
267.330.8202
daniel.garrett@us.pwc.com

Peter Harries
Principal
602.750.3404
peter.harries@us.pwc.com

Mick Coady
Principal
713.356.4366
mick.coady@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

Power & Utilities

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents evolve in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global utilities industry are heeding the need to fund enhanced security activities and have improved technology safeguards, processes, and strategies. Budgets are rising, confidence is high, and detected breaches are down.

But while many utilities organizations have raised the bar on security, their adversaries have done better.

Threats are constantly multiplying and evolving. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many utilities executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few utilities organizations have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that utilities organizations identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the organizational strategy, one that is championed by the CEO and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

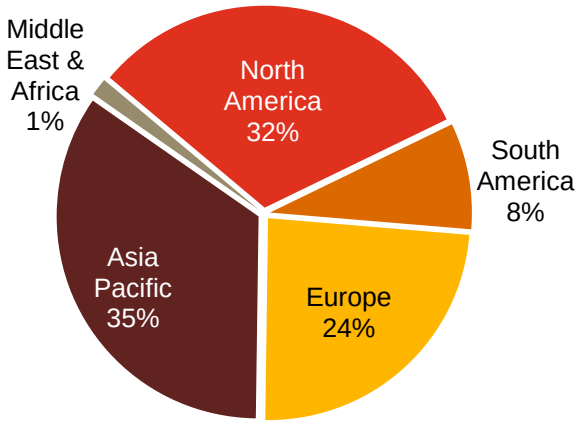
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

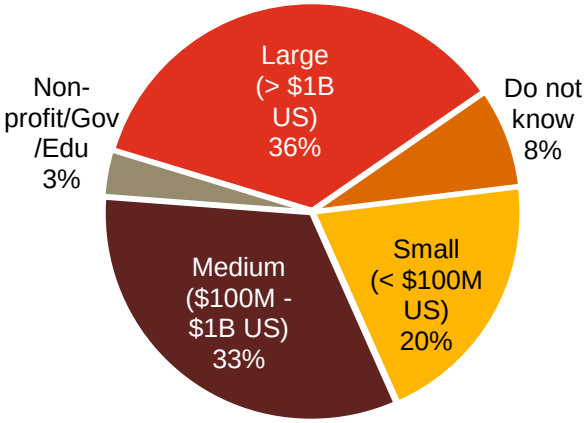
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 143 respondents from the utilities industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

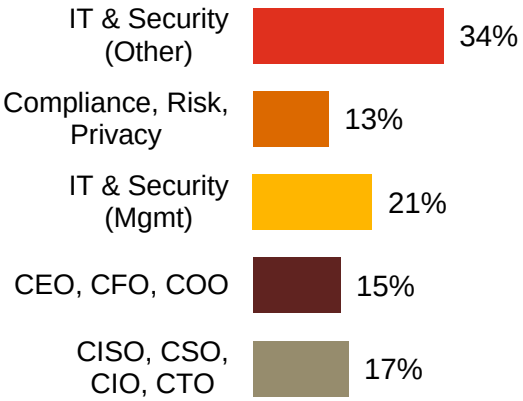
Utilities respondents by region of employment



Utilities respondents by company revenue size



Utilities respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

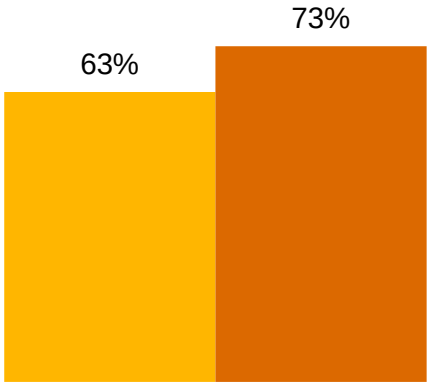
Confidence in an era of advancing risks

Confidence is high: 73% of utilities respondents believe their security activities are effective.

The same number say their partners and suppliers have effective security programs, an increase of 16% over last year.

Confidence in effectiveness of security activities

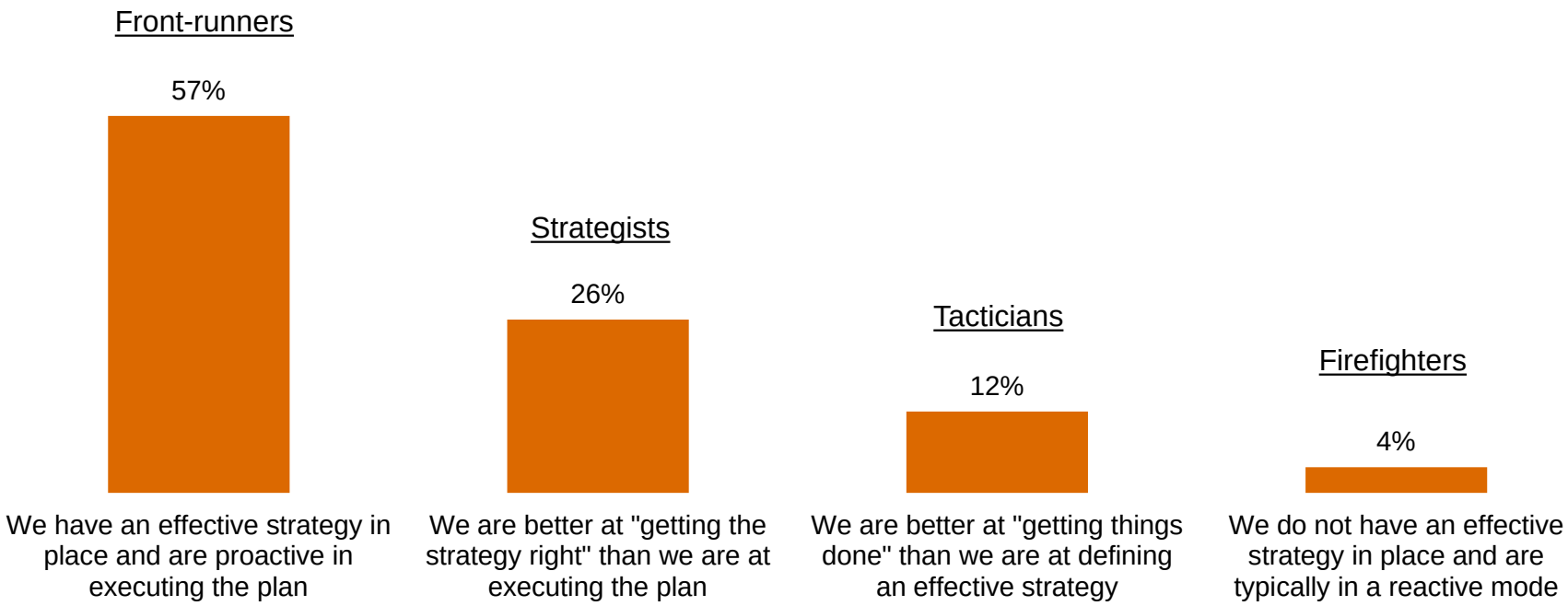
Confidence in effectiveness of partners'/suppliers' security activities



Question 39: "How confident are you that your organization's information security activities are effective?" Question 40: "How confident are you that your partners'/suppliers' information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.")

57% of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

The number of utilities respondents reporting that they have an effective strategy in place and are proactive in executing the plan increased 51% over last year, indicating growing confidence.



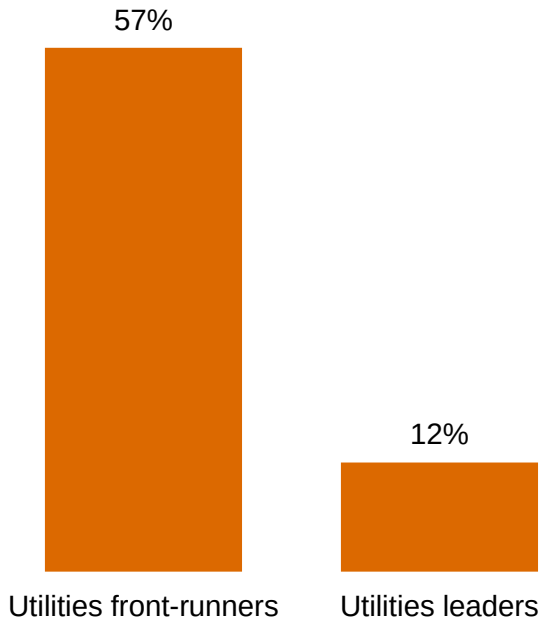
Question 27: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding.)

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured utilities respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

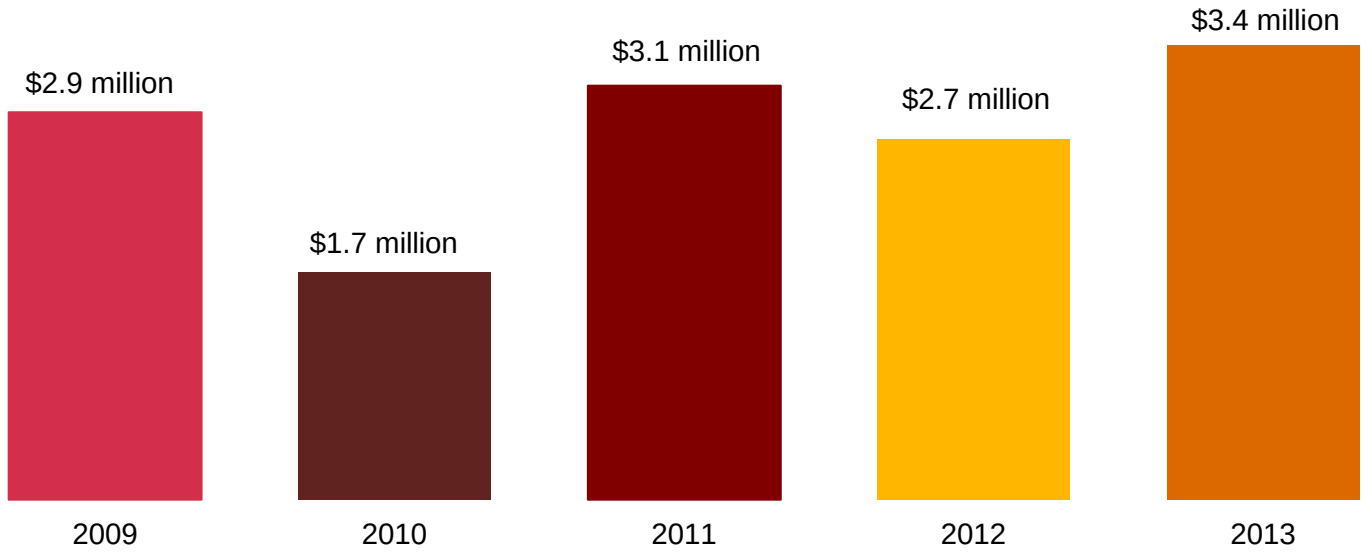


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Utilities information security budgets increase significantly.

Security budgets average $3.4 million this year, an increase of 25% over 2012. This boost suggests that utilities companies understand that today's elevated threat landscape demands a greater investment in security.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

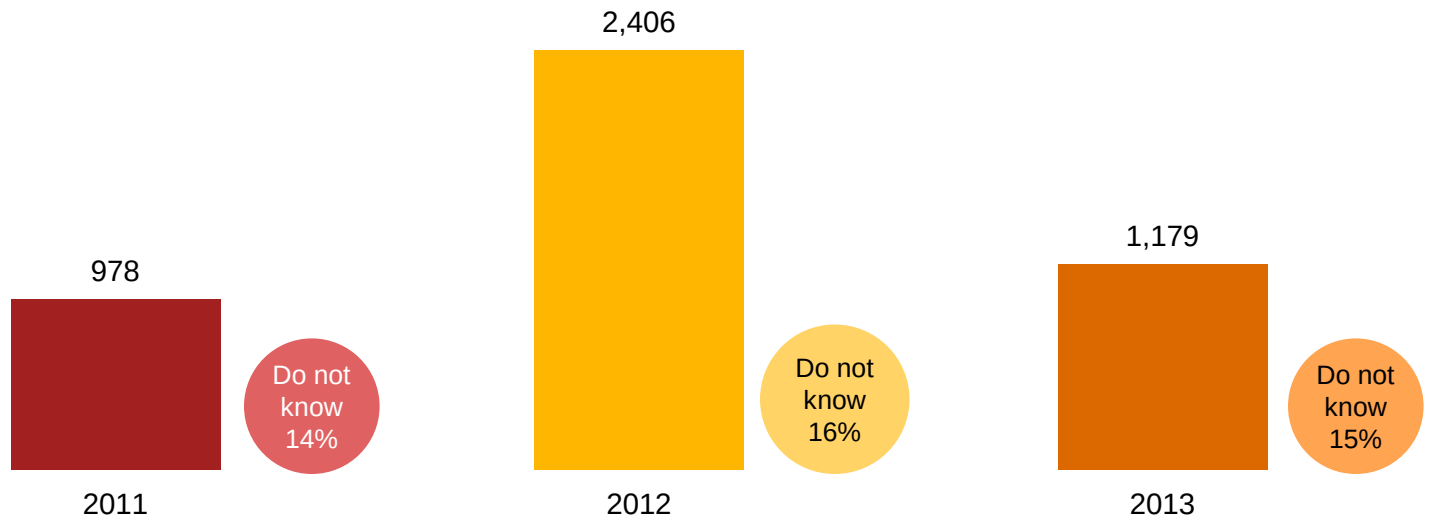
Section 3

Today's incidents, yesterday's strategies

*Utilities respondents detect fewer security incidents.**

After a spike in 2012, the number of security incidents detected dropped 51% over last year, perhaps an indication of the industry's implementation of sophisticated safeguards.

Average number of security incidents in past 12 months



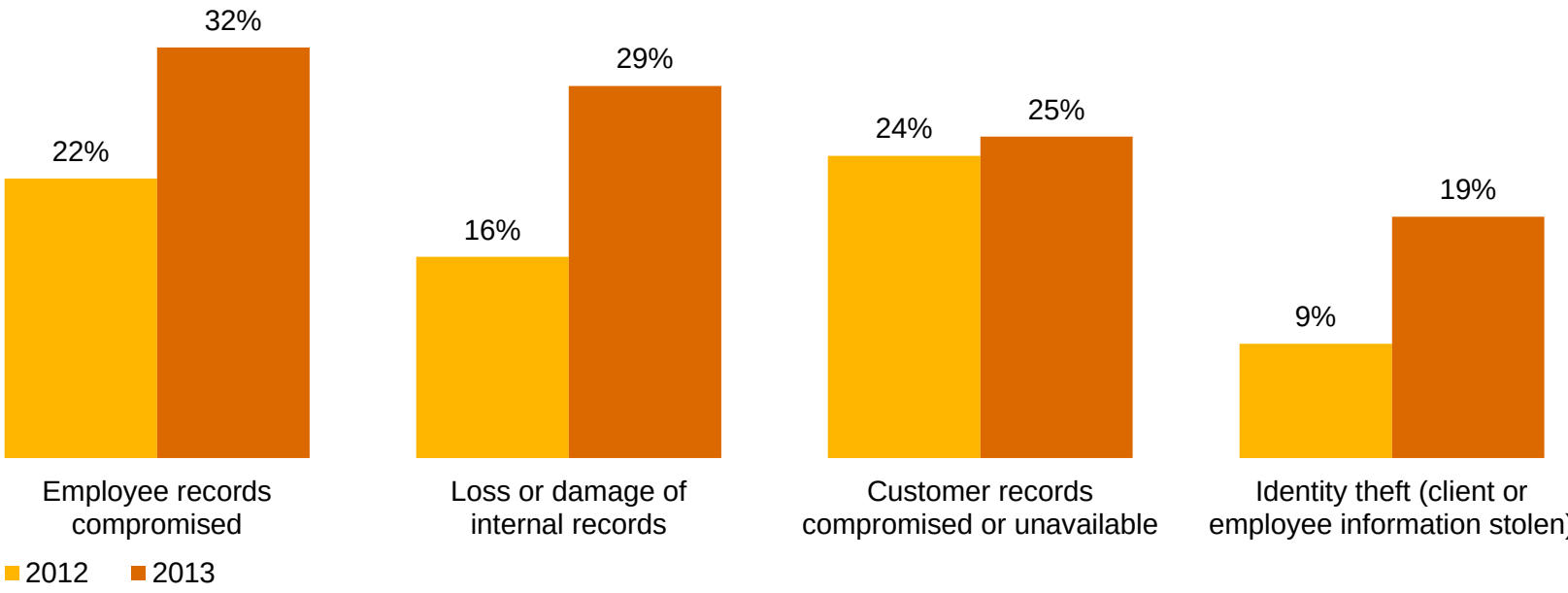
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months?

Utilities respondents report an increase in data loss as a result of security incidents.

Compromise of employee records is up sharply this year, potentially jeopardizing a utilities company's most valuable relationships. Also significant: Identity theft more than doubled over last year.

Impact of security incidents

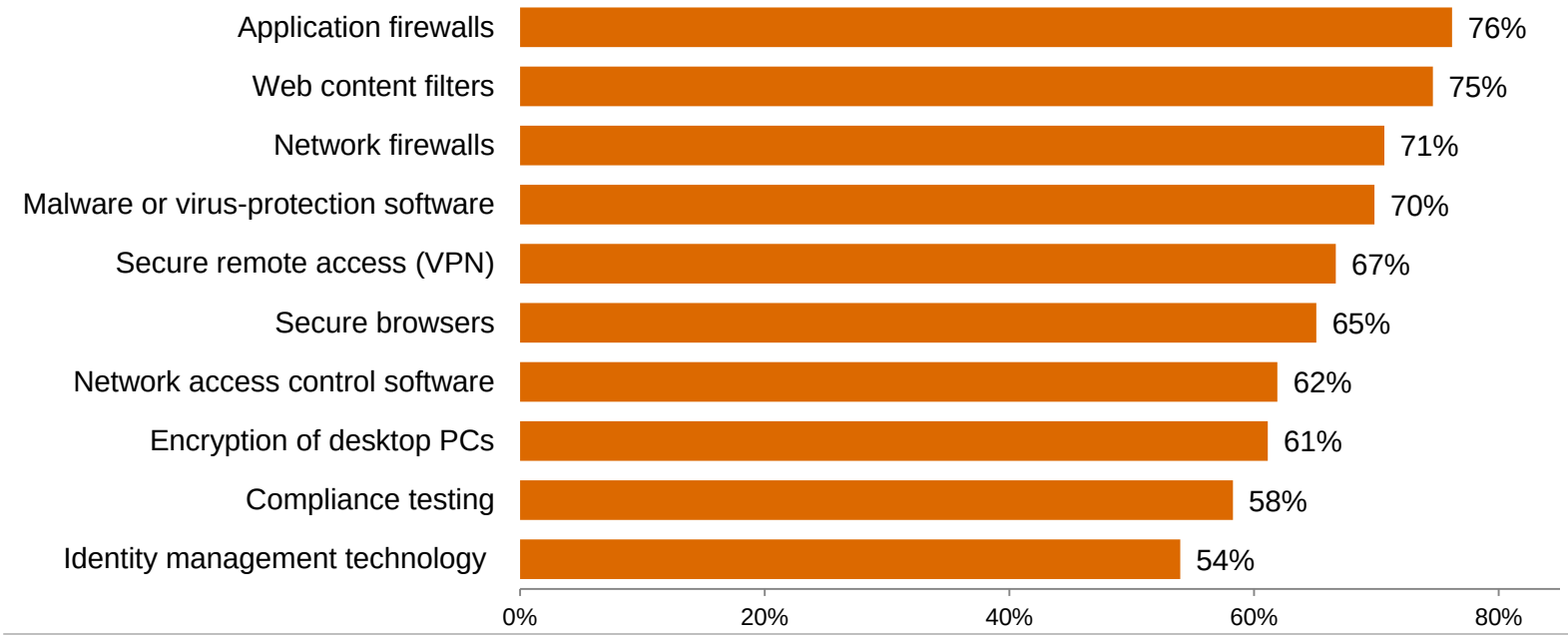


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

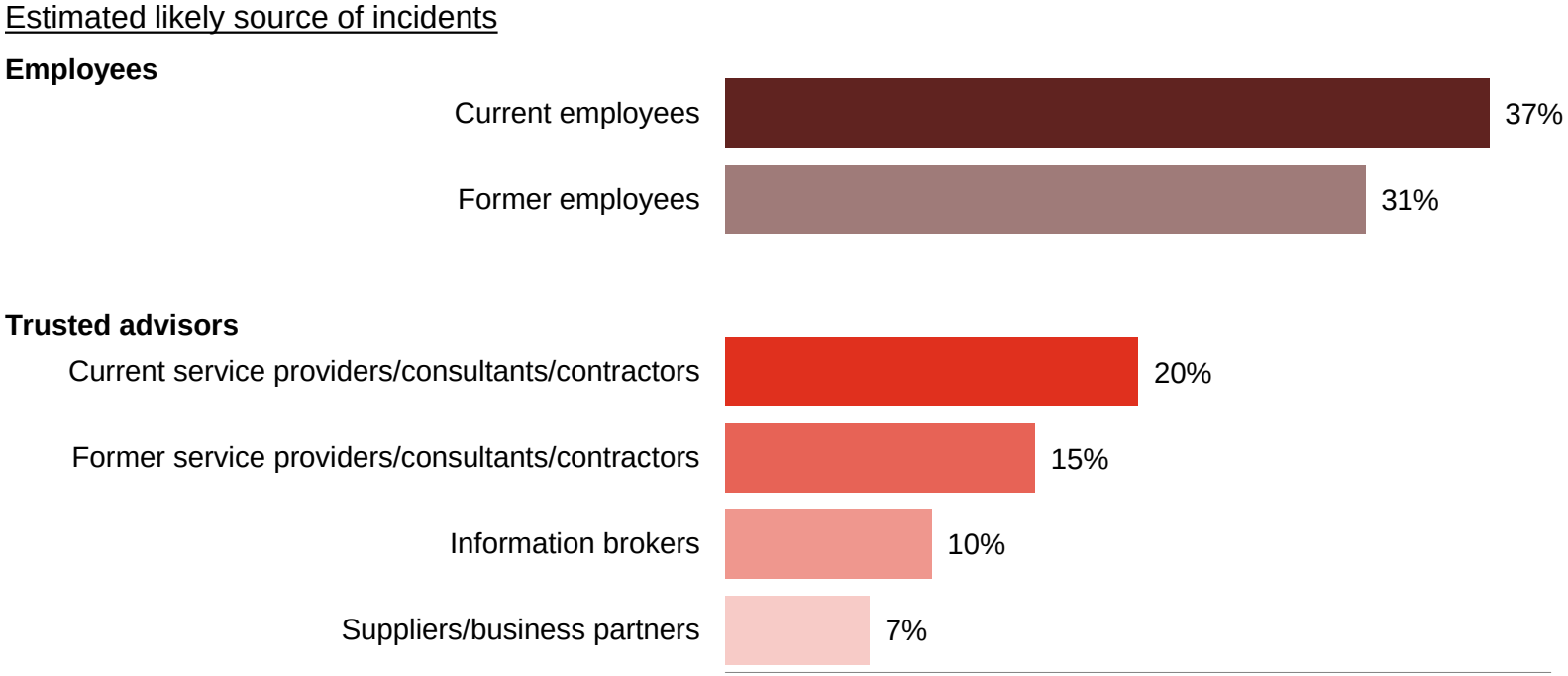
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most utilities respondents.

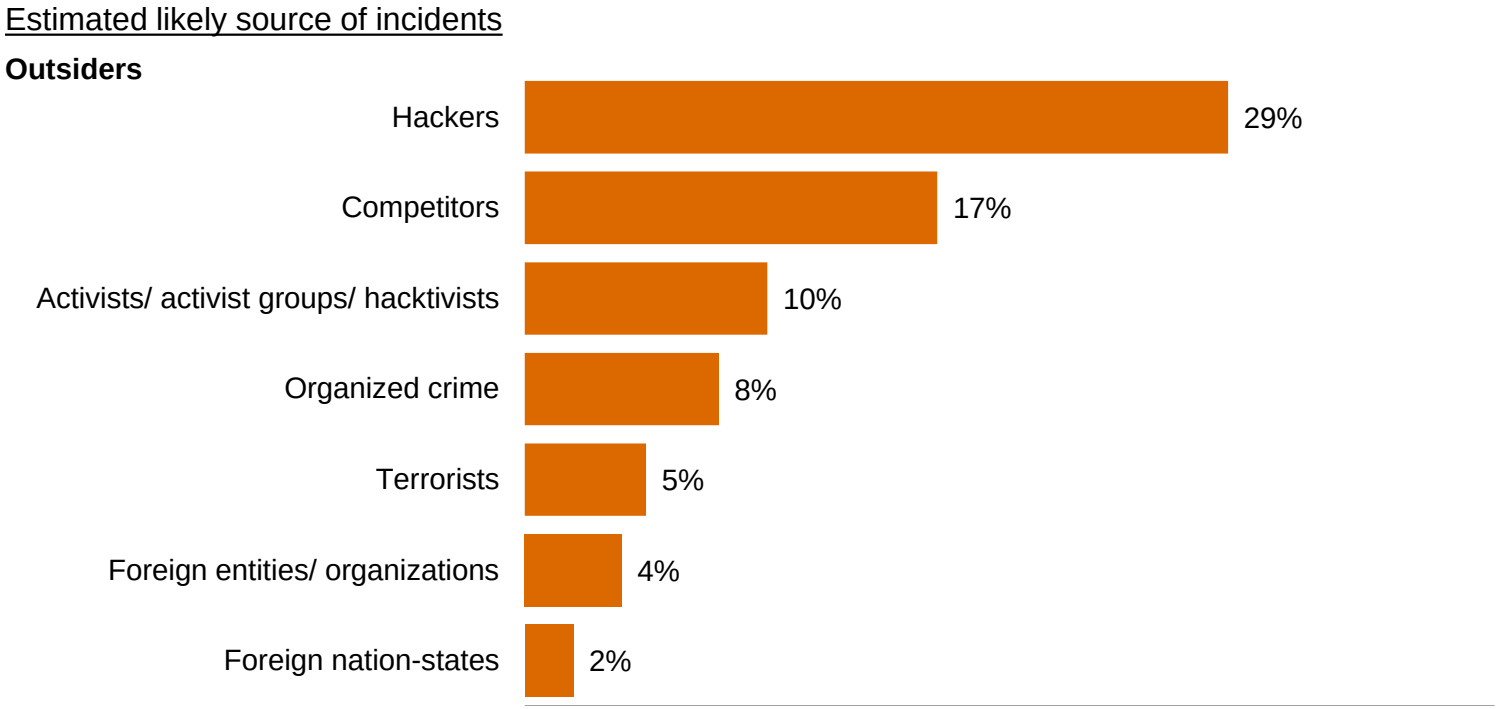
It's the people you know—current and former employees, as well as other insiders—who are most likely to perpetrate security incidents.



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, utilities are more likely to be hit by other outsiders.

Only 2% of utilities respondents report security incidents perpetrated by foreign nation-states. Hackers represent a more likely danger.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

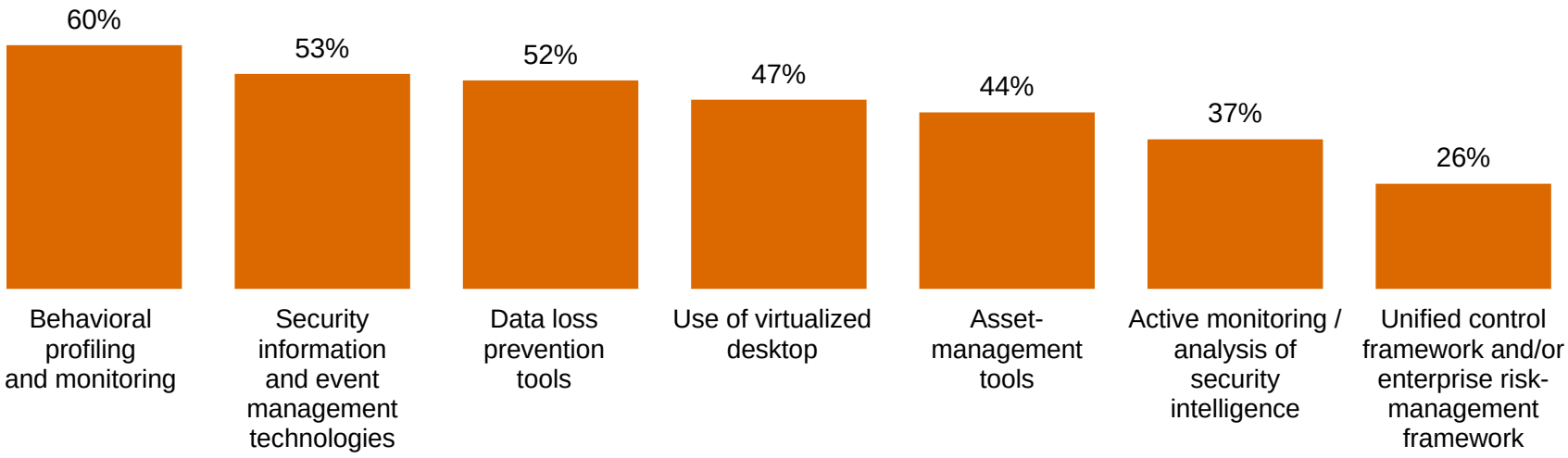
Section 4

A weak defense against adversaries

Many utilities respondents have not implemented technologies and processes that provide insight into risks.

Security safeguards that monitor data and assets are less likely to be in place than traditional safeguards. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place

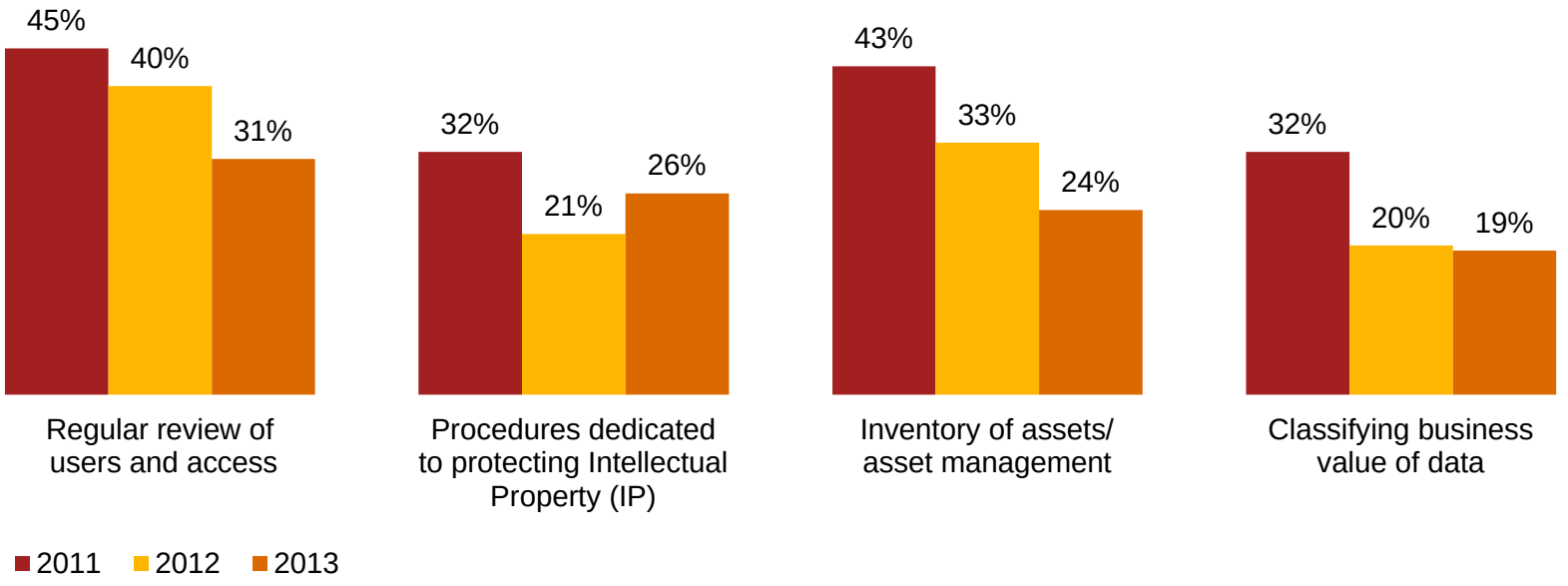


Question 14: “What process information security safeguards does your organization currently have in place?” Question 15: “Which technology information security safeguards does your organization currently have in place?” (Not all factors shown.) (Asked only of utilities respondents) Question 2: “Does your company employ a unified control framework and/or enterprise risk management framework for addressing cyber security risks?”

Despite the potential consequences, many utilities companies do not adequately safeguard their important assets.

It is imperative that organizations identify, prioritize, and protect their information assets, including critical infrastructure data. But implementation of many basic policies to safeguard this information is declining among utilities.

Have policies to help safeguard important assets

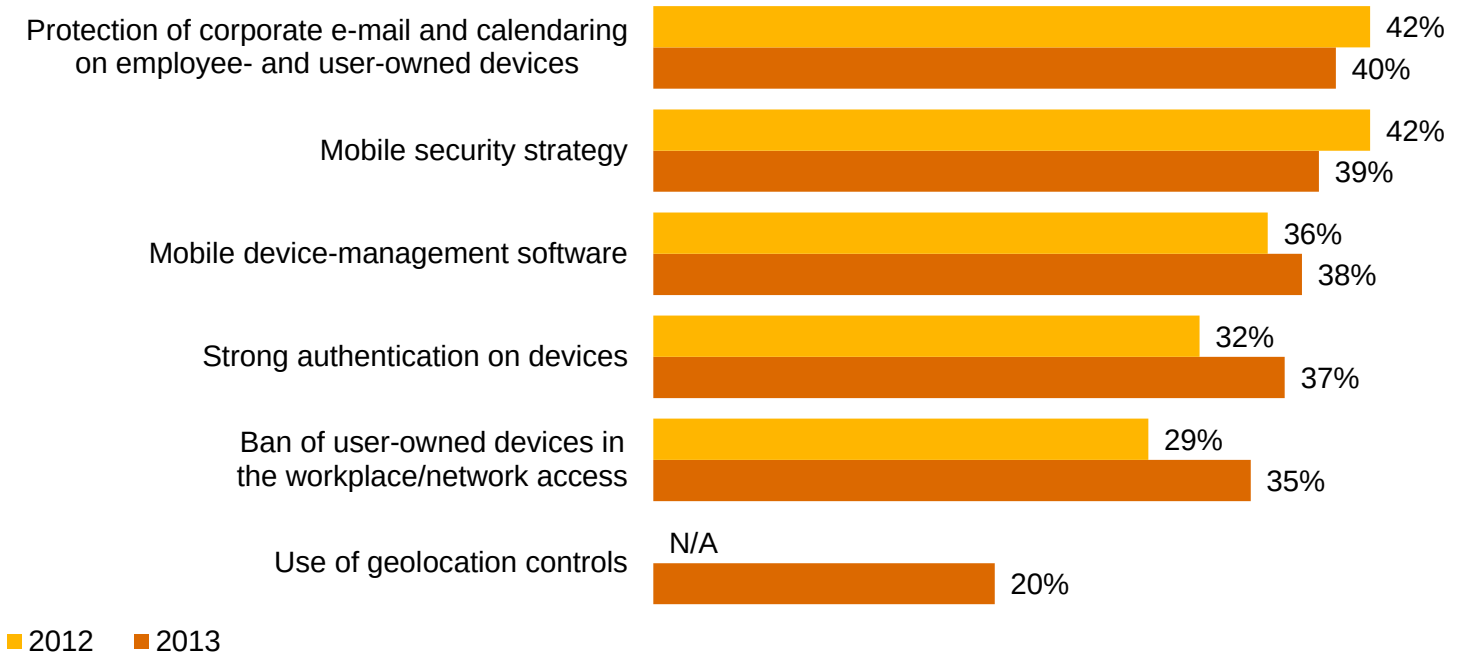


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet utilities respondents' efforts to implement mobile security programs do not show consistent gains over last year, and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

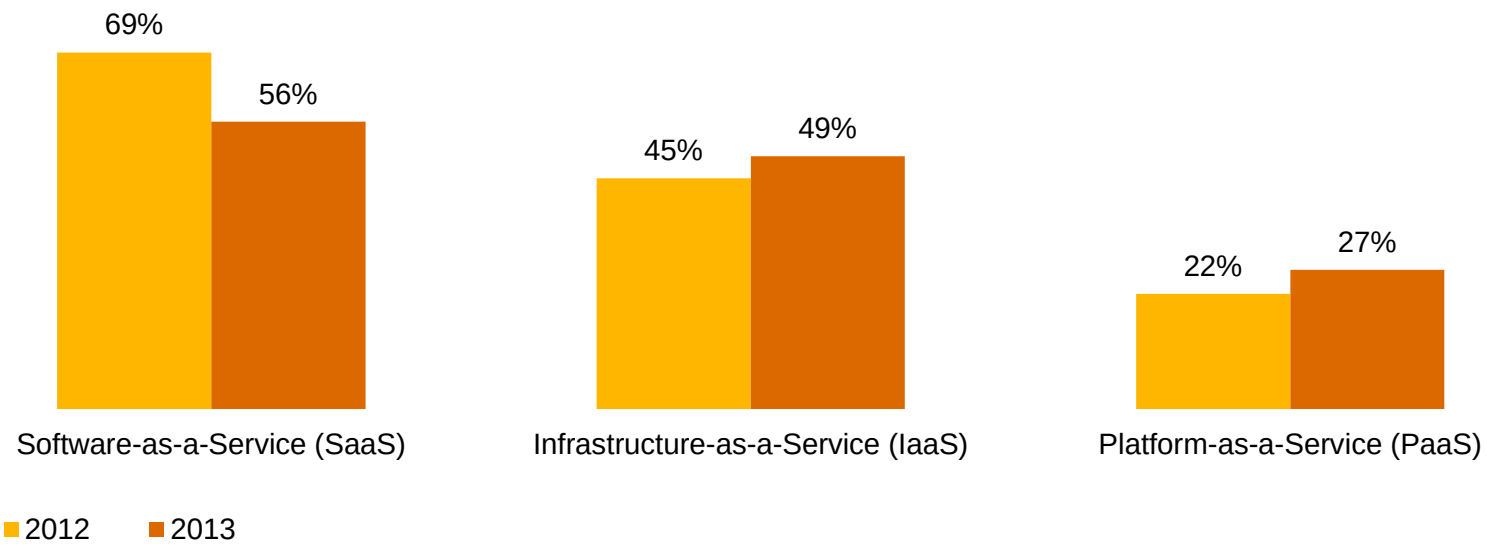


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Almost half of utilities respondents use cloud computing, but they often do not include cloud in their security policies.

While 48% of utilities respondents report using cloud computing—and 58% say the technology has improved security—only 14% include provisions for cloud in their security policy. SaaS, while still dominant, has declined over last year.

Type of cloud service used



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

29% of respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.[1]

Reasons for not collaborating on information security

[1] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

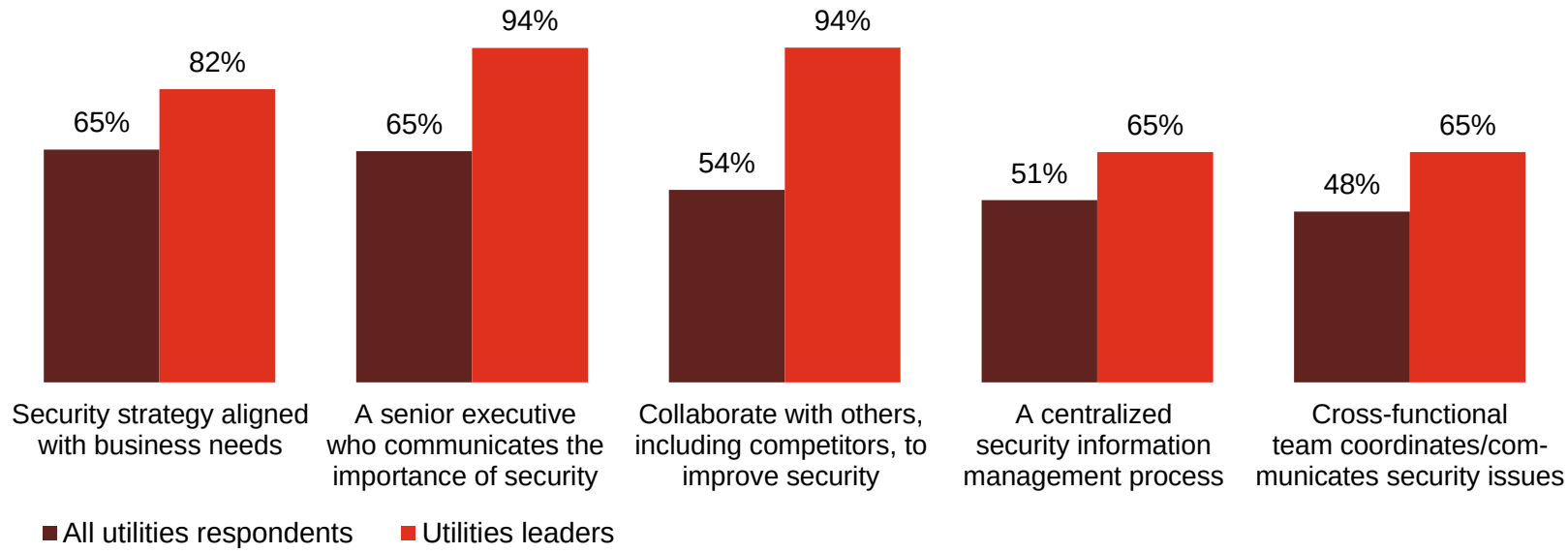
Section 5

Preparing for the threats of tomorrow

Utilities leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT challenge.

Aligning security with business needs, improving communications, and collaborating with others show leaders, in particular, are rethinking the fundamentals of security.

Security policies and safeguards currently in place: All respondents vs. leaders

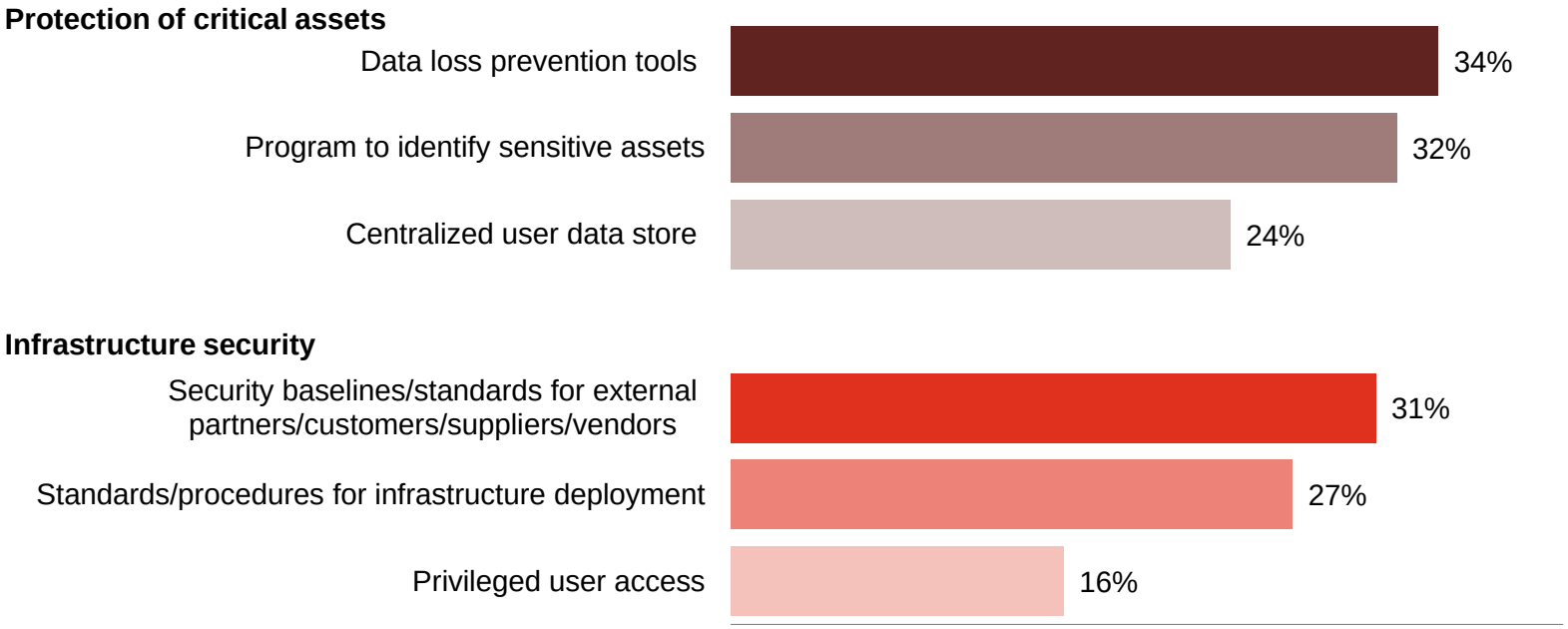


Question 14: "What process information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?" Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?"

What business imperatives and processes will utilities respondents prioritize this year?

Some of the highest priorities cited by respondents include technologies that can help the organization protect its most valuable assets and set security standards for third parties.

Safeguards not in place but a top priority over the next 12 months

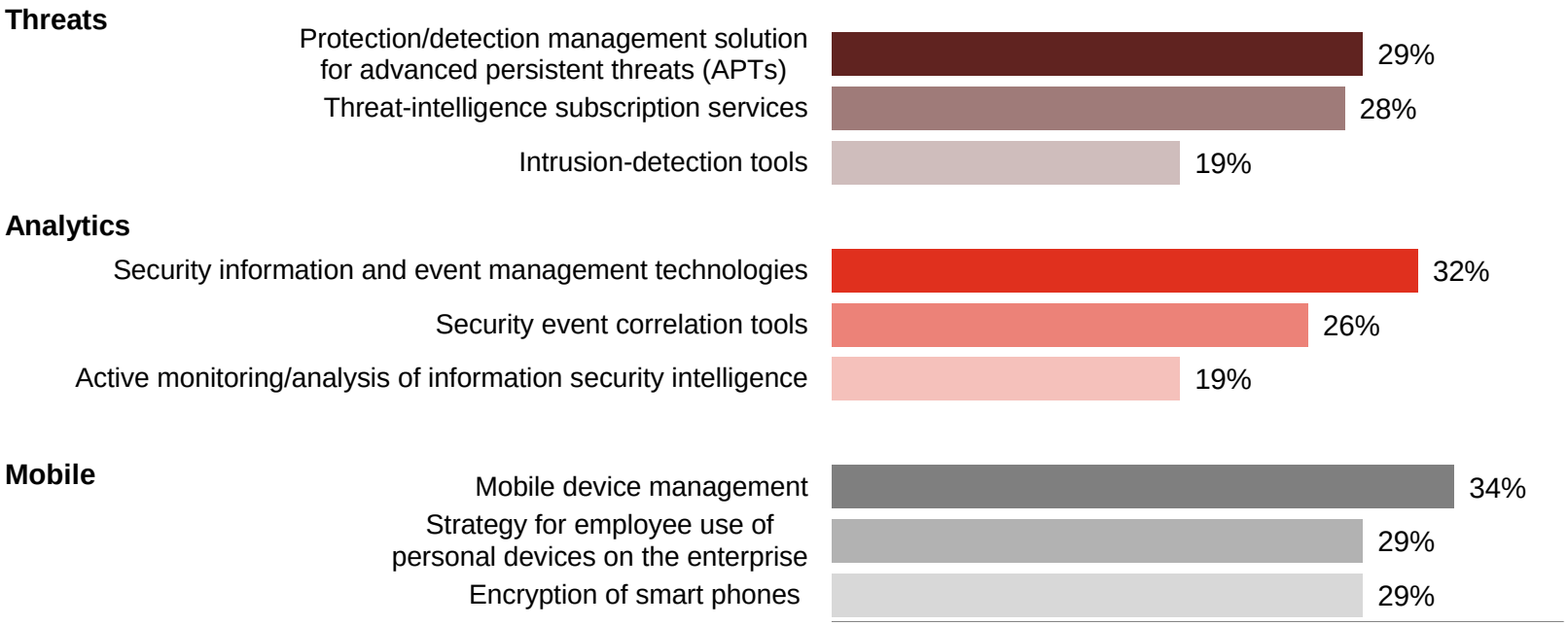


Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?"
Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and utilities are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months

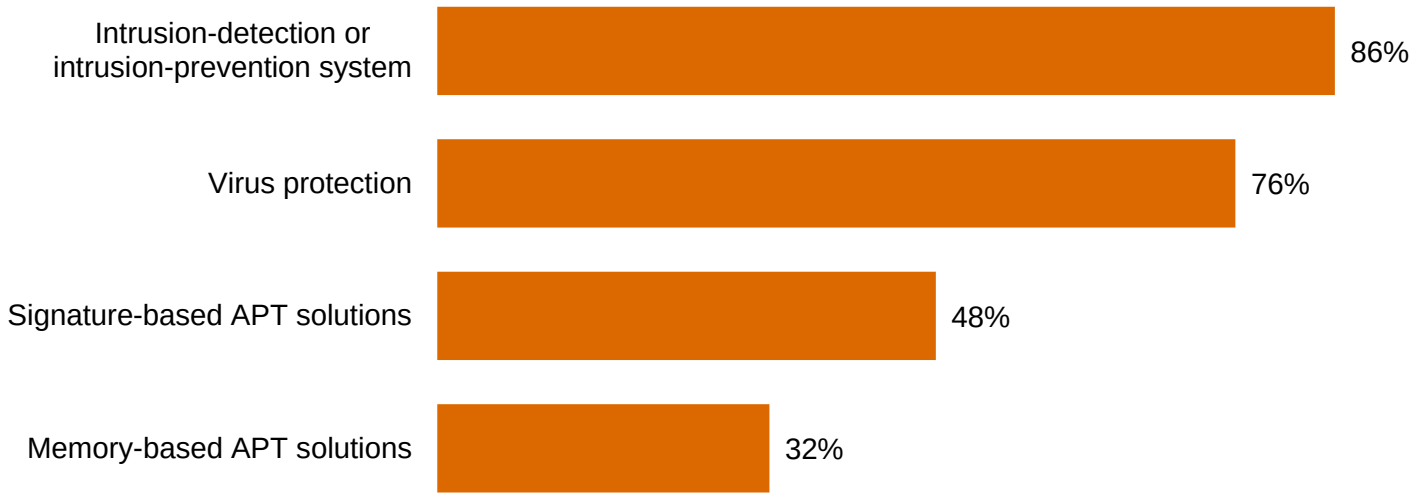


Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Utilities companies are beginning to address the risks of advanced persistent threats.

56% of utilities respondents say they have deployed technologies to help prevent APTs, an approximate increase of 60% over last year. Most rely on intrusion detection and prevention tools.

Technologies for protection against APTs



(Asked only of utilities respondents) Question 3: "Does your company have a program in place to monitor for and respond to advanced persistent threats (APTs)?" Question 3A: "What technologies does your organization employ to protect against APTs?'' (Not all factors shown.)

Effective security demands that utilities companies align security policies and spending with business objectives.

This year, more utilities respondents say security policies and spending are aligned with business objectives. This suggests they understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

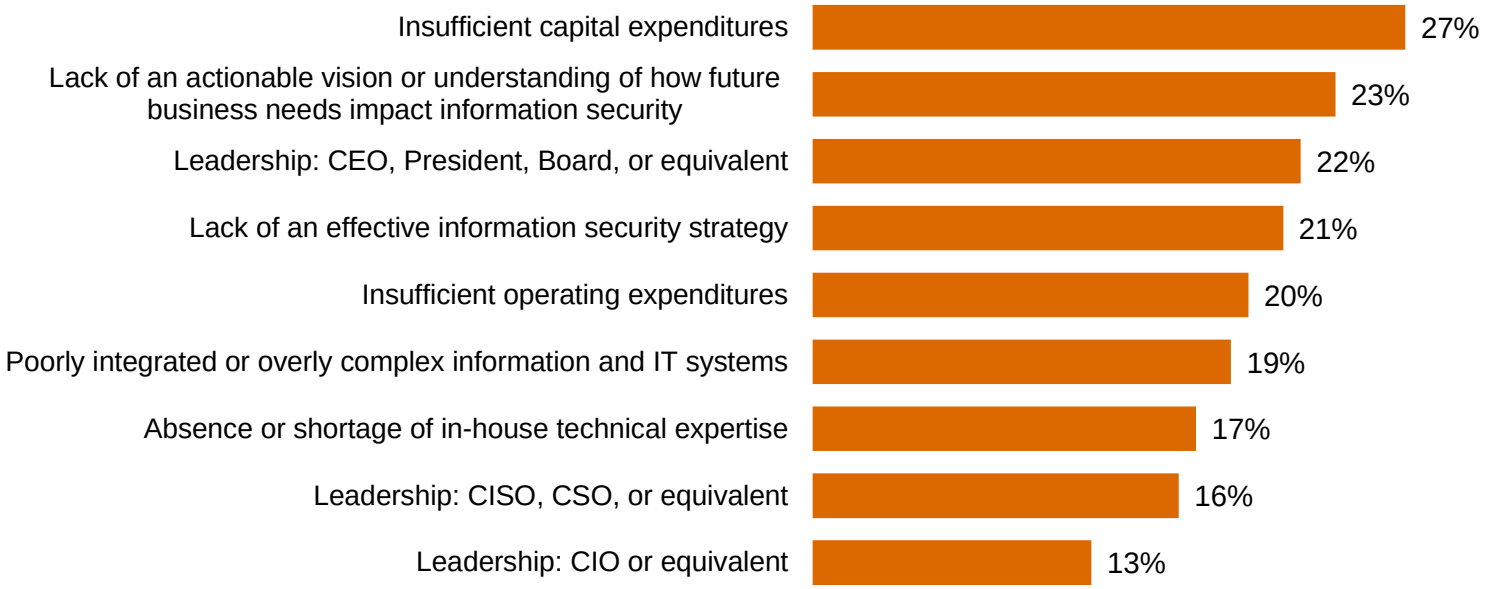
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

More money, an informed vision, and committed leadership are needed to advance security.

These are critical because an effective approach to security requires an adequate budget that is aligned with business needs and a vision of how future business needs will impact security.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are 10 key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
+1 949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
+1 646.471.5731
mark.a.lobel@us.pwc.com

US Power & Utilities Contacts

Brad Bauch
Principal
+1 713.356.4536
brad.bauch@us.pwc.com

Jon Stanford
Director
+1 971.544.4325
jonathan.k.stanford@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

Public Sector

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that administrators in global public sector organizations are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising and confidence is high.

But while many organizations have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased, while the cost of breaches has soared. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many public sector executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few public sector organizations have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that public sector organizations identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the organizational strategy, one that is championed by the CEO, and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

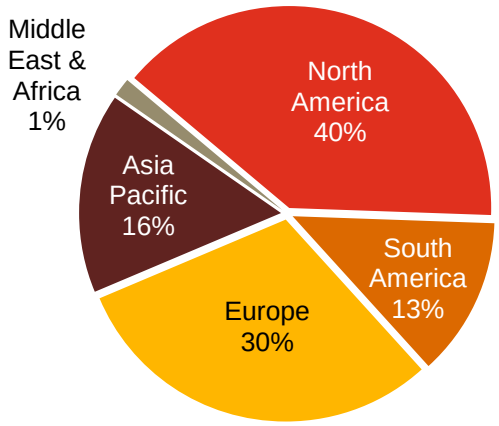
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, CIO magazine, and CSO magazine, was conducted online from February 1, 2013 to April 1, 2013.

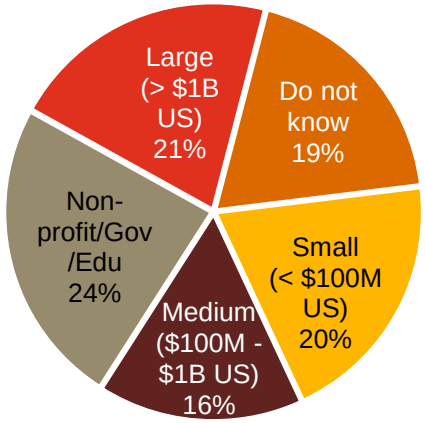
- PwC's 16th year conducting the online survey, 11th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 694 respondents from the public sector, which includes national/federal and state/provincial/local governments, education, and healthcare industries
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

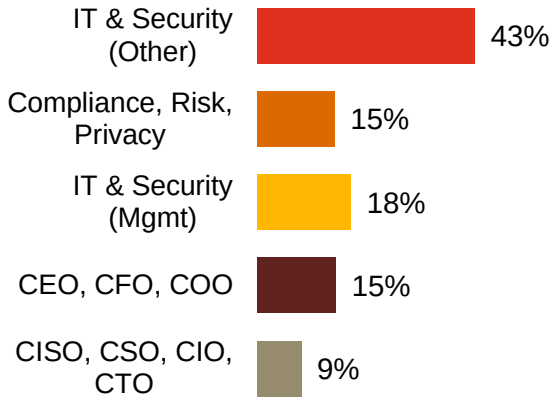
Public sector respondents by region of employment



Public sector respondents by company revenue size



Public sector respondents by title



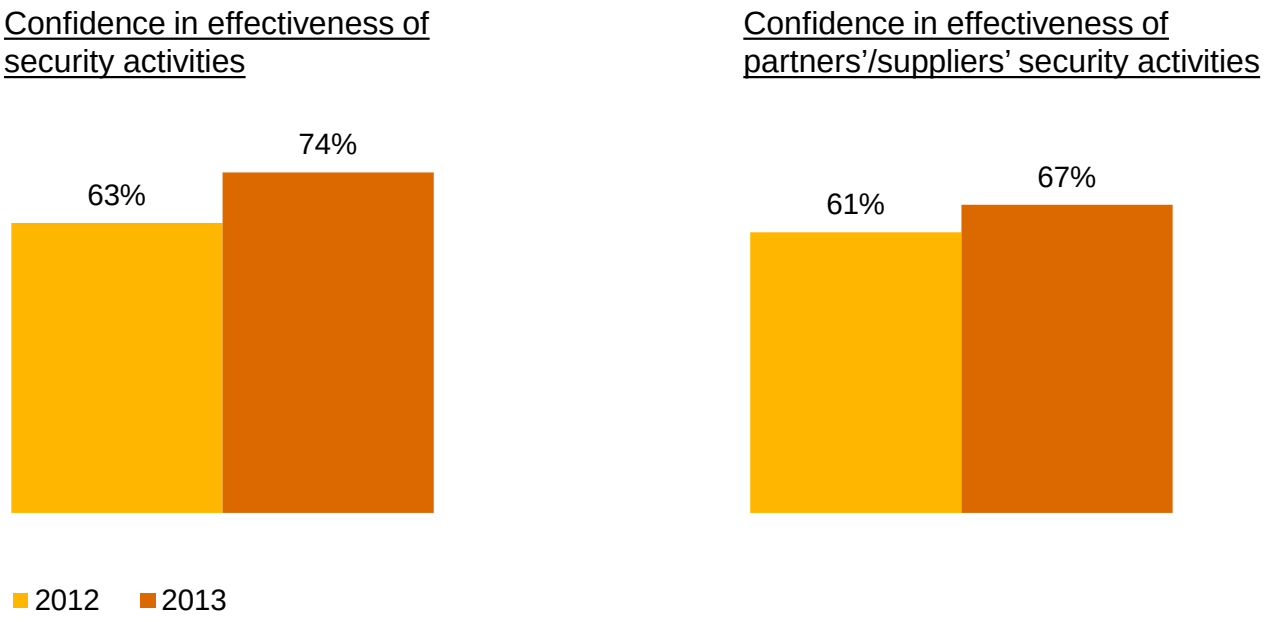
(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence in an era of advancing risks

Confidence is increasing: 74% of public sector respondents believe their security activities are effective.

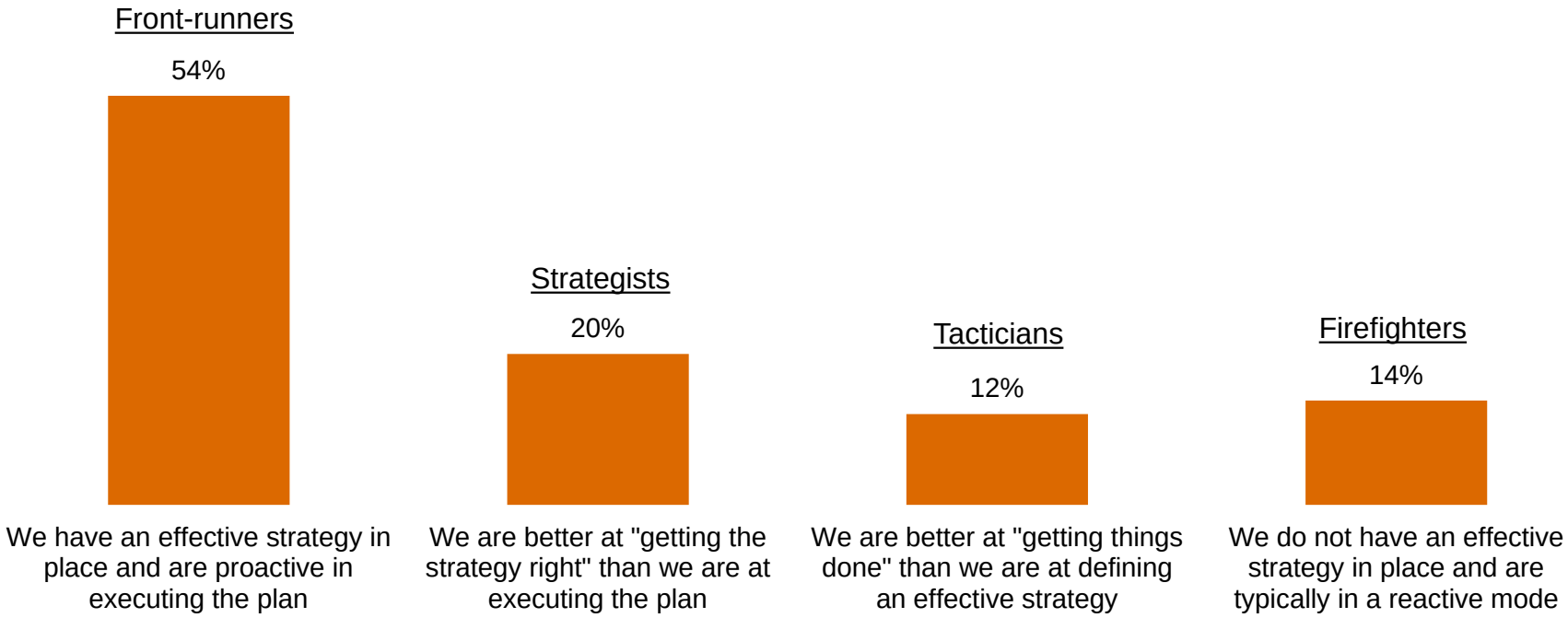
The number of public sector respondents who report their security programs are effective increased 17% over last year. Those reporting confidence in the efficacy of partners' and suppliers' security practices also advanced.



Question 39: "How confident are you that your organization's information security activities are effective?" Question 40: "How confident are you that your partners'/suppliers' information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.") (Not all factors shown.)

54% of respondents consider themselves "front-runners," ahead of the pack in security strategy and practices.

The number of public sector respondents who say they have an effective strategy in place and are proactive in executing the plan increased 30% over last year, a strong indicator of confidence.



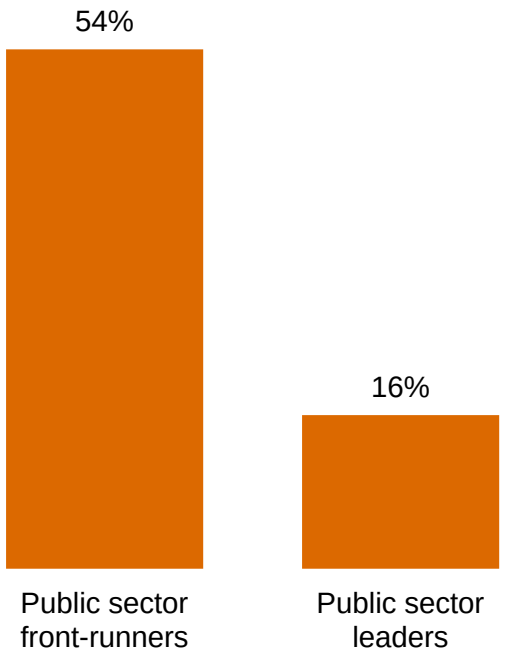
Question 27: "Which statement best characterizes your organization's approach to protecting information security?"

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured public sector respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

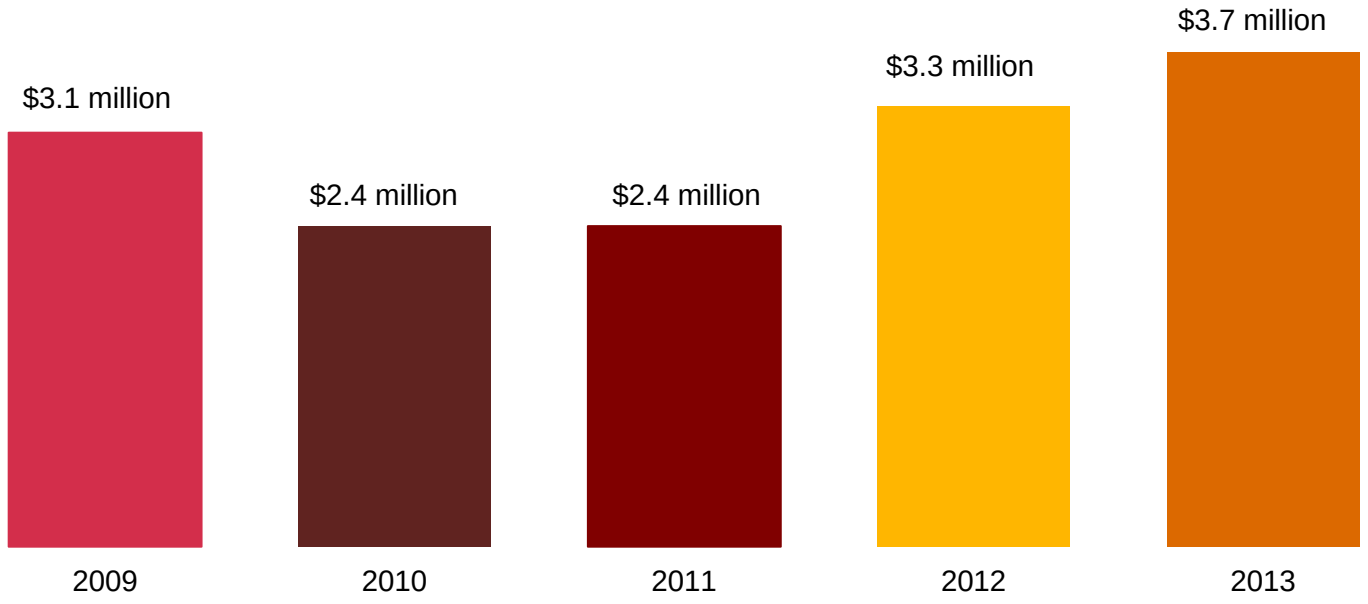


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Public sector information security budgets have increased.

Public sector information security budgets average $3.7 million this year, an increase 0f 14% over last year. This suggests that public sector entities understand that today's elevated threat landscape demands a boost in security investment.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

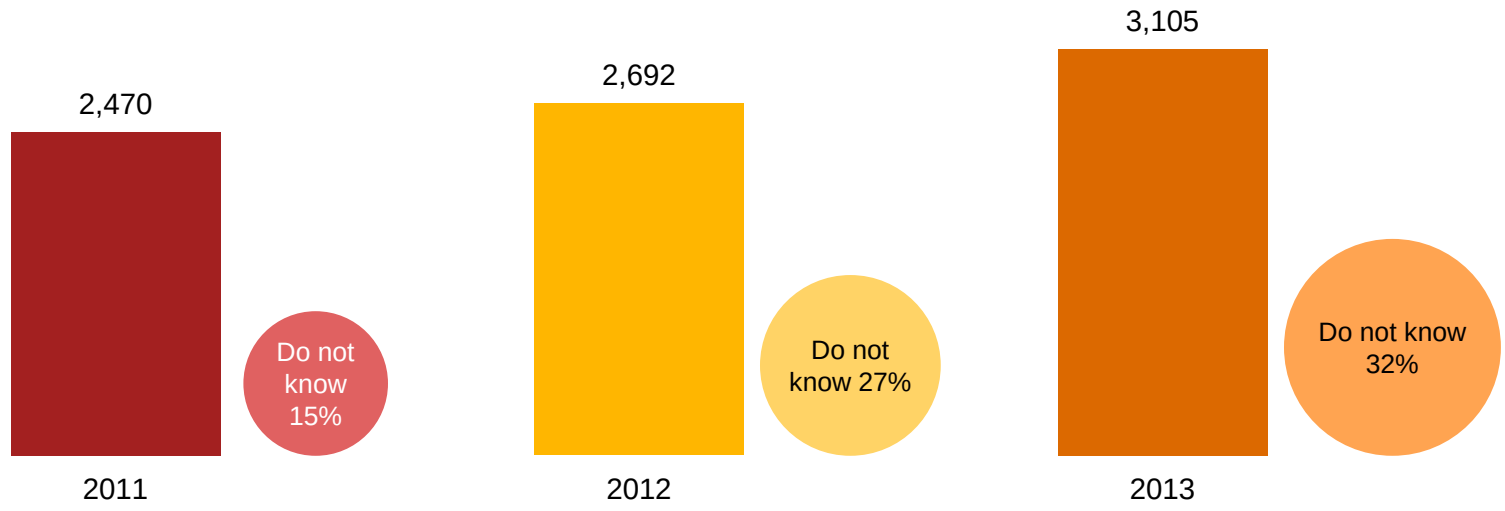
Section 3

Today's incidents, yesterday's strategies

*Public sector respondents detect more security incidents.**

The number of incidents detected in the past 12 months increased by 15%, perhaps an indication of today's elevated threat environment. The average financial losses as a result of security incidents skyrocketed 101% over 2012, which is not surprising given the cost and complexity of responding to incidents.

Average number of security incidents in past 12 months



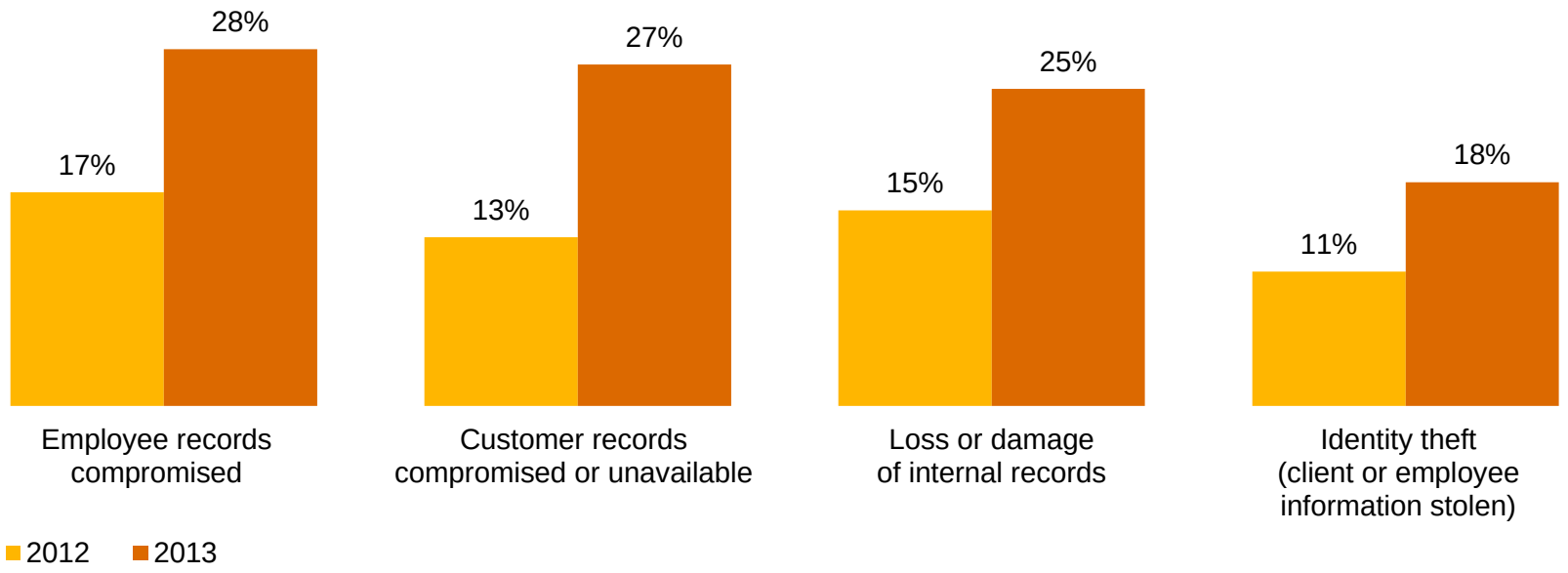
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

Public sector respondents report a significant increase in data loss as a result of security incidents.

Compromise of employee and customer records remain the most cited impacts, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records jumped by 62% over 2012.

Impact of security incidents

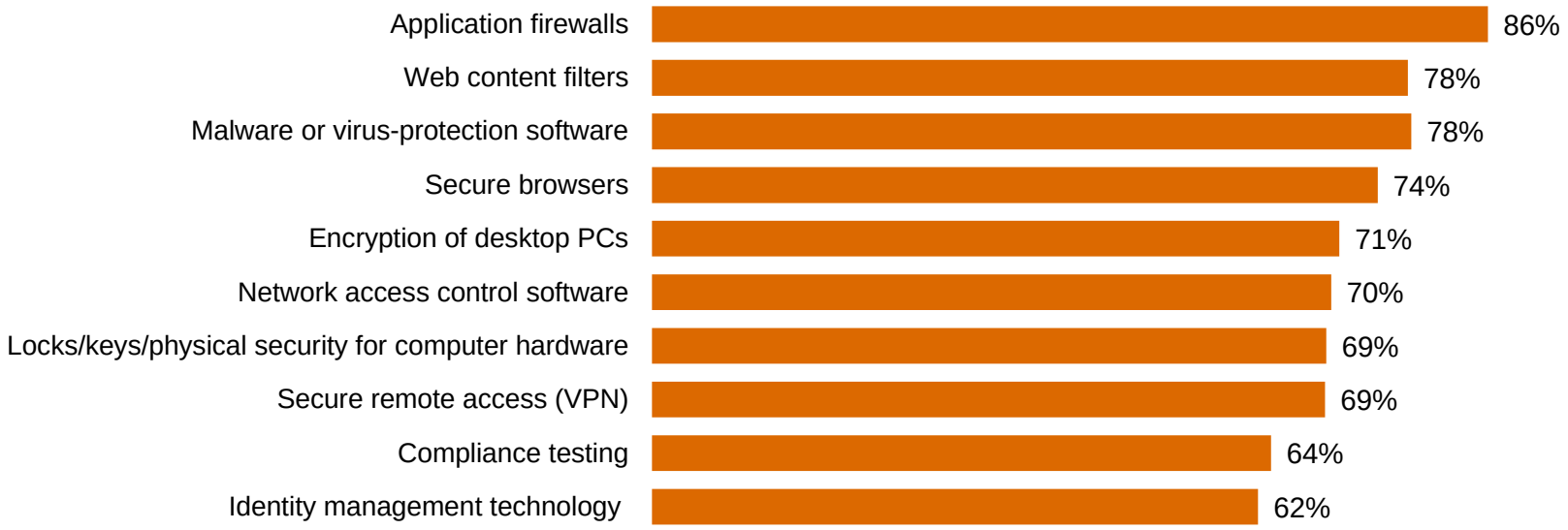


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

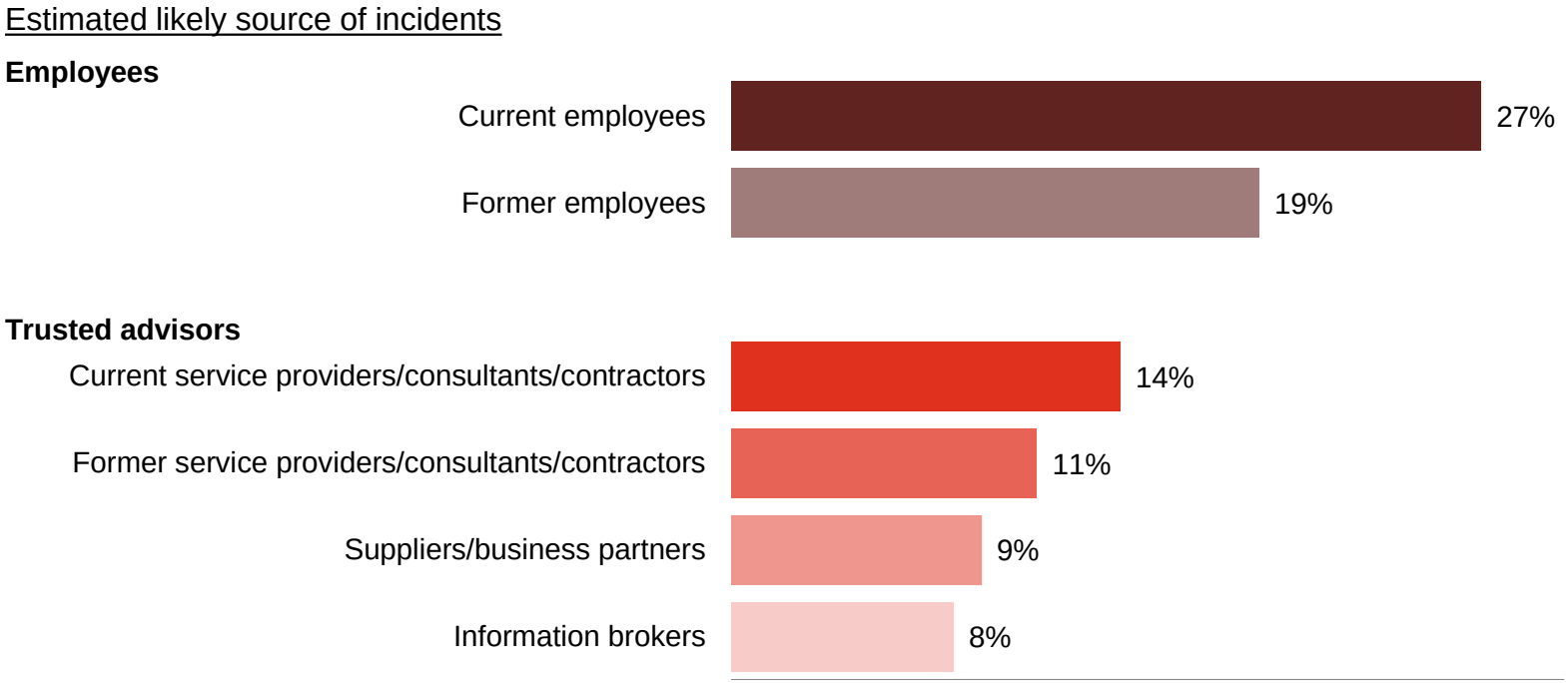
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most public sector respondents.

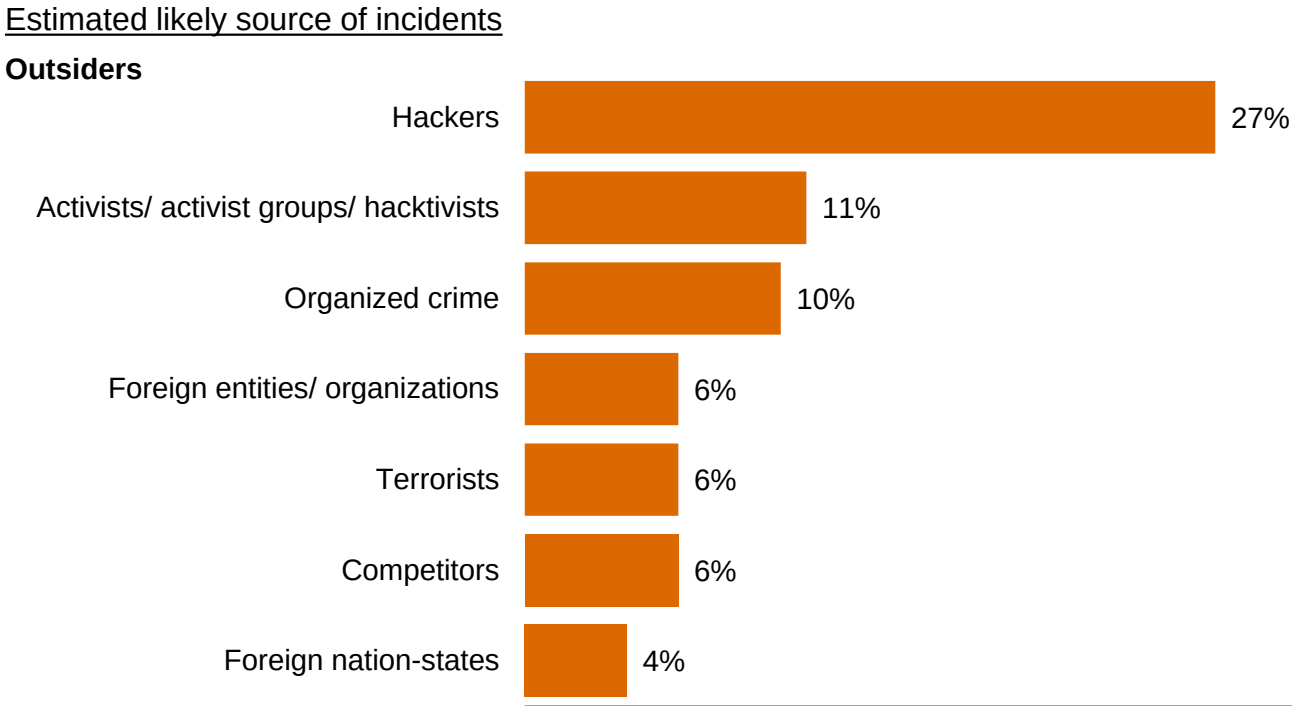
It's the people you know—current and former employees, as well as service providers and contractors—who are most likely to perpetrate security incidents.



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, organizations are more likely to be hit by other outsiders.

Only 4% of public sector respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

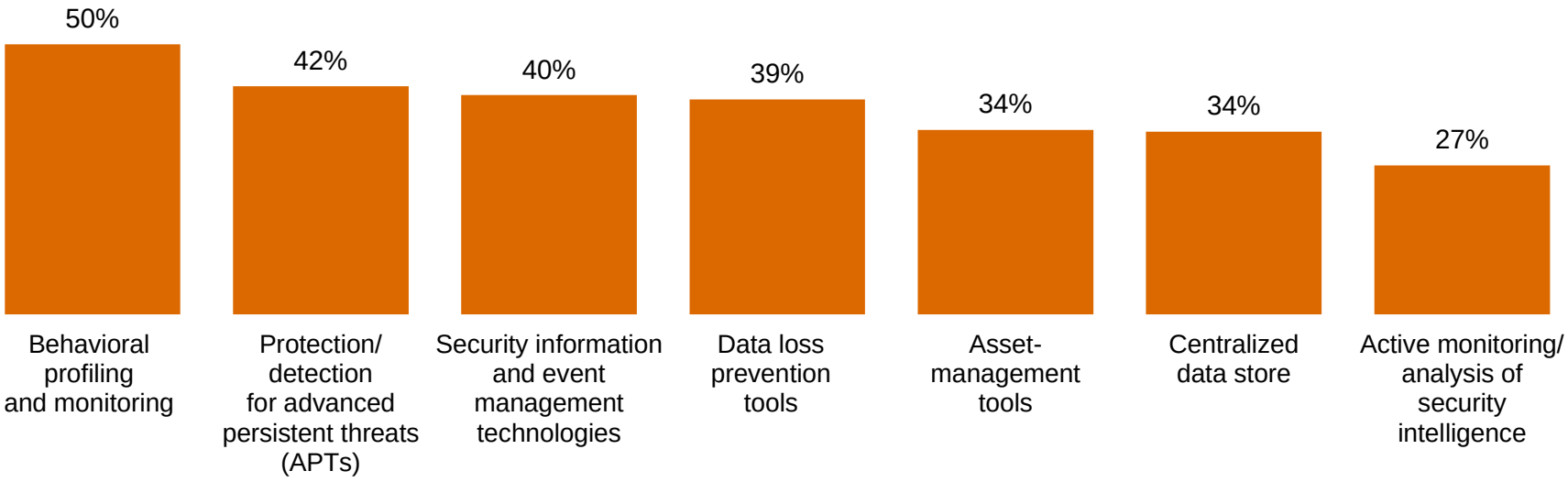
Section 4

A weak defense against adversaries

Many public sector entities have not implemented technologies that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place

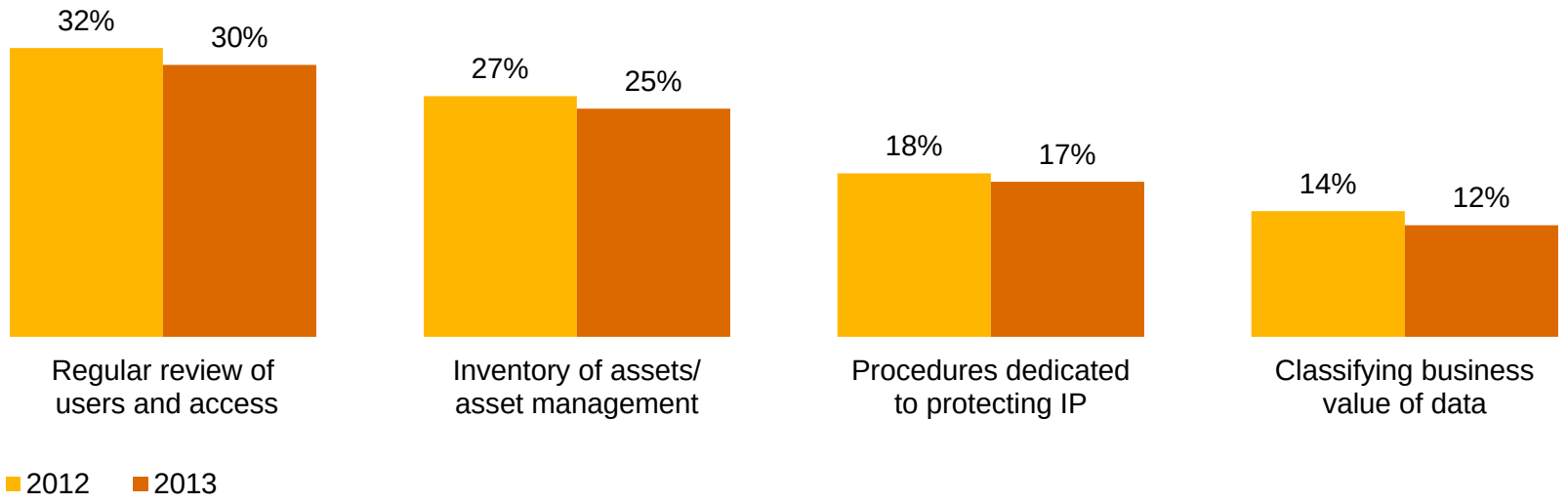


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite the potential consequences, many organizations do not adequately safeguard their high-value information.

It is imperative that public sector organizations identify, prioritize, and protect their "crown jewels." But respondents report a decline in implementation of basic policies to safeguard intellectual property (IP).

Have policies to help safeguard IP and trade secrets

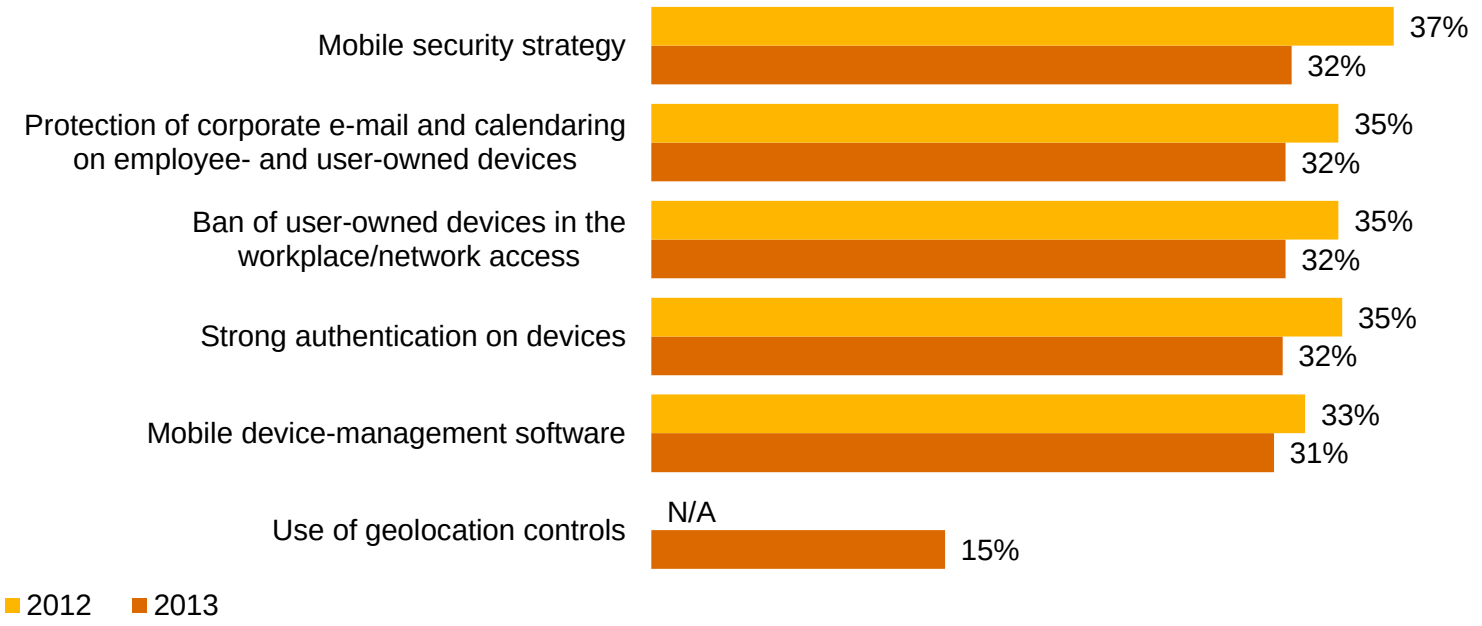


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of security initiatives has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet the public sector's efforts to implement mobile security programs show declines over last year, and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

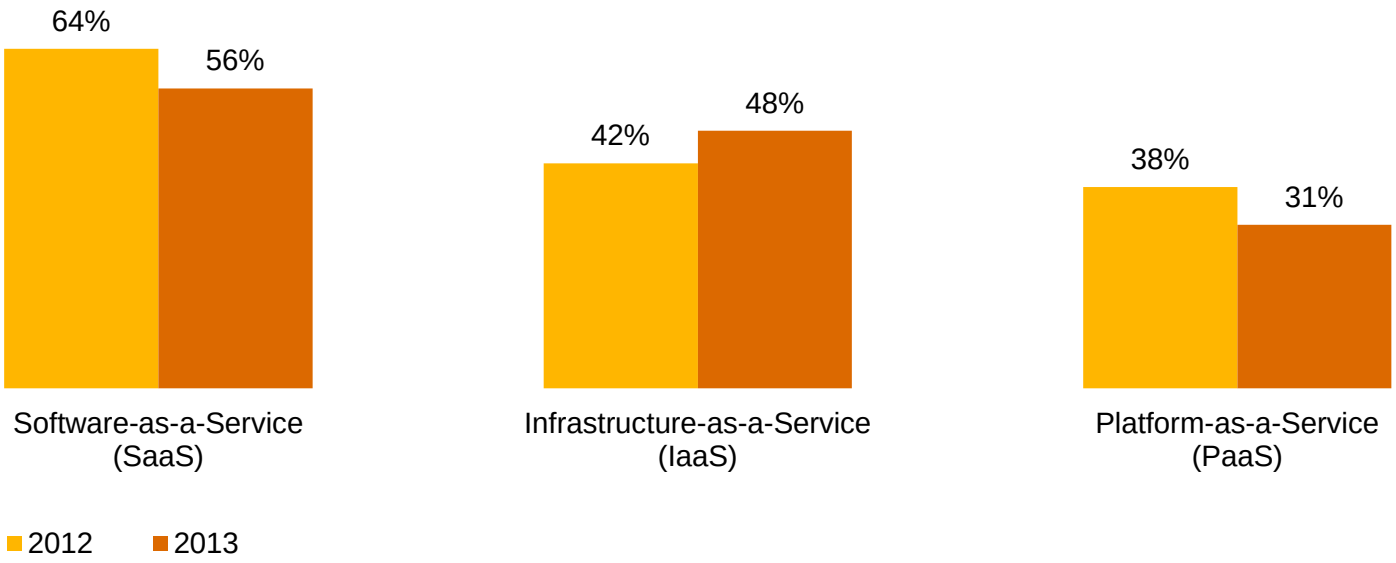


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Only 35% of public sector entities use cloud computing, but those that do often omit cloud from their security policies.

Adoption of cloud computing lags that of other industries, and few (14%) public sector respondents include cloud computing in their security policy. Public sector users of cloud services 59% report better security.

Type of cloud service used



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

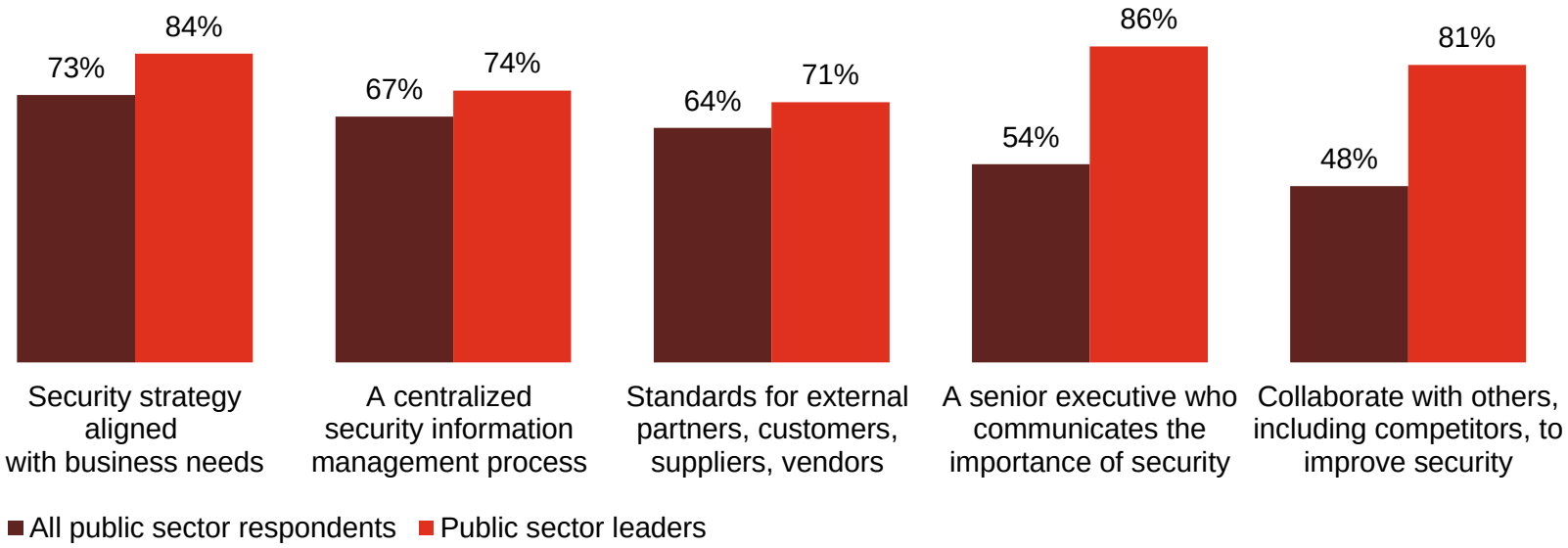
Section 5

Preparing for the threats of tomorrow

Public sector leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT issue.

Aligning security with business needs, setting standards for external partners, and collaborating with others show leaders, in particular, are rethinking the basics of security.

Security policies and safeguards currently in place: All respondents vs. leaders

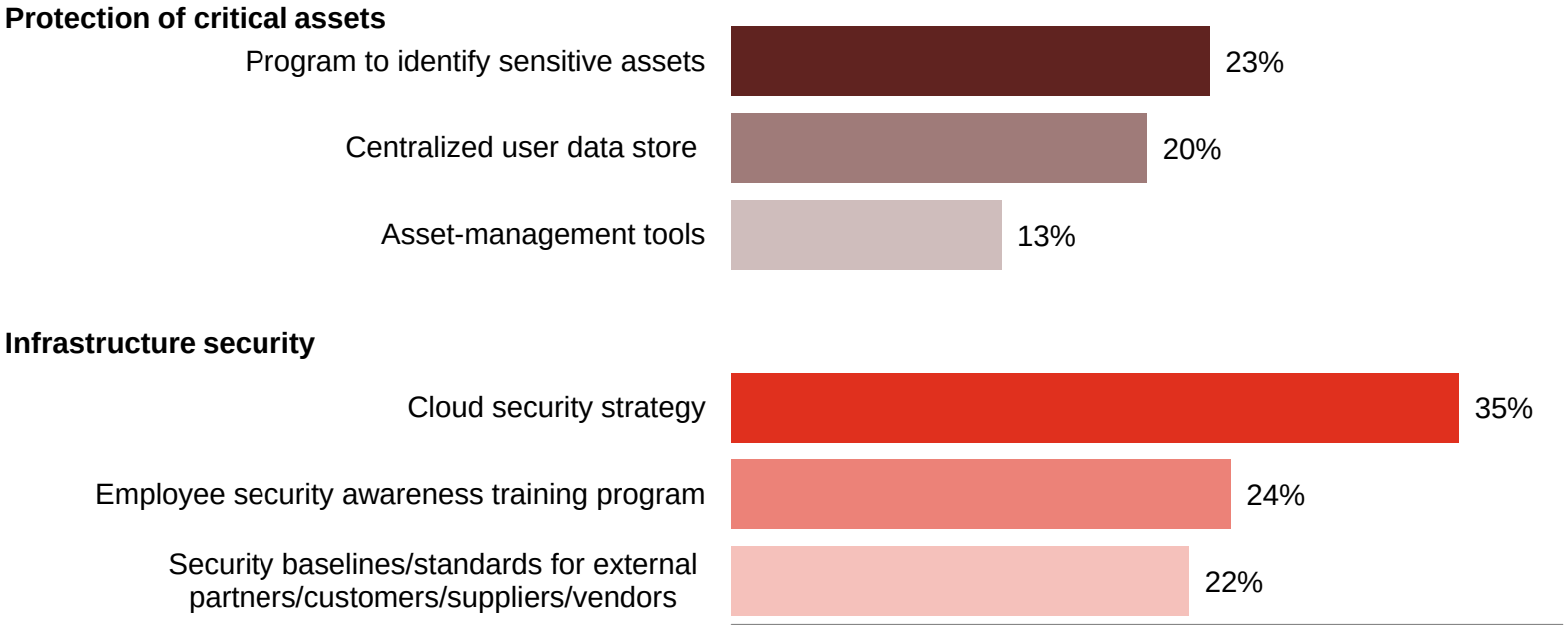


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?" Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?"

What business imperatives and processes will the public sector prioritize this year?

Some of the highest priorities cited by respondents include technologies that can help the organization safeguard its most valuable assets and protect the infrastructure.

Safeguards not in place but a top priority over the next 12 months

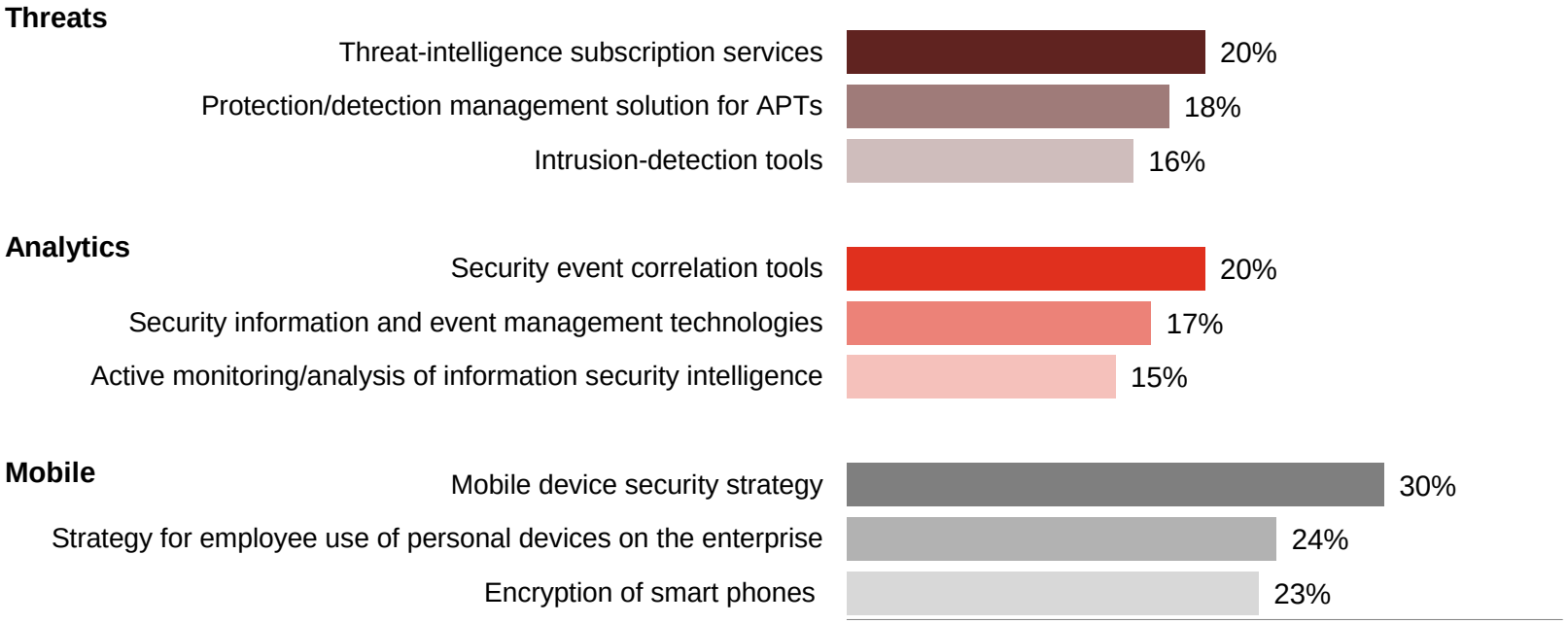


Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Other priorities focus on detecting and responding to threats and managing mobile devices.

Knowledge is power, and organizations are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Effective security demands that organizations align security policies and spending with business objectives.

This year, more public sector respondents say security policies and spending are aligned with business objectives. This suggests they understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

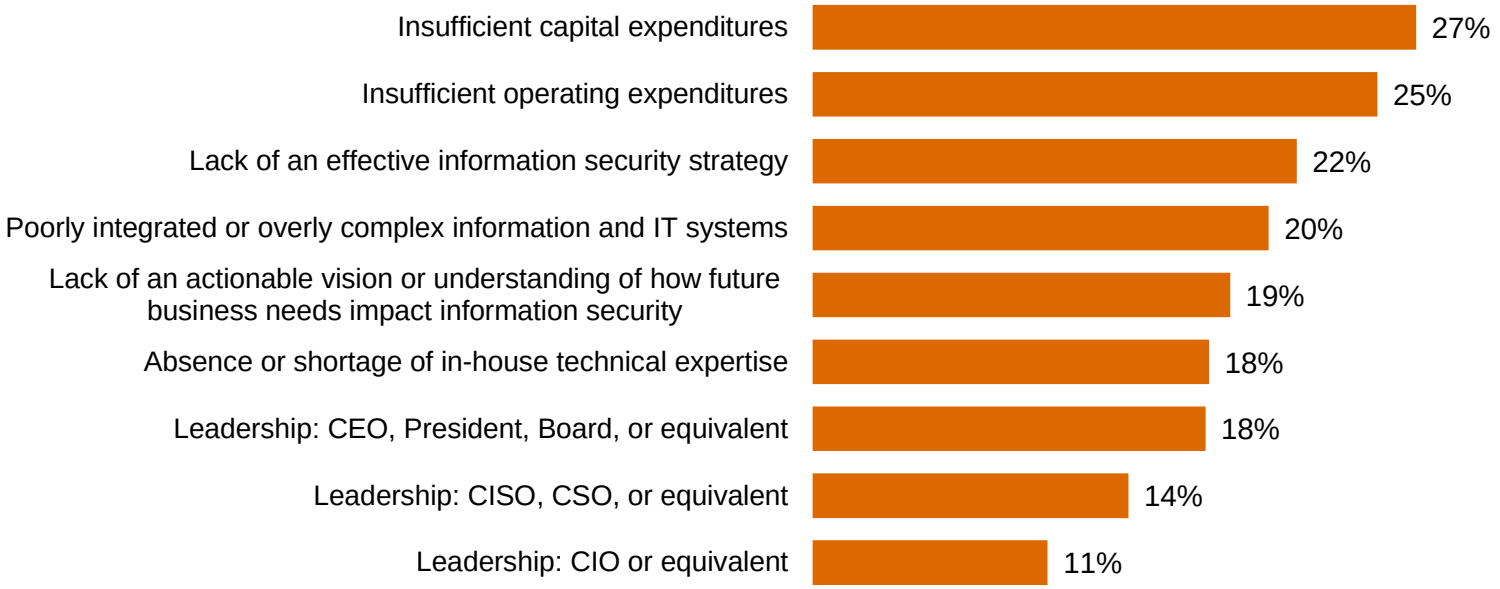
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

More money—both capital and operating expenditures—are needed to advance security in the public sector.

Respondents say inadequate funding—both capital and operating expenditures—is standing in the way of better information security. Other significant obstacles include a lack of an effective strategy and overly complex IT systems.

Greatest obstacles to improving the strategic effectiveness of the organization's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are 10 key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- Top executives and senior leaders should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts—Private Sector

Gary Loveland
Principal
+1 949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
+1 646.471.5731
mark.a.lobel@us.pwc.com

US Public Sector Contacts

Jack Johnson
Principal
+1 703.918.1303
johnson.jack@us.pwc.com

John Hunt
Principal
+1 703.918.3767
john.d.hunt@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

Retail & Consumer

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global retail and consumer (R&C) industry are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising and confidence is high.

But while many R&C companies have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased, as has the cost of breaches. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few R&C companies have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that companies identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

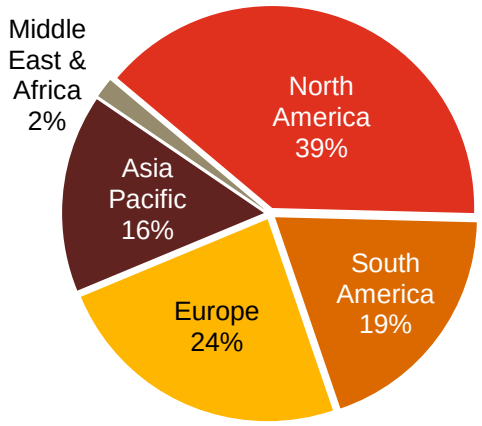
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

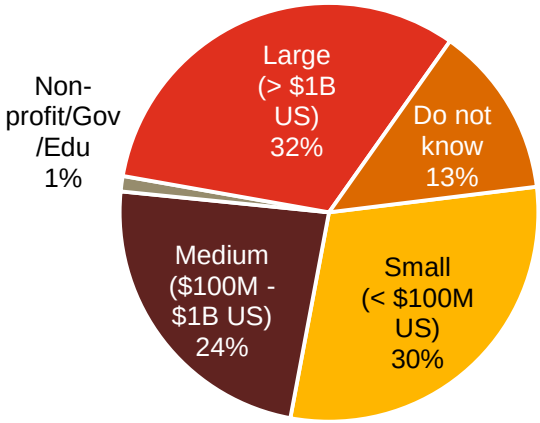
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- The survey included 820 respondents from the retail and consumer industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

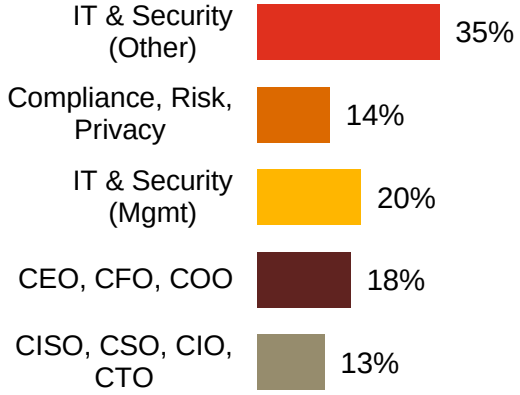
R&C respondents by region of employment



R&C respondents by company revenue size



R&C respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

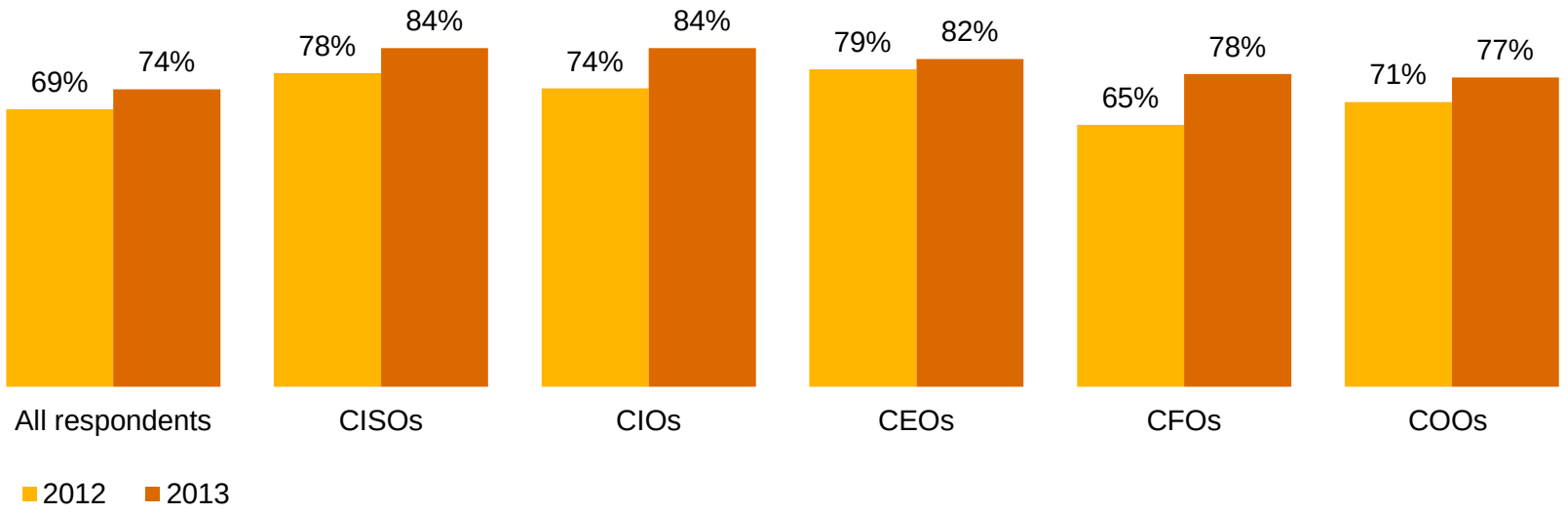
Section 2

Confidence in an era of increasing risks

Confidence is high: 74% of R&C respondents say their security activities are effective, with top execs even more optimistic.

In the C-suite,* 82% of CEOs say they are confident in their security program. Among all executives, CISOs and CIOs report the highest confidence.

Executive confidence in effectiveness of security activities (somewhat or very confident)

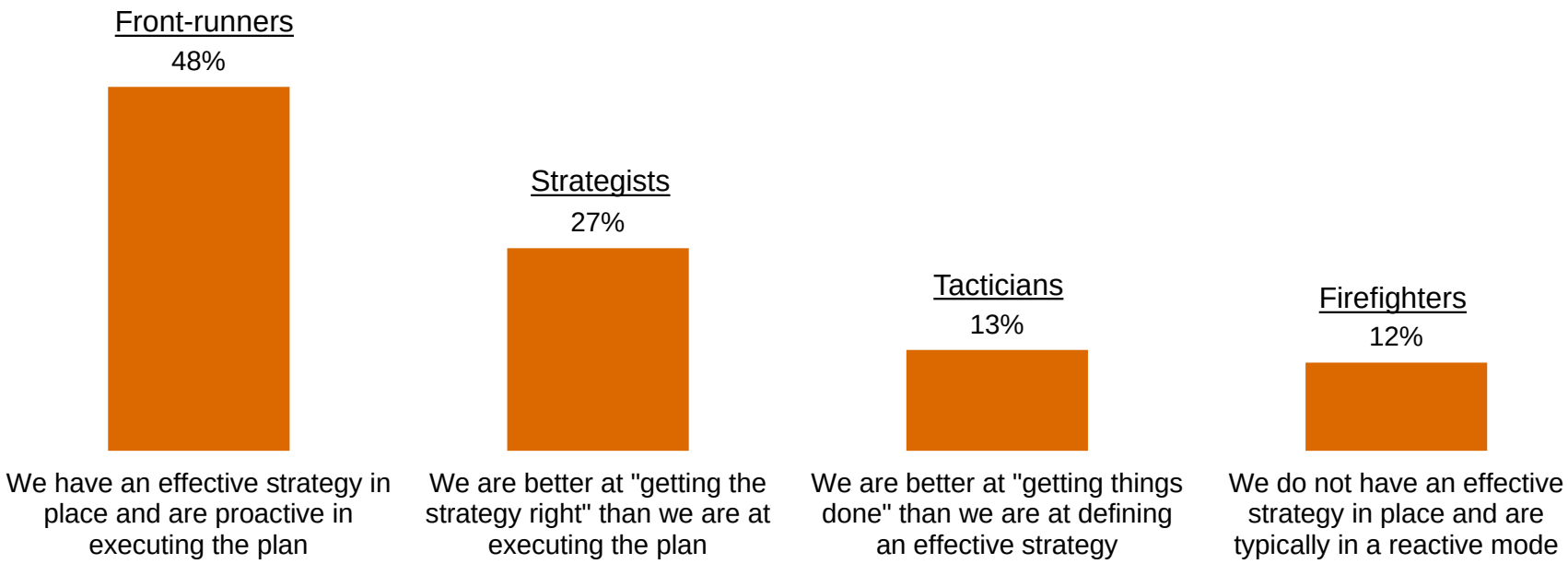


* CEOs, CFOs, and COOs

Question 39: "How confident are you that your organization's information security activities are effective?" (Respondents who answered "Somewhat confident" or "Very confident.") Question 1: "My job title most closely resembles"

48% of R&C respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

Almost half say they have an effective strategy in place and are proactive in executing the plan, a 24% increase over last year. More than one in four (27%) say that they are better at getting the strategy right than executing the plan.



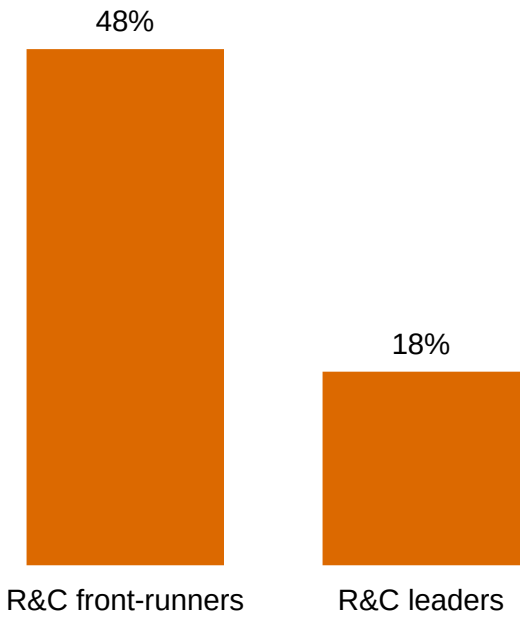
Question 27: "Which statement best characterizes your organization's approach to protecting information security?"

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured R&C respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

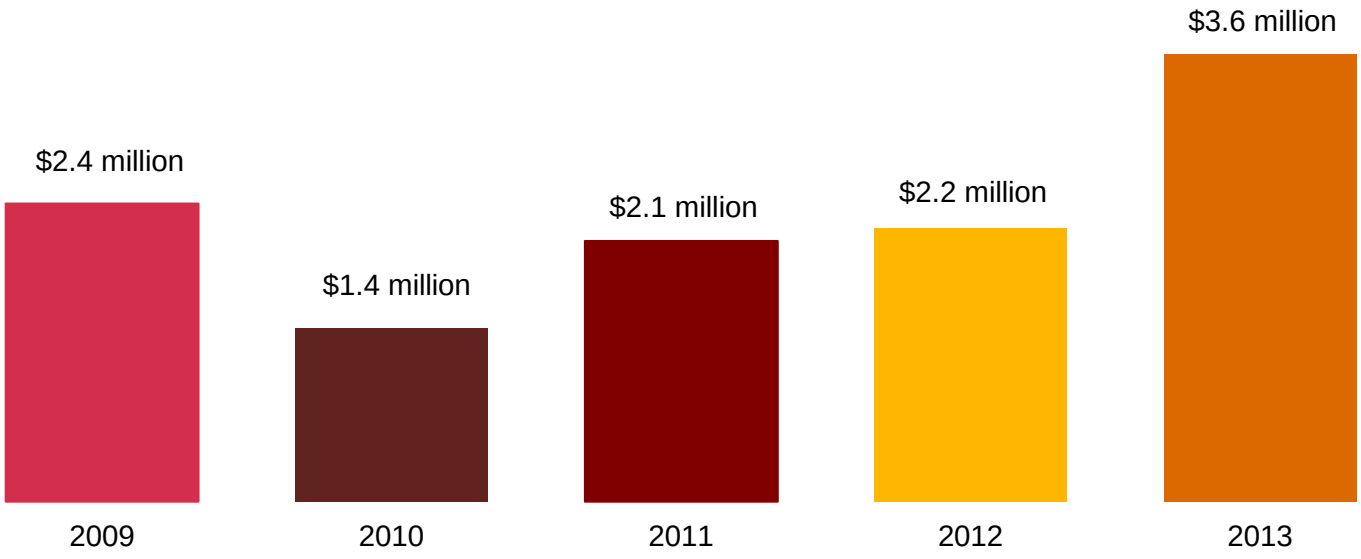


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

R&C information security budgets increase significantly.

Security budgets average $3.6 million this year, an increase of 61% over last year. R&C companies appear to understand that today's elevated threat landscape demands a substantial boost in security investment.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

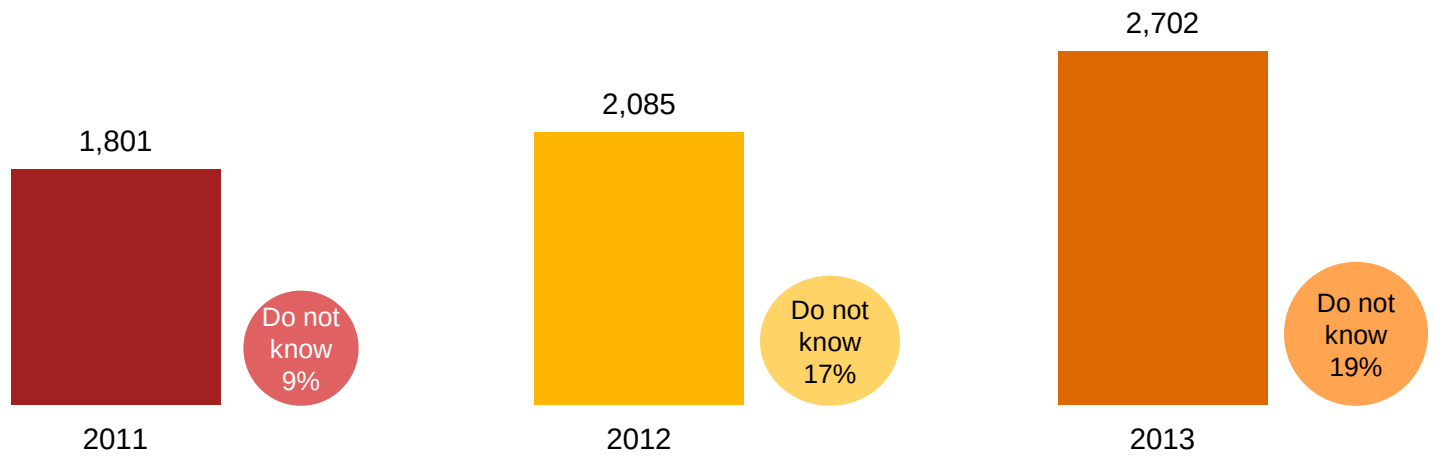
Section 3

Today's incidents, yesterday's strategies

*R&C companies detect more security incidents.**

The average number of incidents detected by R&C respondents in the past 12 months increased 30% over last year, perhaps an indication of today's elevated threat environment. Average financial losses as a result of security incidents are up 46%, which is not surprising given the cost and complexity of responding to incidents.

Average number of security incidents in past 12 months



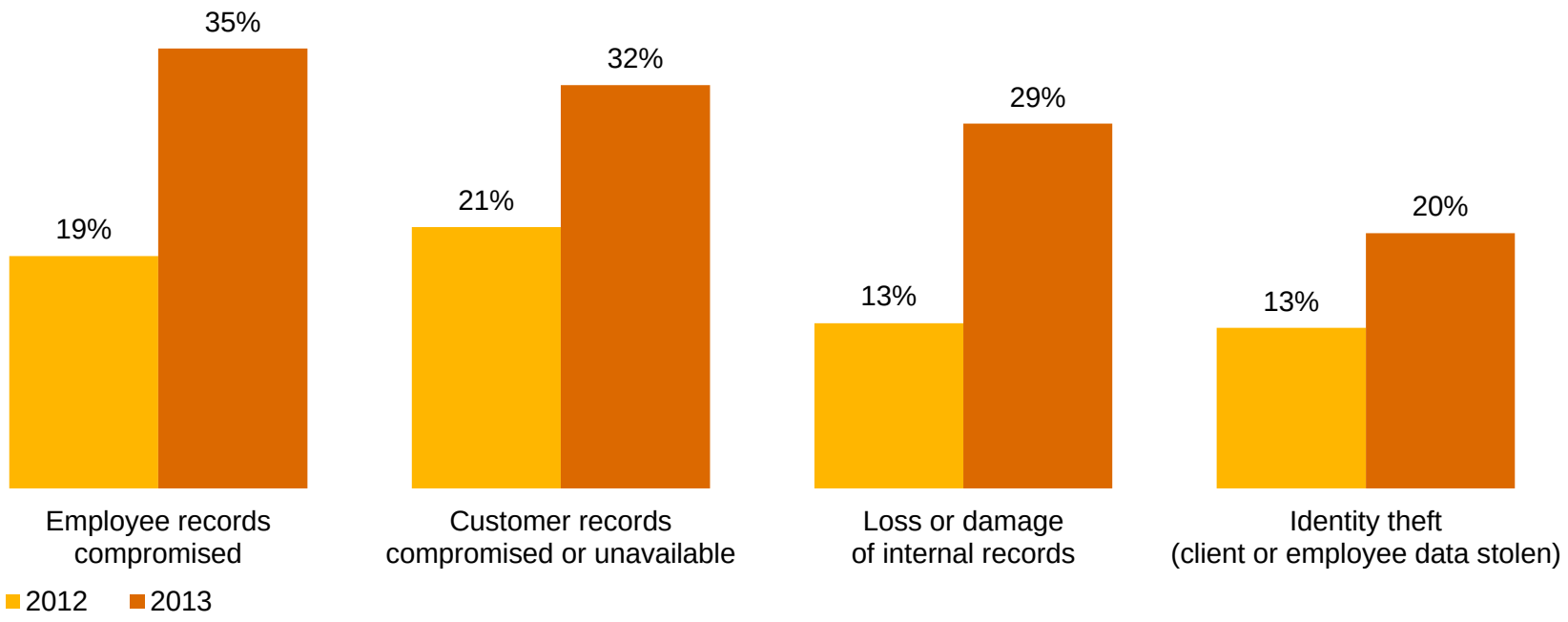
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

R&C respondents report increases in data loss as a result of security incidents.

Compromise of employee and customer records is up sharply this year, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records more than doubled over 2012.

Impact of security incidents

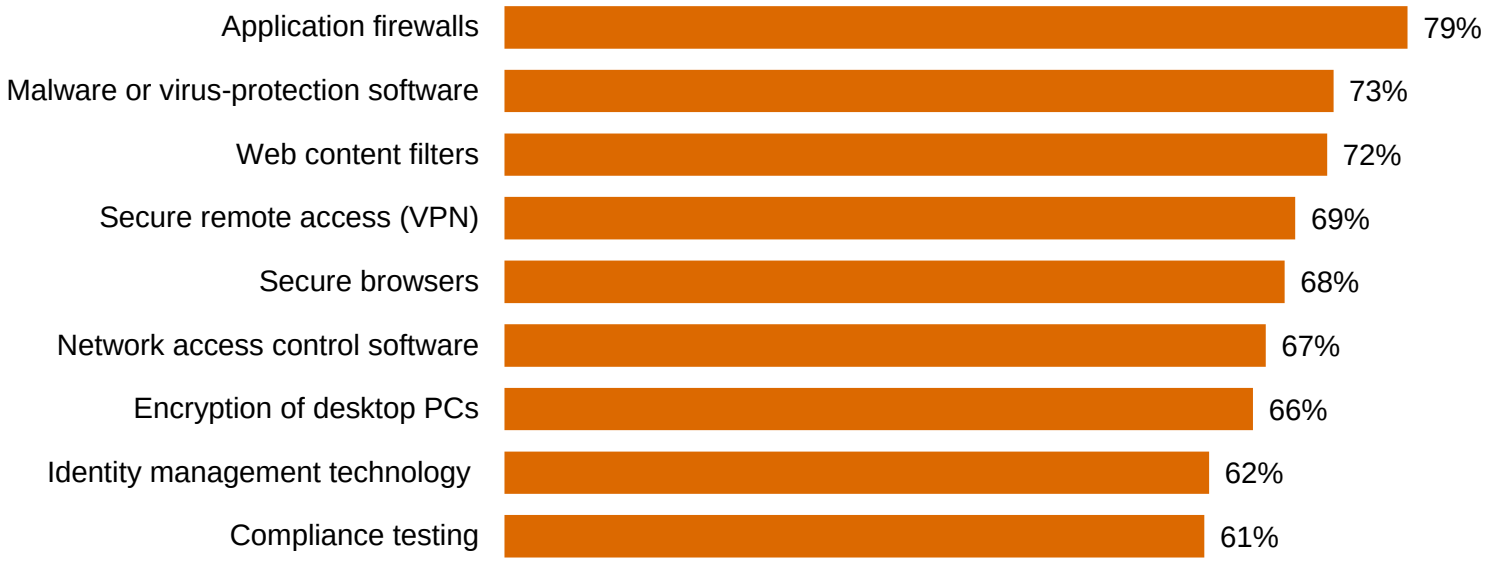


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

Information security safeguards and processes currently in place

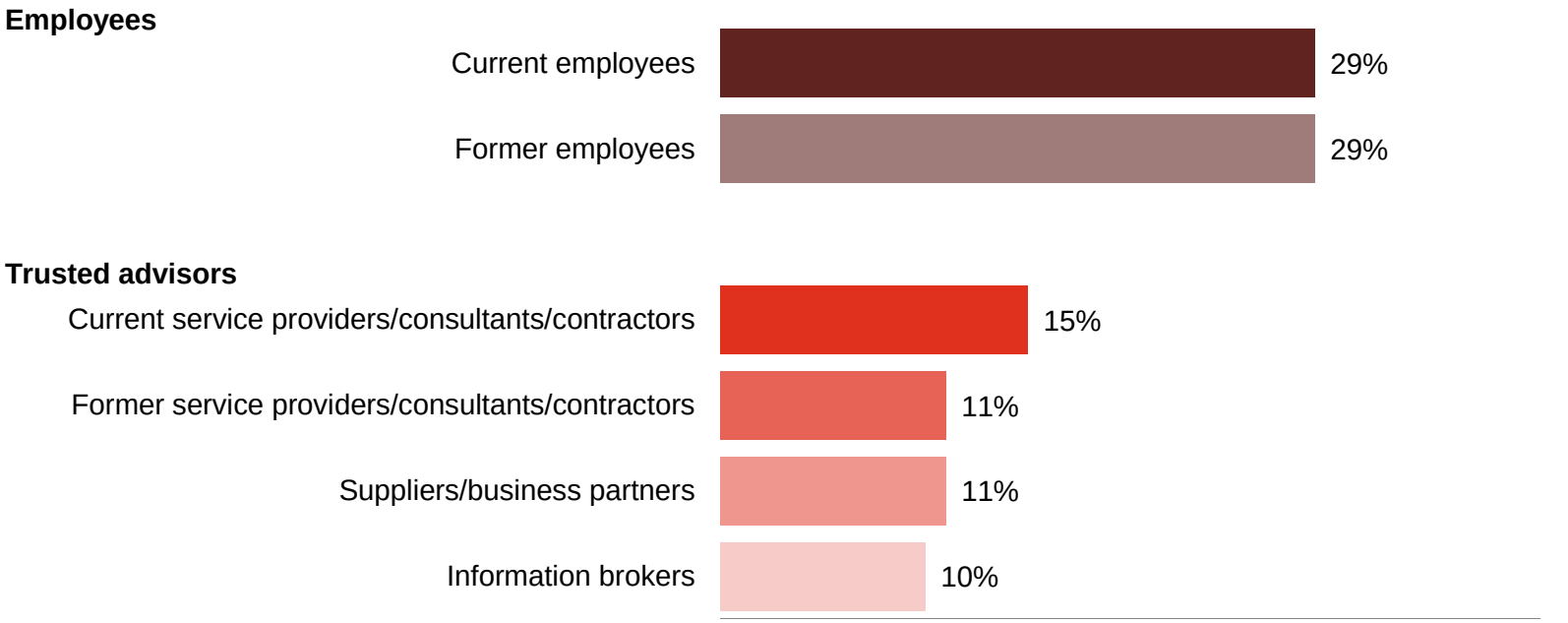


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most R&C respondents.

While 57% of R&C respondents say they monitor user compliance with security policies, the high turnover rate in the industry may be attributed to elevated employee security incidents.

Estimated likely source of insider incidents

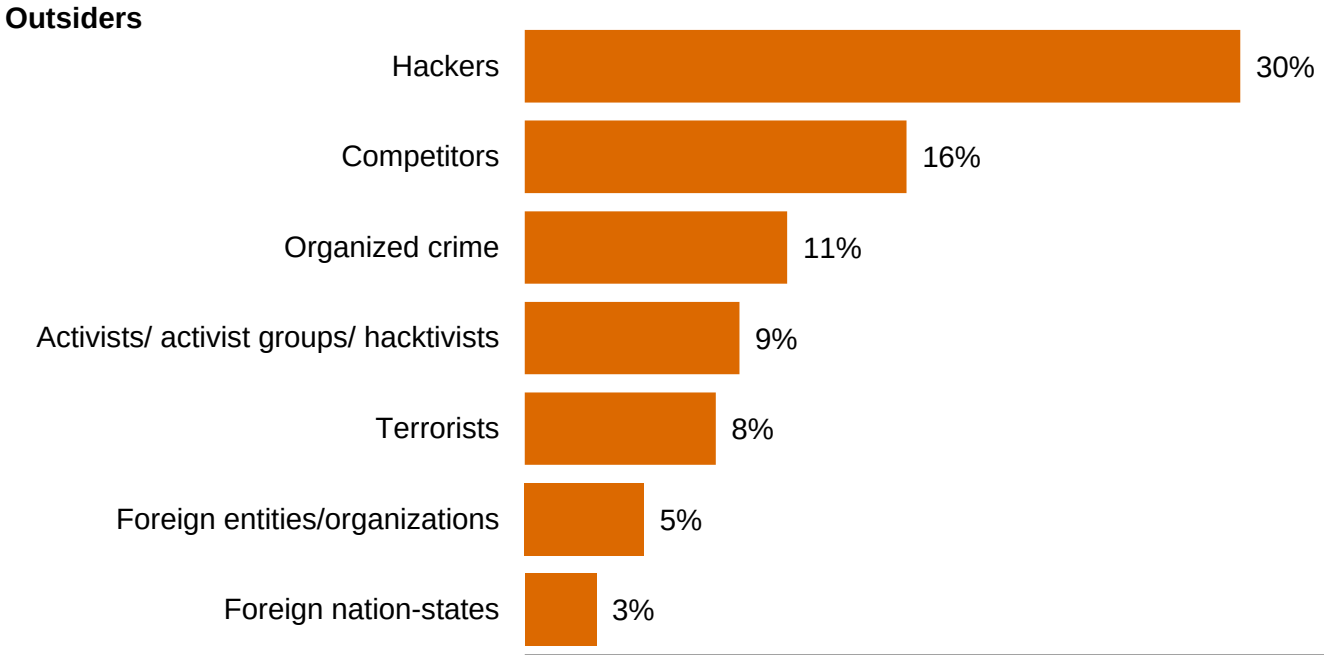


Question 21: “Estimated likely source of incidents” Question 14: “What process information security safeguards does your organization currently have in place? (Not all factors shown.)

While attacks backed by nation-states make headlines, R&C companies are more likely to be hit by other outsiders.

Only 3% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger.

Estimated likely source of outsider incidents



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

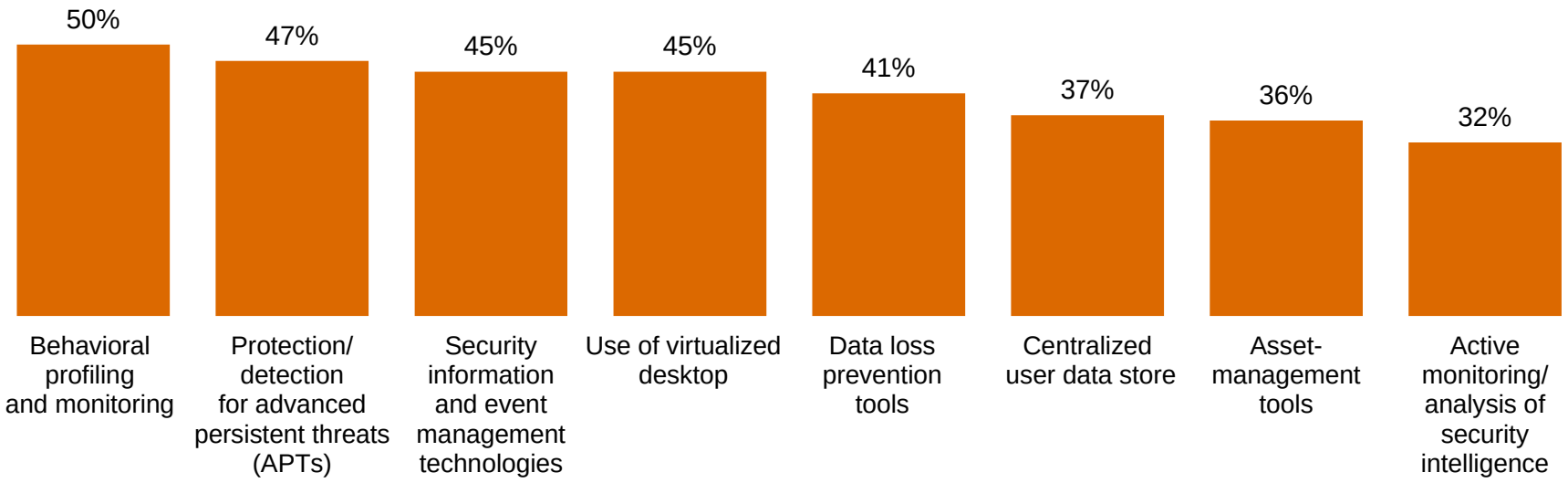
Section 4

A weak defense against adversaries

Many R&C companies have not implemented technologies that can provide better insight into today's risks.

Security safeguards that monitor data, assets, and events are less likely to be in place than traditional safeguards. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place

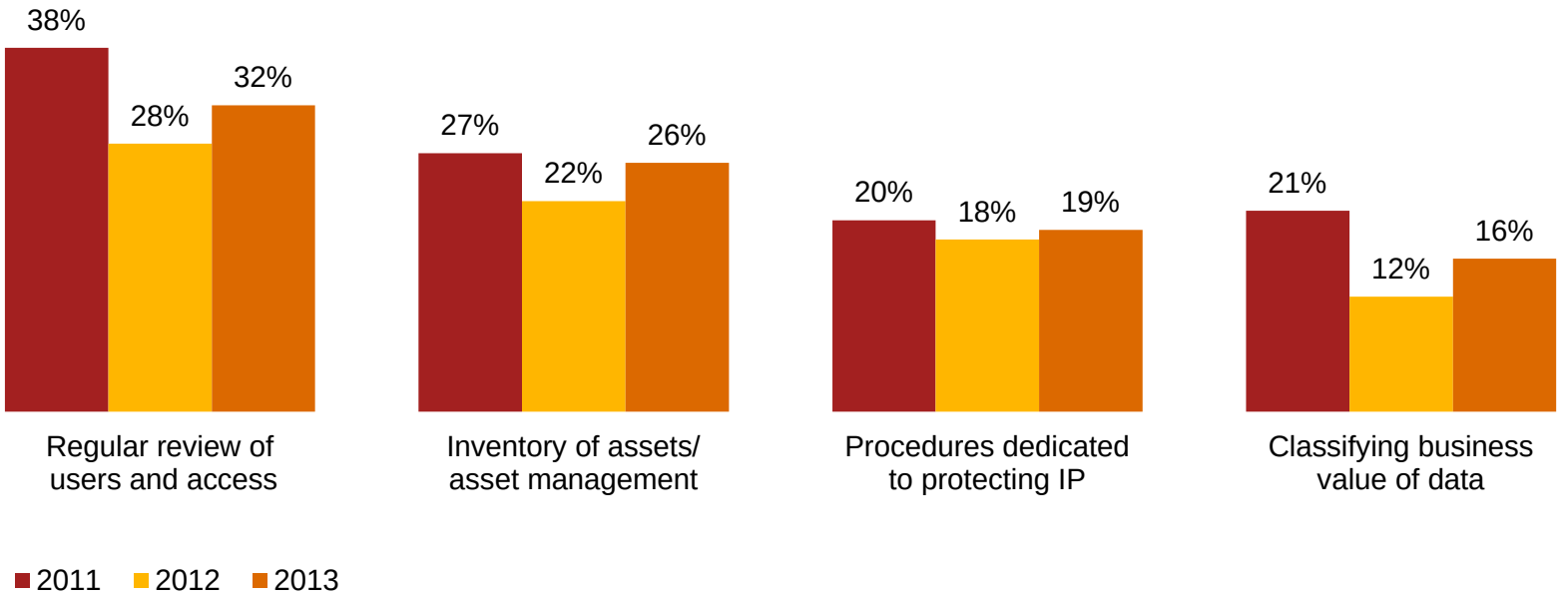


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite the potential consequences, most R&C companies do not adequately define and inventory high-value data.

It is imperative that organizations identify, prioritize, and protect their "crown jewels." Most R&C respondents, however, have not inventoried their data assets or classified the business value of data.

Have policies to help safeguard IP and trade secrets

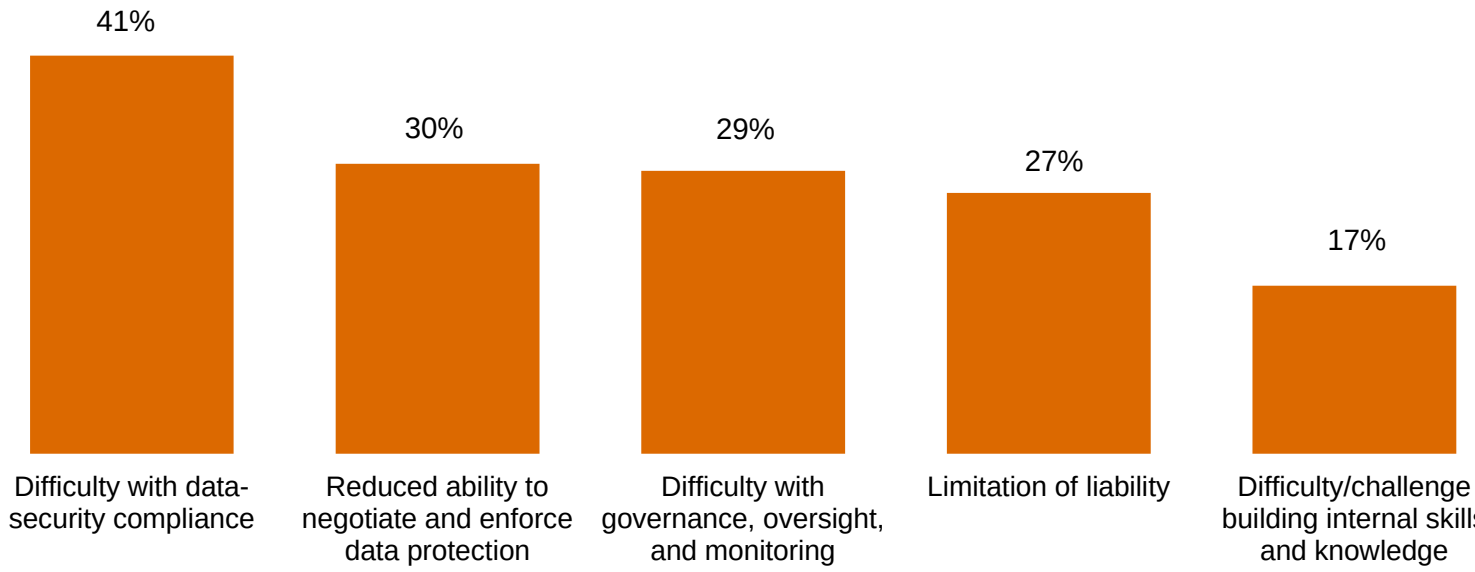


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

44% of R&C companies use cloud computing, but they often do not include cloud in their security policies.

Among those that do use cloud services, 54% report improved information security—but only 14% include provisions for cloud in their security policy. Top challenges to cloud use include compliance, enforcement of data protection, and governance.

Potential issues regarding use of third-party cloud environments

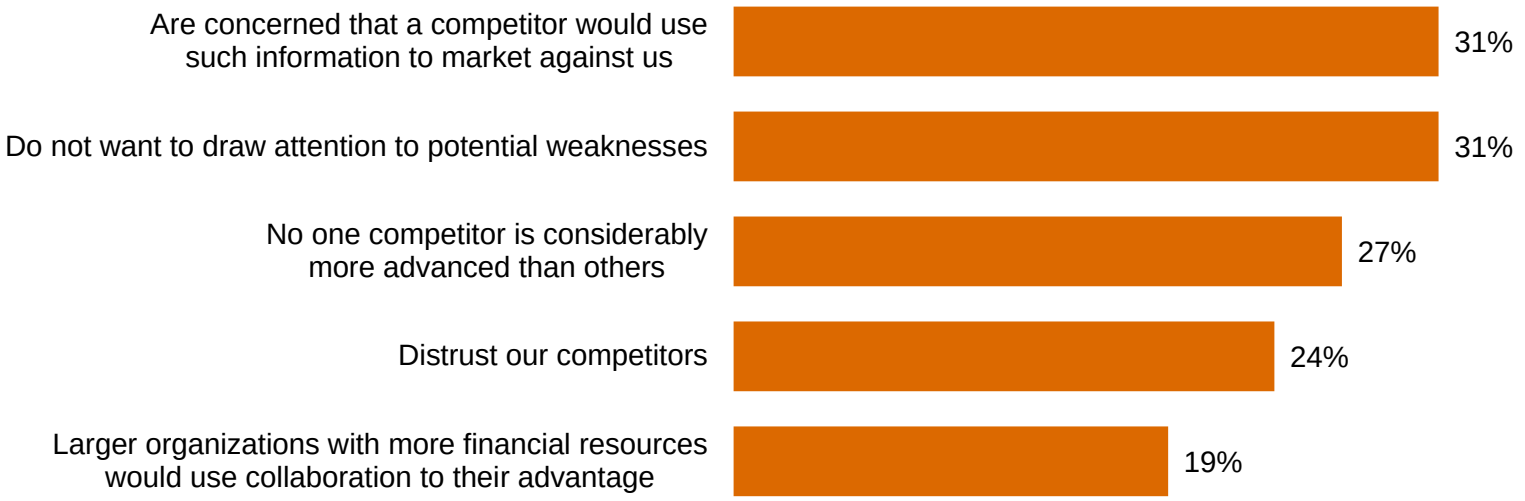


Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.) (Asked only of retail and consumer respondents) Question 2: “What potential issues does your organization face regarding third-party cloud environments?” (Not all factors shown.)

29% of R&C respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.[1]

Reasons for not collaborating on information security



[1] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

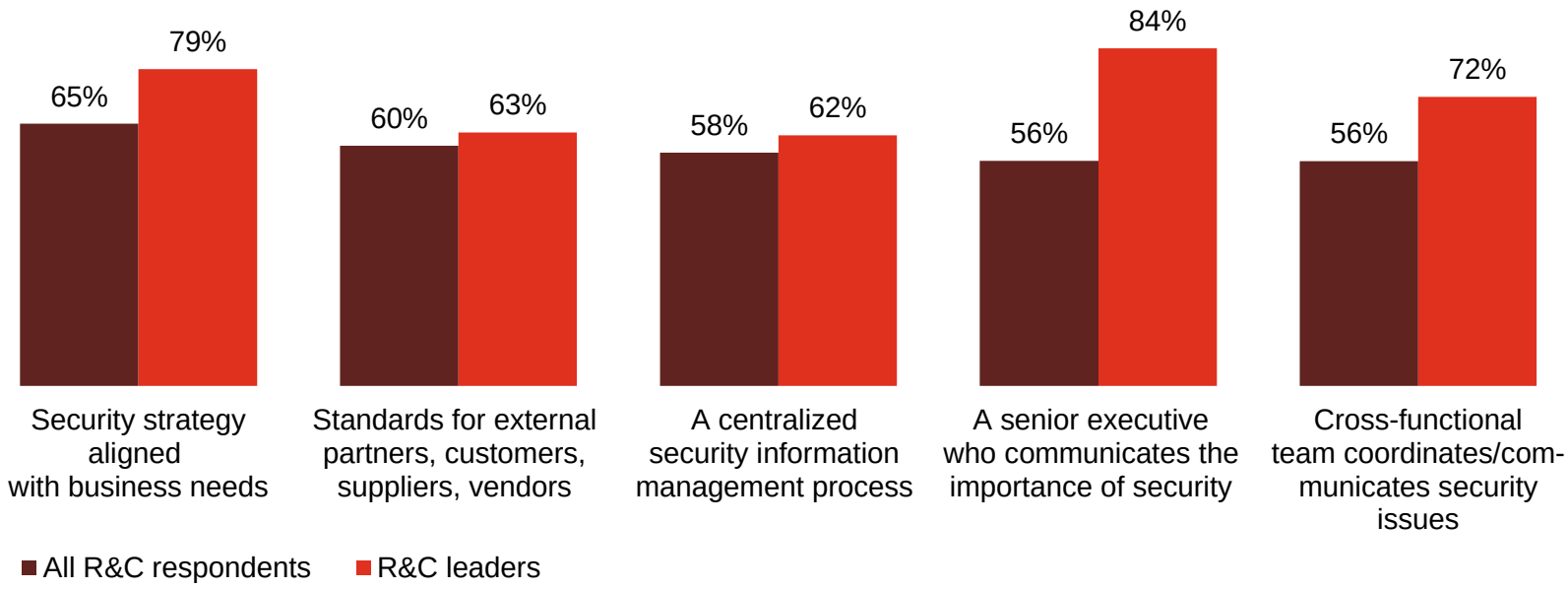
Section 5

Preparing for the threats of tomorrow

R&C leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT challenge.

R&C leaders show higher levels of support from senior executives to drive business alignment and integration.

Security policies and safeguards currently in place: All respondents vs. leaders



Question 14: "What process information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?"

Many R&C companies have invested in technology to secure their ecosystems against today's evolving threats.

Leaders are more likely to have implemented these technologies. But given today's elevated threat landscape, *all* organizations should strongly consider implementation of these safeguards.

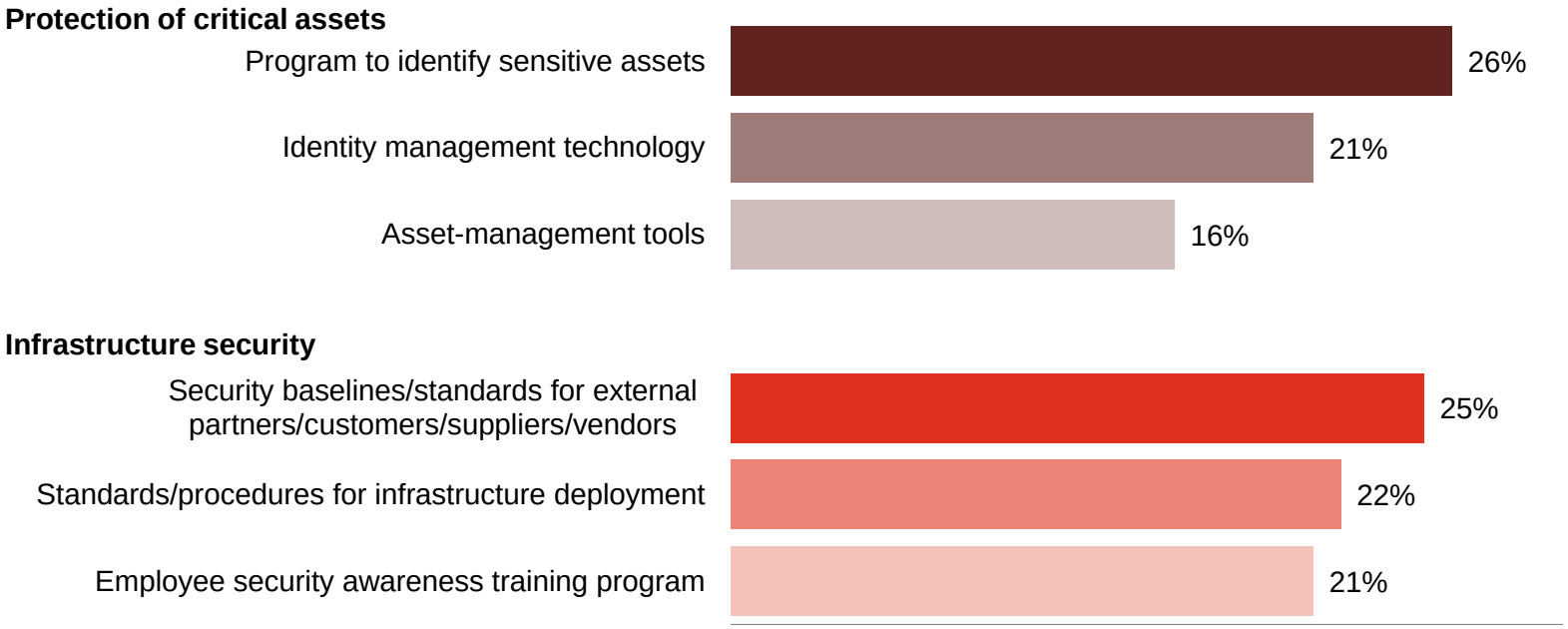
Technology safeguards currently in place	All R&C respondents	R&C leaders
Malicious code detection tools	74%	89%
Privileged user access	67%	77%
Intrusion prevention tools	66%	82%
Vulnerability scanning tools	64%	77%
User-activity monitoring tools	62%	73%
Security event correlation tools	58%	72%
Mobile device management	56%	65%
Encryption of smartphones	56%	69%
Federated identity management	51%	64%
Secure supply chain management solution	31%	36%

Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.) (Asked only of retail and consumer respondents.) Question 4: "Do you plan to implement a secure supply chain management solution?" (Respondents who answered "Already in place").

What business imperatives and processes will R&C respondents prioritize this year?

Some of the highest priorities cited by R&C respondents include technologies that can help the company protect its most valuable assets and set security standards for third parties.

Safeguards not in place but a top priority over the next 12 months

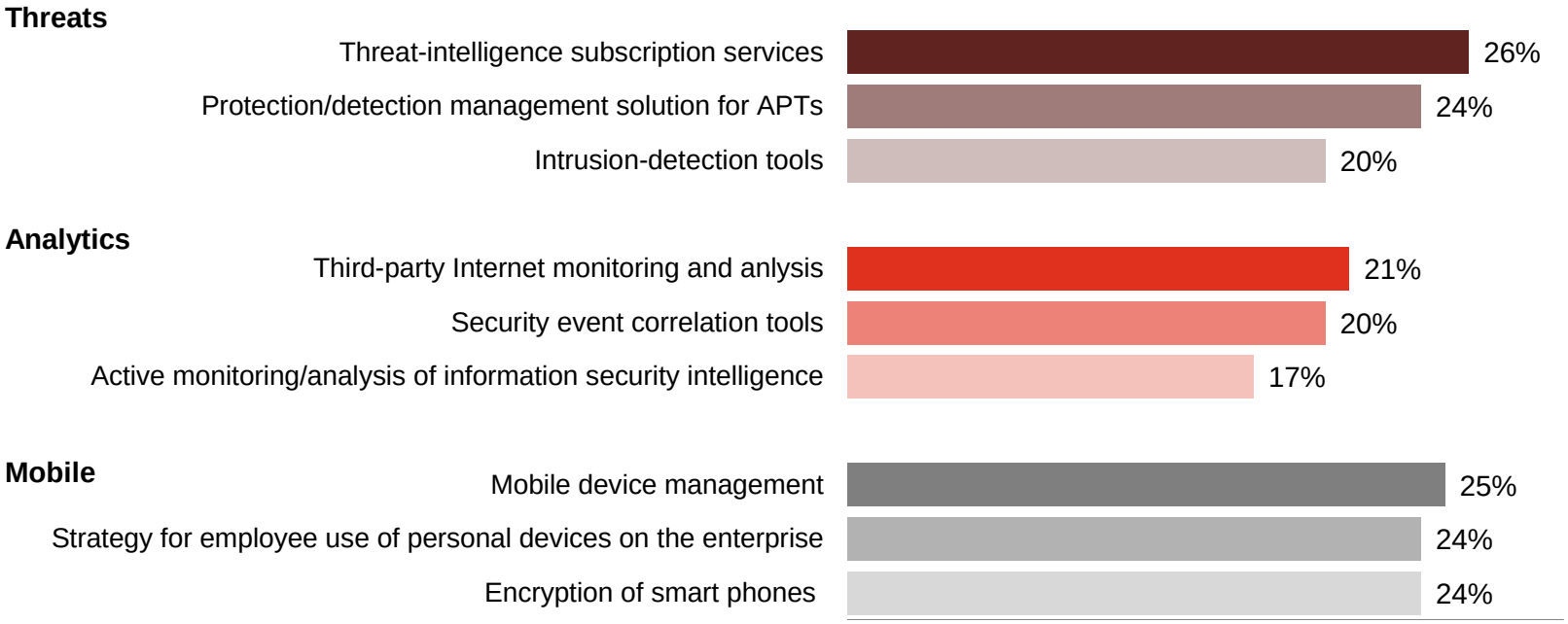


Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?"
Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and R&C organizations are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Effective security demands that organizations align policies and spending with business objectives.

This year, more R&C respondents say security policies and spending are aligned with business objectives. This suggests they understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

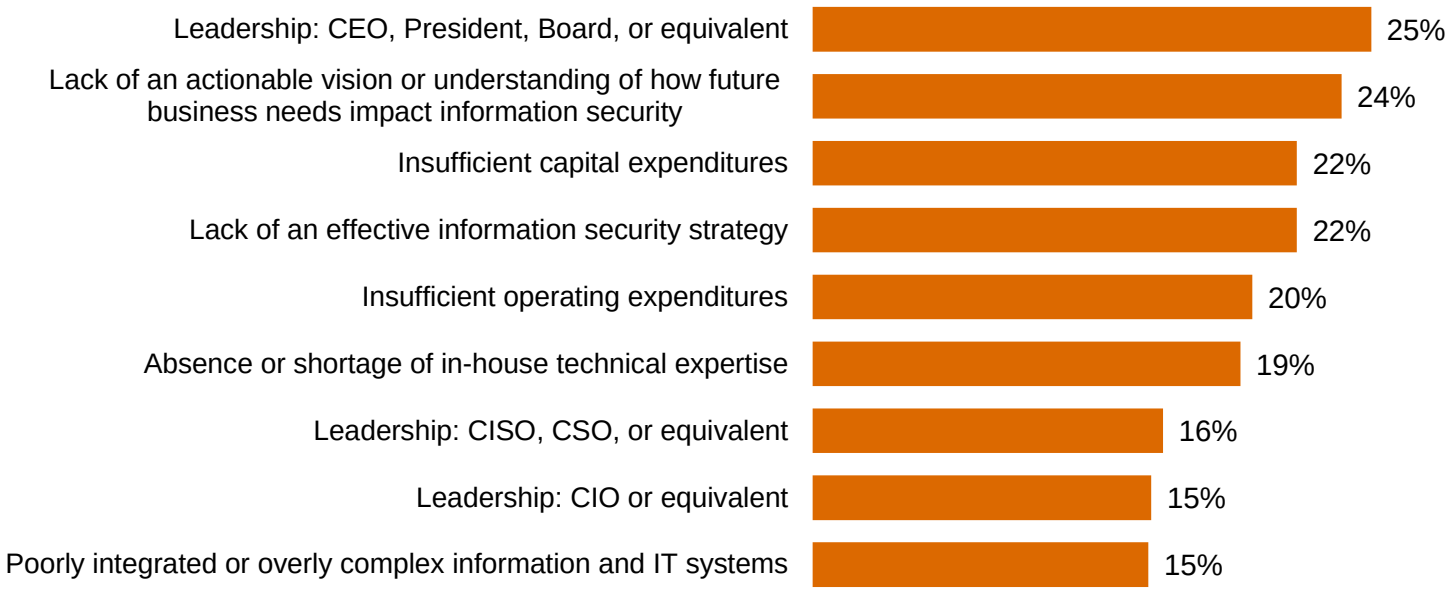
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

Committed leadership, vision, and more money are needed to advance security.

Effective security requires the support of top executives—particularly the CEO—and an informed security vision that is aligned with future business needs.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
+1 949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
+1 646.471.5731
mark.a.lobel@us.pwc.com

US Retail & Consumer Contacts

Lisa Dugal
Principal
+1 646.471.6916
lisa.feigen.dugal@us.pwc.com

Pieter Penning
Principal
+1 678.419.1094
peter.penning@us.pwc.com

Paul Ritters
Director
+1 612.596.6356
paul.j.ritters@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

PwC

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

Technology

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents evolve in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global technology industry are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Detected security incidents have declined slightly and confidence is high.

But while many technology organizations have raised the bar on security, their adversaries have done better.

The financial costs of security incidents are up, while threats are constantly multiplying and evolving. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many technology executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few technology companies have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that technology companies identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the organizational strategy, one that is championed by business leadership and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

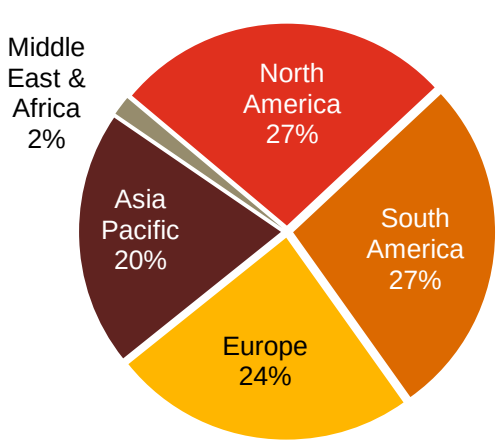
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

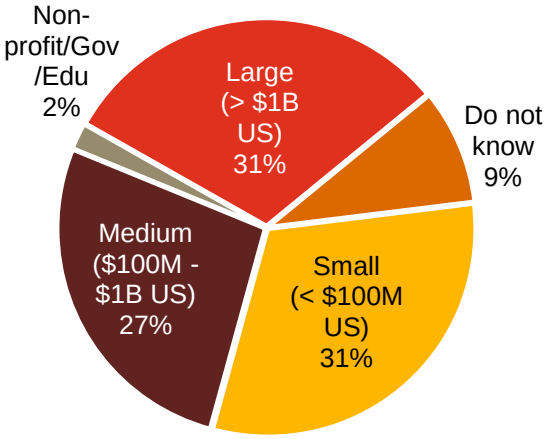
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 1,226 respondents from the technology industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

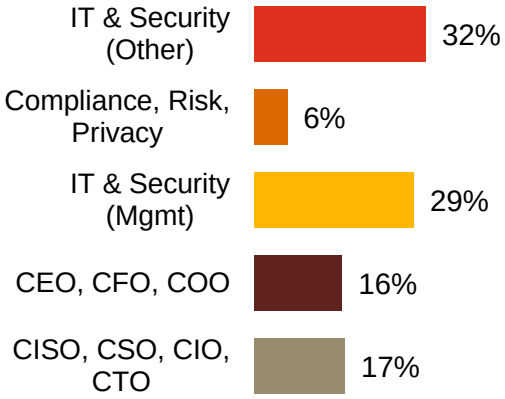
Technology respondents by region of employment



Technology respondents by company revenue size



Technology respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

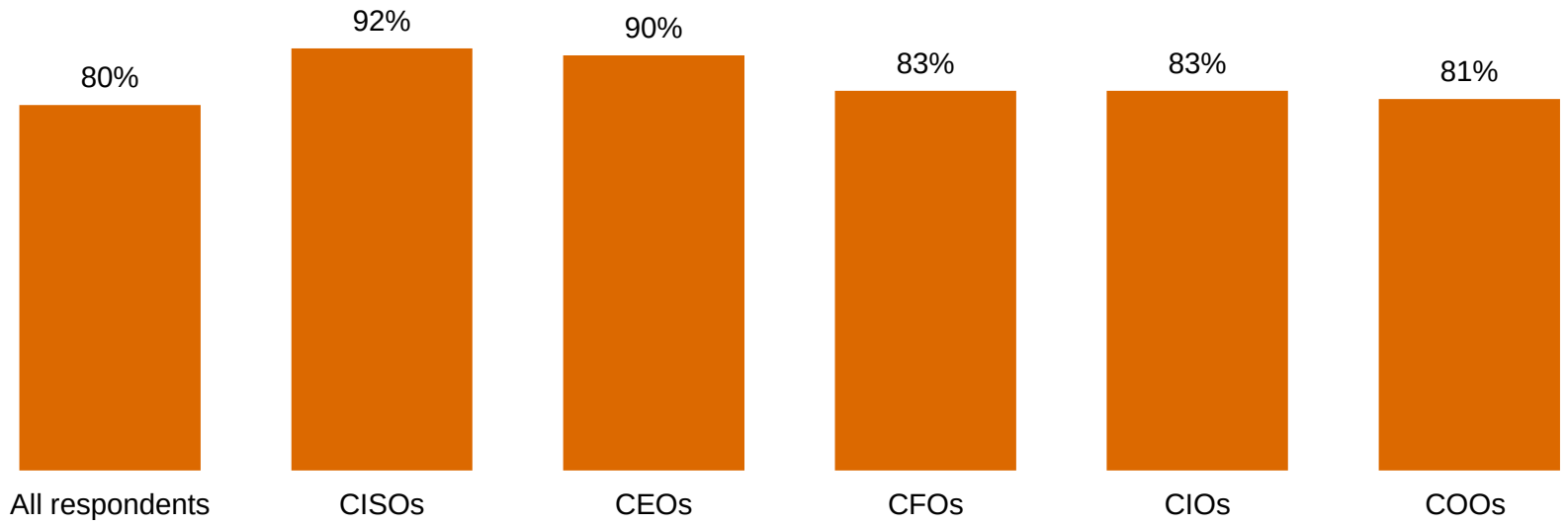
Section 2

Confidence in an era of advancing risks

80% of technology respondents say their security activities are effective, and top executives are even more confident.

In the C-suite,* 90% of CEOs say they are confident in their security program. CISOs report the highest level of confidence.

Executive confidence in effectiveness of security activities (somewhat or very confident)

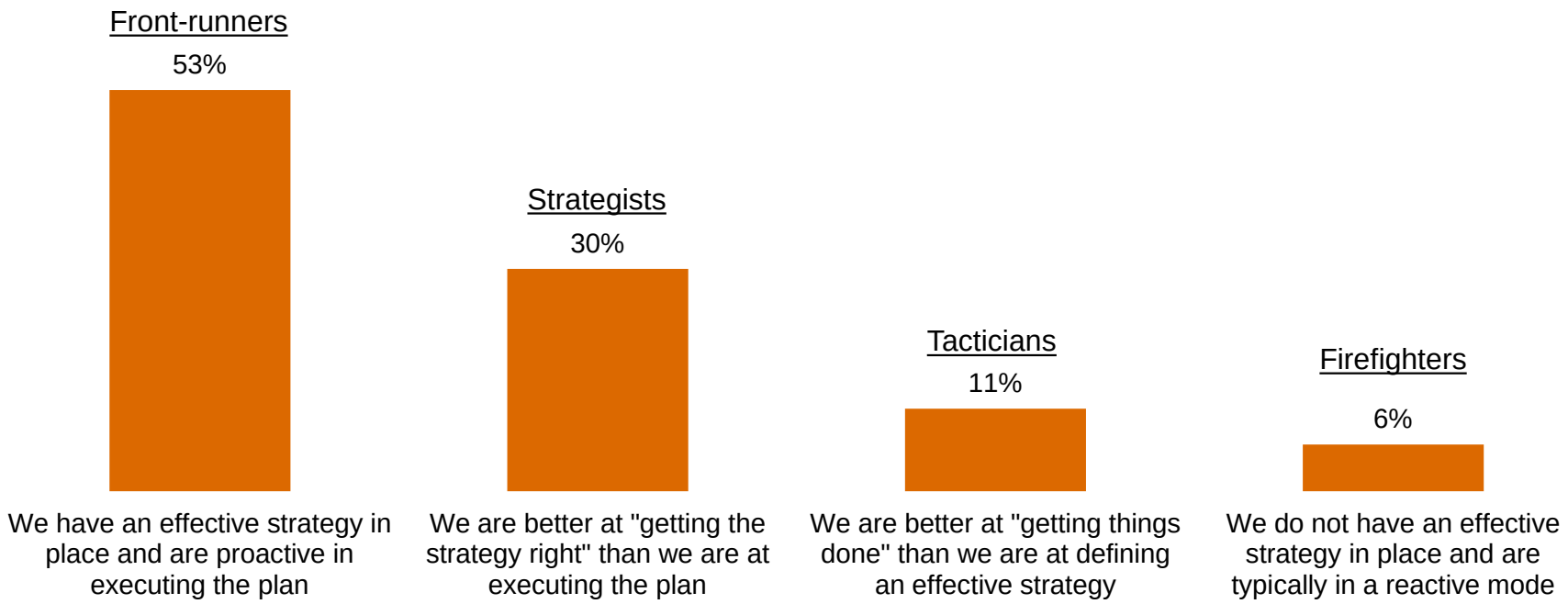


* CEOs, CFOs, and COOs

Question 39: “How confident are you that your organization’s information security activities are effective?” (Respondents who answered “Somewhat confident” or “Very confident.”) Question 1: “My job title most closely resembles”

53% of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

More than half of technology respondents say they have an effective strategy in place and are proactive in executing the plan, up slightly over last year. Almost one in three (30%) say they are better at getting the strategy right than executing the plan.



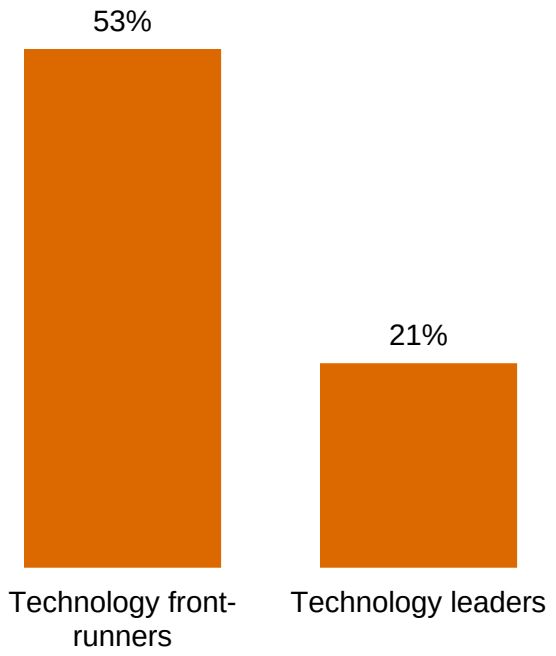
Question 27: "Which statement best characterizes your organization's approach to protecting information security?"

But closer scrutiny reveals far fewer real leaders than front-runners.

We measured technology respondents' self-appraisal against four key criteria to filter for leadership. To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are significantly fewer real leaders than self-identified front-runners.

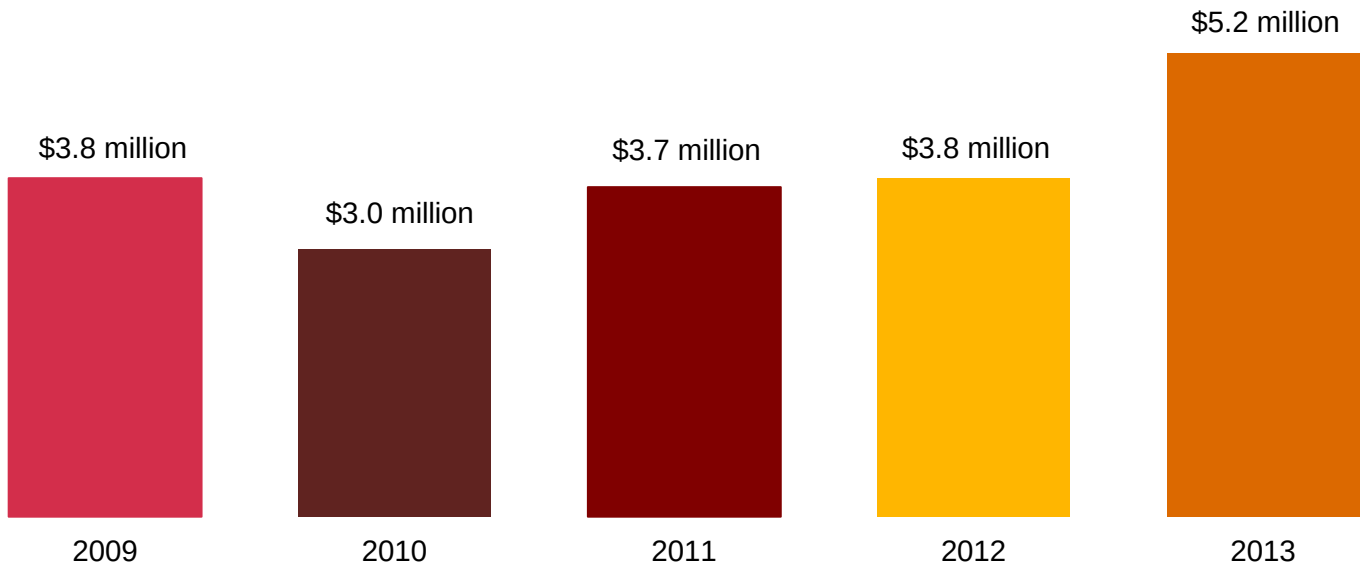


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Technology respondents' security budgets have increased substantially.

Security budgets average $5.2 million this year, a gain of 39% over 2012. Technology companies appear to understand that today's elevated threat landscape demands a substantial boost in security investment.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

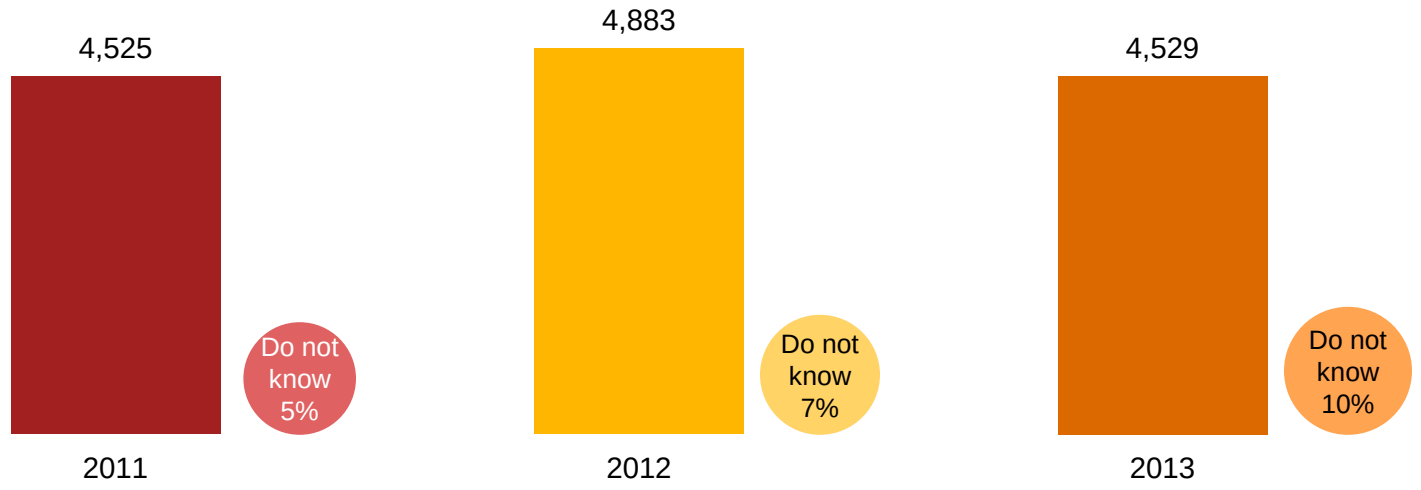
Section 3

Today's incidents, yesterday's strategies

*Technology companies detect fewer security incidents.**

The number of incidents detected by technology respondents decreased 7% over last year, perhaps an indication of the industry's implementation of sophisticated tools. Average financial losses are up 15% over last year, not surprising given the cost and complexity of responding to incidents.

Average number of security incidents in past 12 months



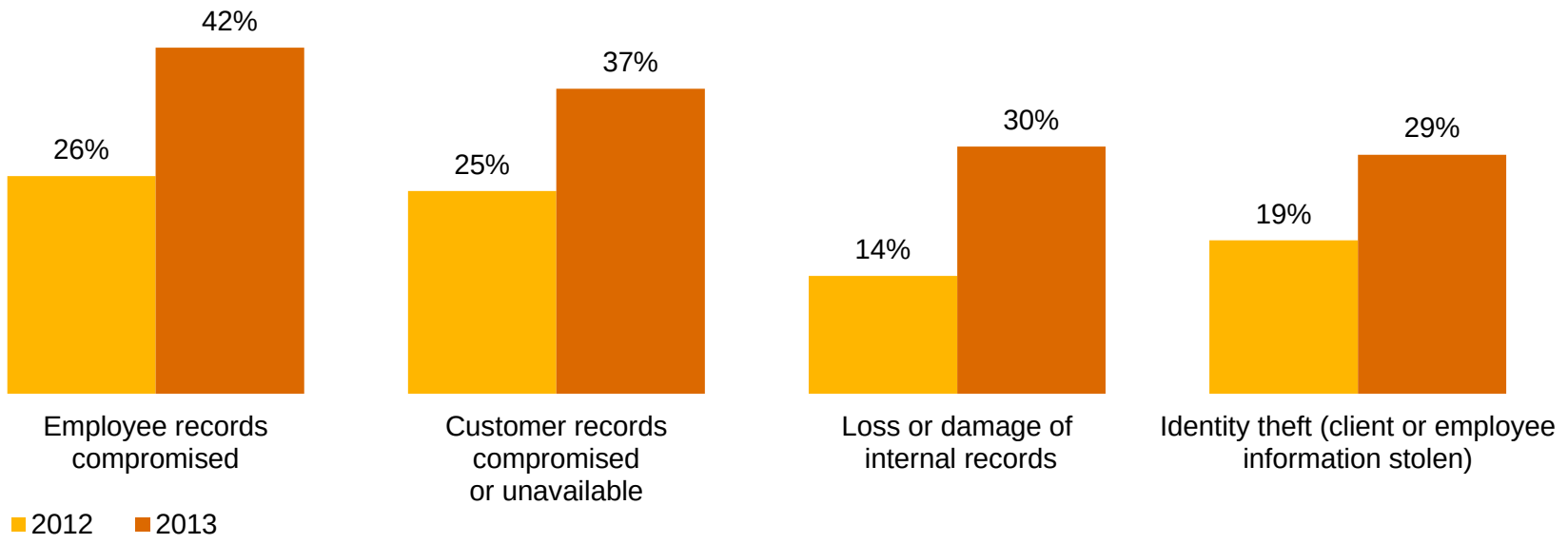
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

Technology respondents report an increase in data loss as a result of security incidents.

Compromise of employee and customer records are up sharply this year, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records more than doubled over 2012.

Impact of security incidents

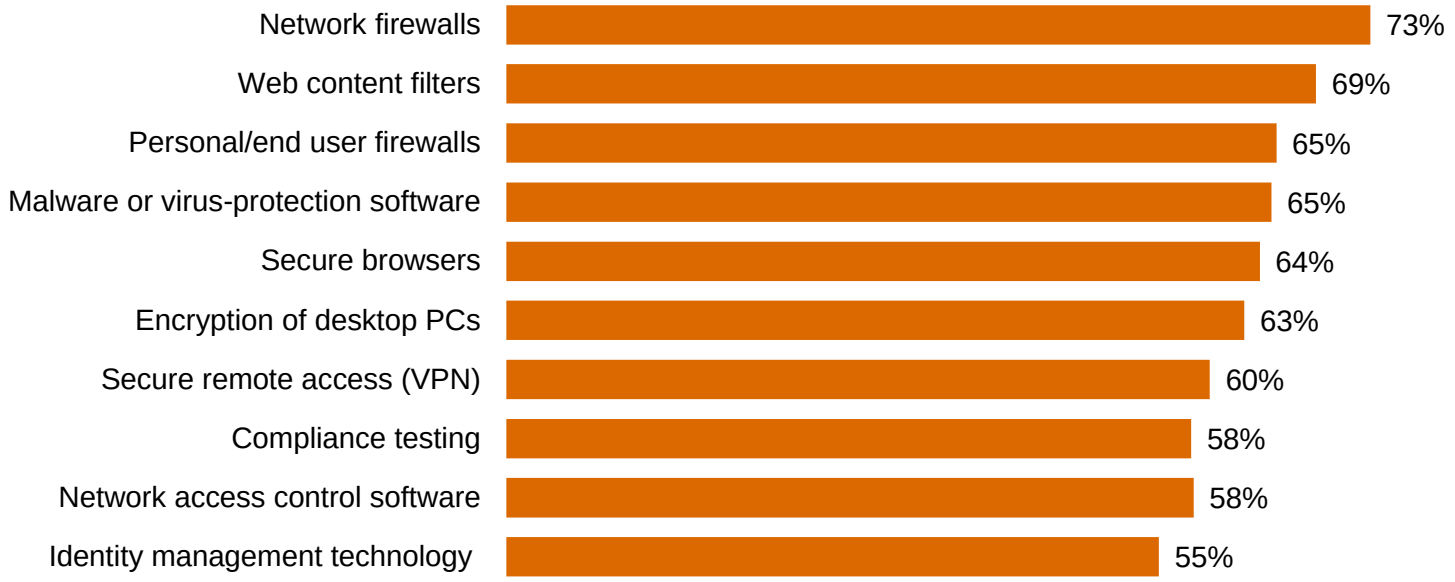


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

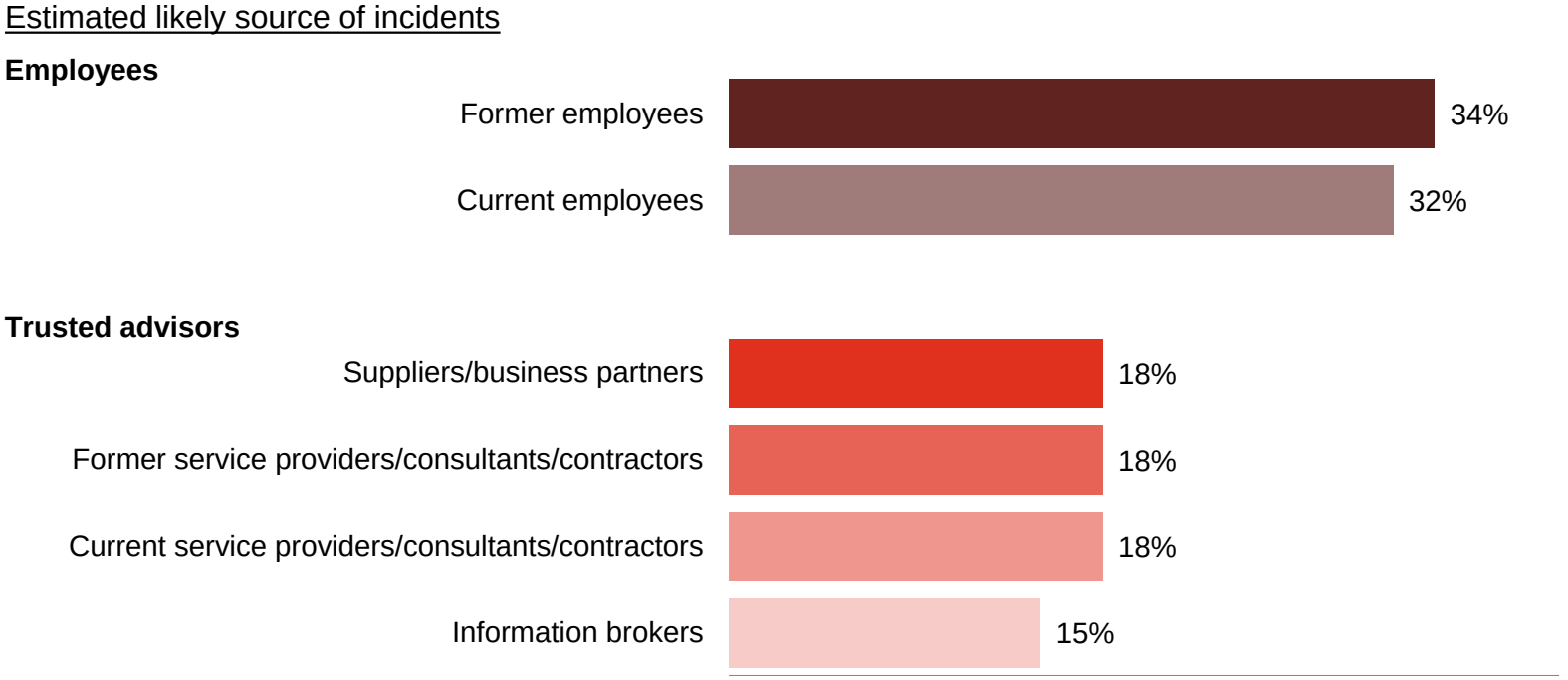
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most technology respondents.

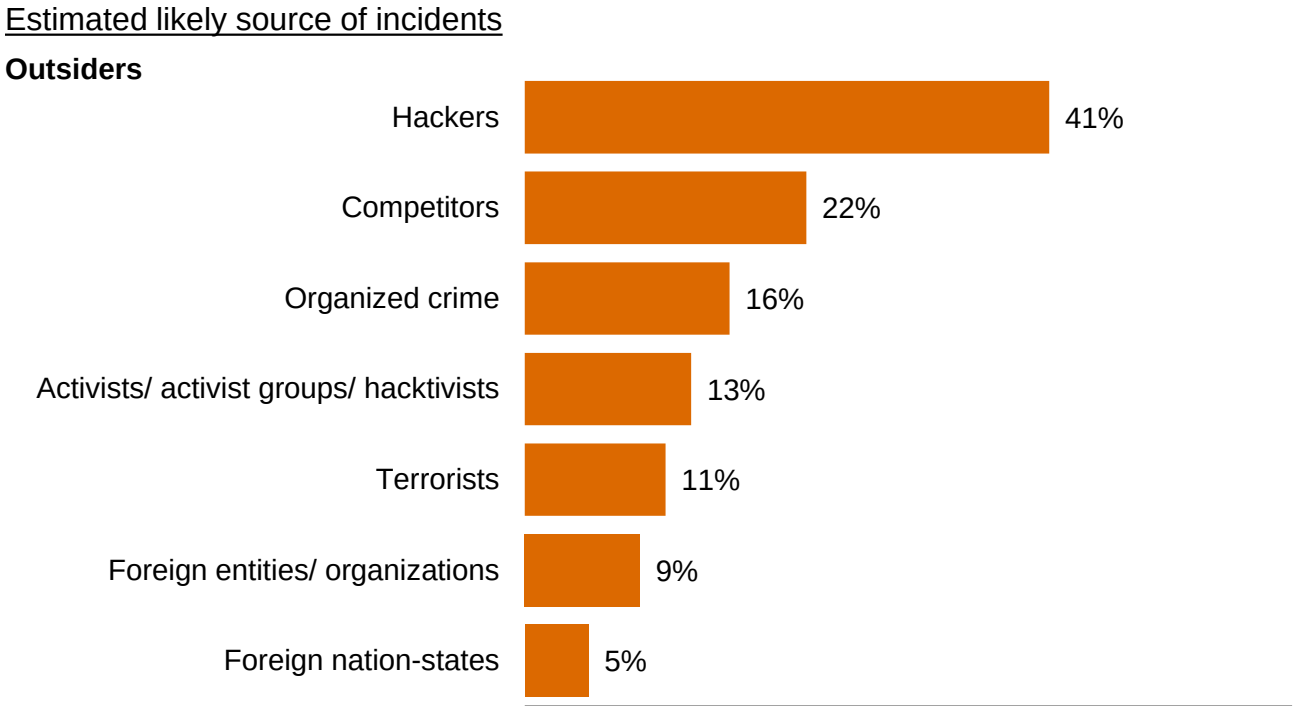
It's the people you know—current and former employees, as well as other insiders—who are most likely to perpetrate security incidents.



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, tech companies are more likely to be hit by other outsiders.

Only 5% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

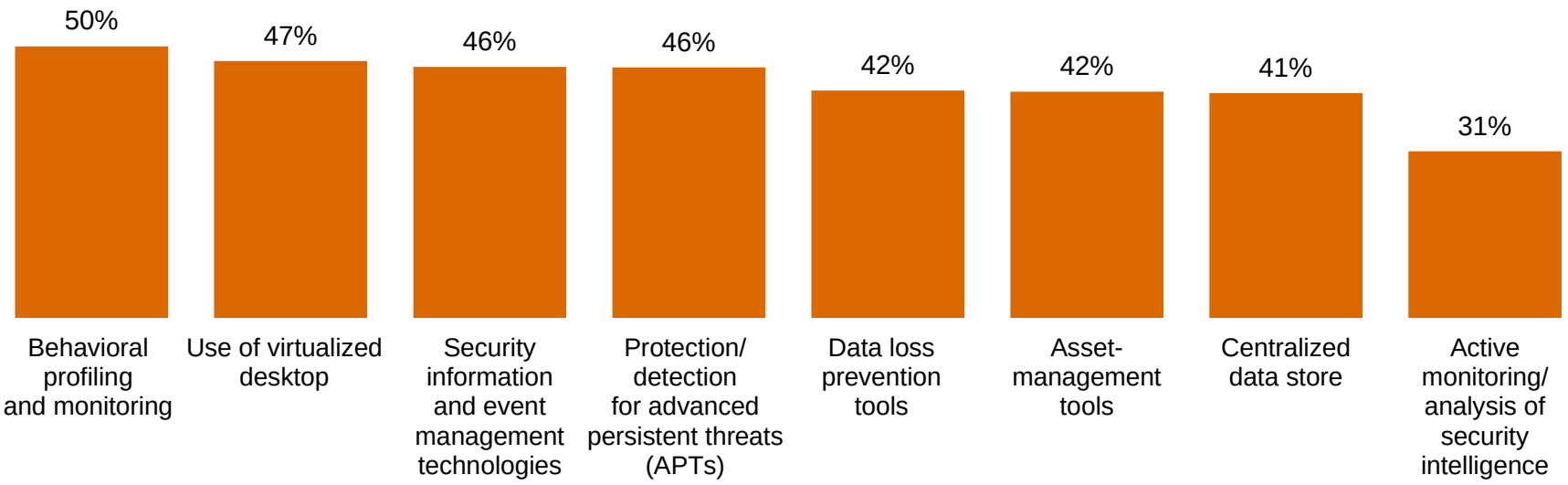
Section 4

A weak defense against adversaries

Many technology companies have not implemented technologies that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place than traditional technologies. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place

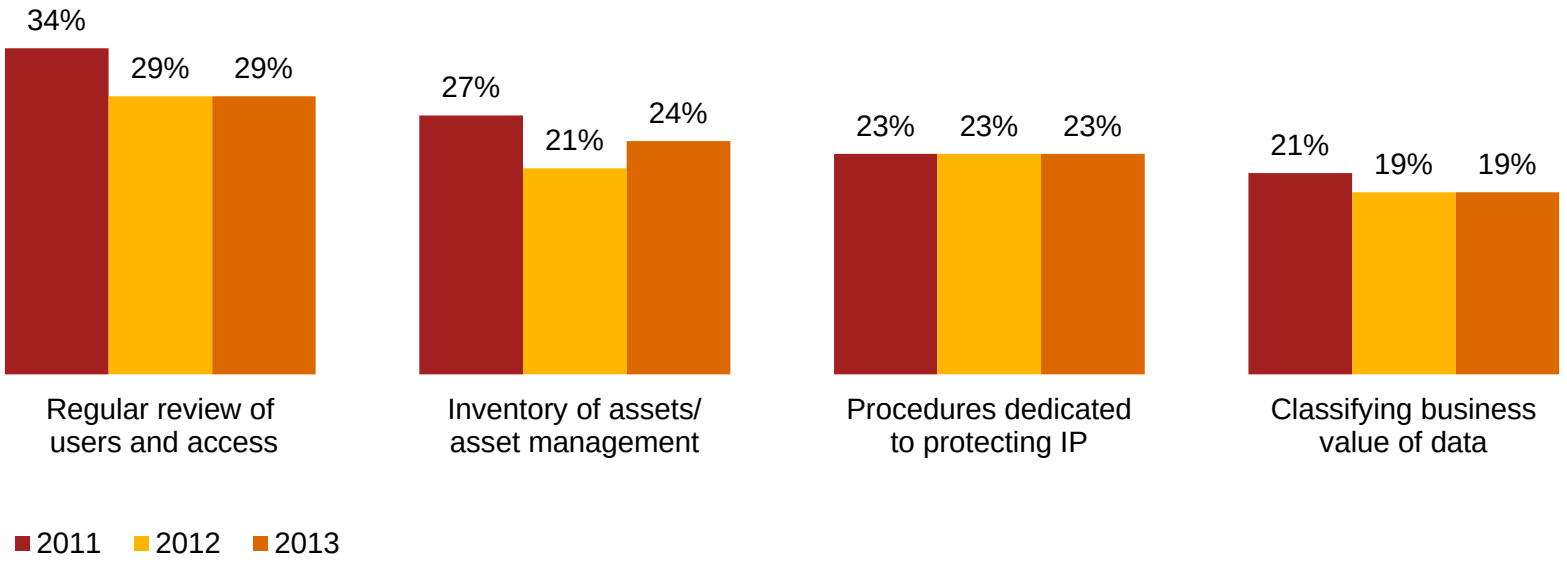


Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite the potential consequences, many tech companies do not adequately safeguard their high-value information.

It is imperative that organizations identify, prioritize, and protect their "crown jewels." Many technology respondents, however, have not yet implemented basic policies necessary to safeguard intellectual property (IP).

Have policies to help safeguard IP and trade secrets

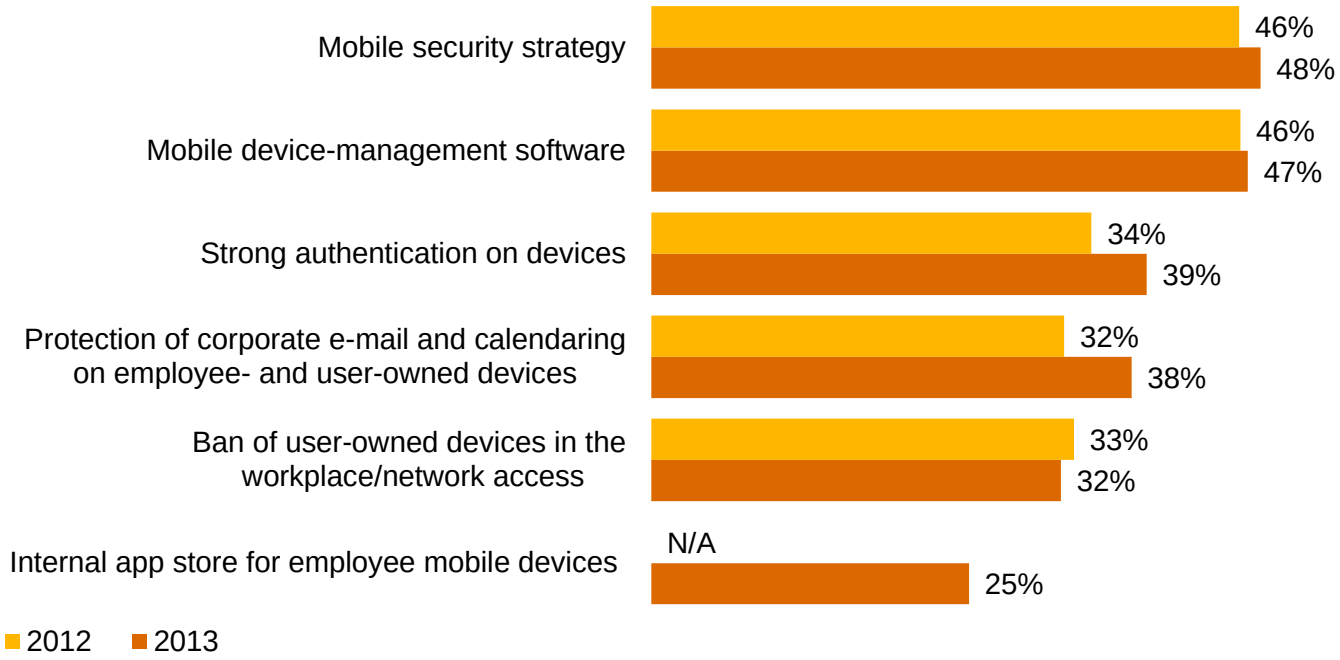


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet technology companies' efforts to implement mobile security programs do not show significant gains over last year, and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

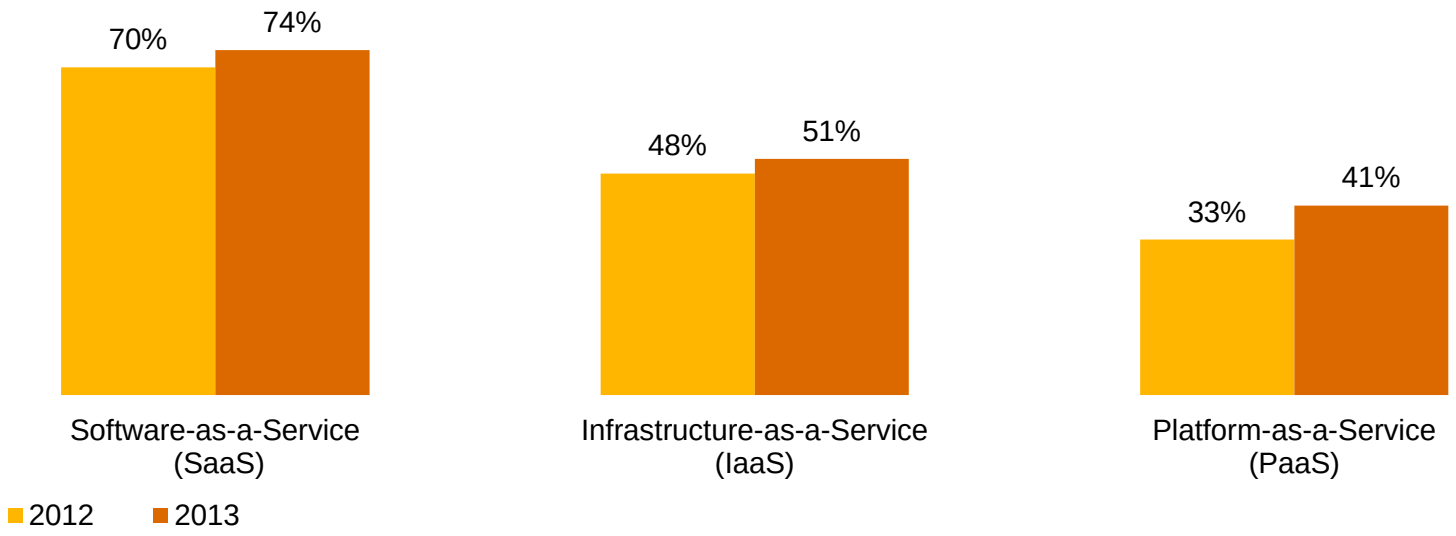


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

61% of technology respondents use cloud computing, but they often do not include cloud in their security policies.

While more than half of respondents use cloud computing—and 65% report better information security as a result—only 22% include provisions for cloud in their security policy. SaaS remains dominant, while PaaS shows growth.

Type of cloud service used



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

24% of respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.[1]

Reasons for not collaborating on information security

[1] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

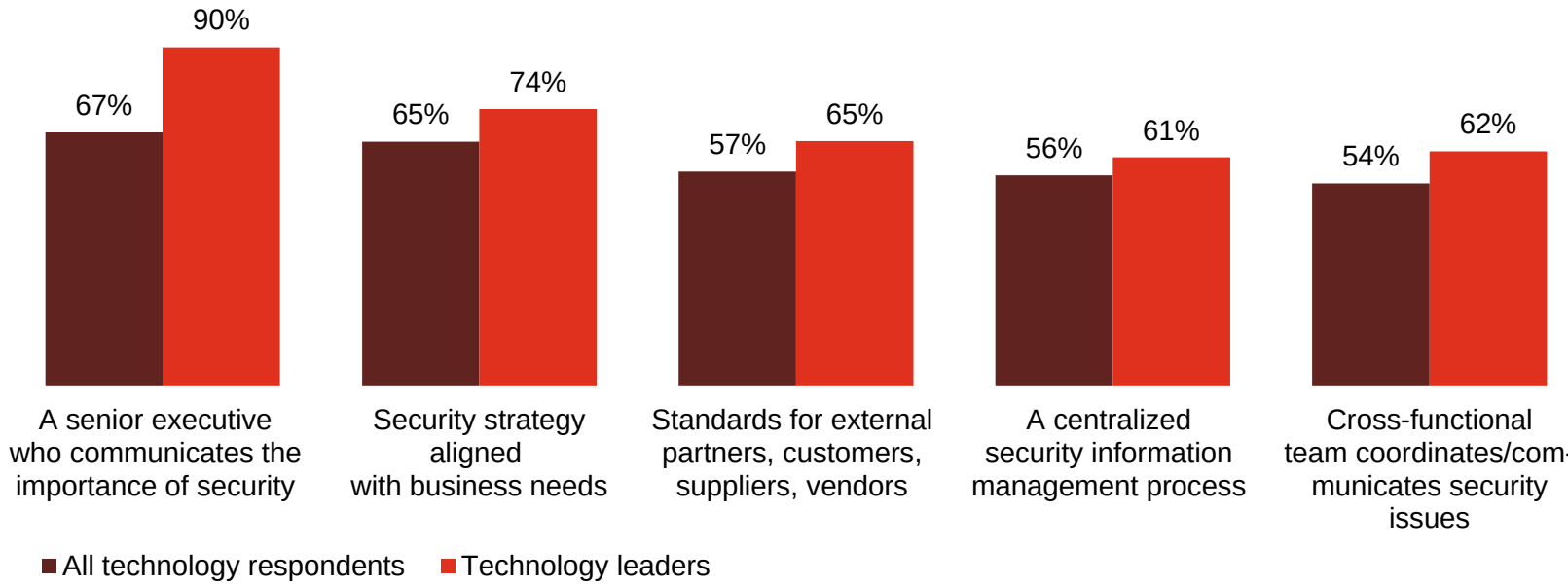
Section 5

Preparing for the threats of tomorrow

Tech leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT challenge.

Better communications, aligning security with business needs, and setting standards for external partners show leaders, in particular, are rethinking the fundamentals of security.

Security policies and safeguards currently in place: All respondents vs. leaders



Question 14: "What process information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?"

Many organizations have invested in technology safeguards to secure their ecosystems against today's evolving threats.

Leaders are more likely to have implemented these technologies. But given today's elevated threat landscape, *all* organizations should strongly consider implementation of these safeguards.

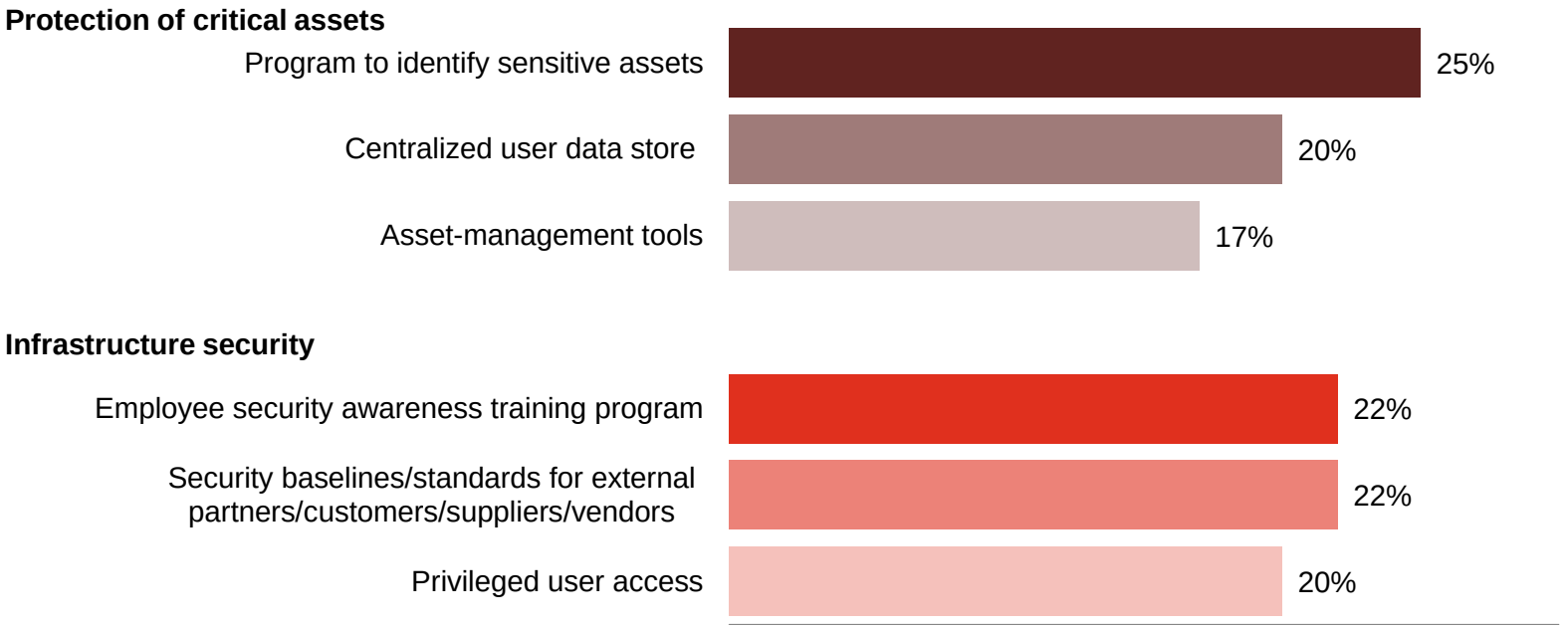
Technology safeguards currently in place	All technology respondents	Technology leaders
Malicious code detection tools	77%	91%
Tools to discover unauthorized devices	64%	76%
Intrusion detection tools	64%	73%
Vulnerability scanning tools	62%	70%
Mobile device malware detection	57%	65%
User-activity monitoring tools	56%	63%
Identity management technology	55%	66%
Code analysis tools	53%	63%
Offensive technologies	52%	60%

Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

What business imperatives and processes will technology companies prioritize this year?

Some of the highest priorities cited by respondents include safeguards that can help the organization protect its most valuable assets and safeguard the infrastructure.

Safeguards not in place but a top priority over the next 12 months

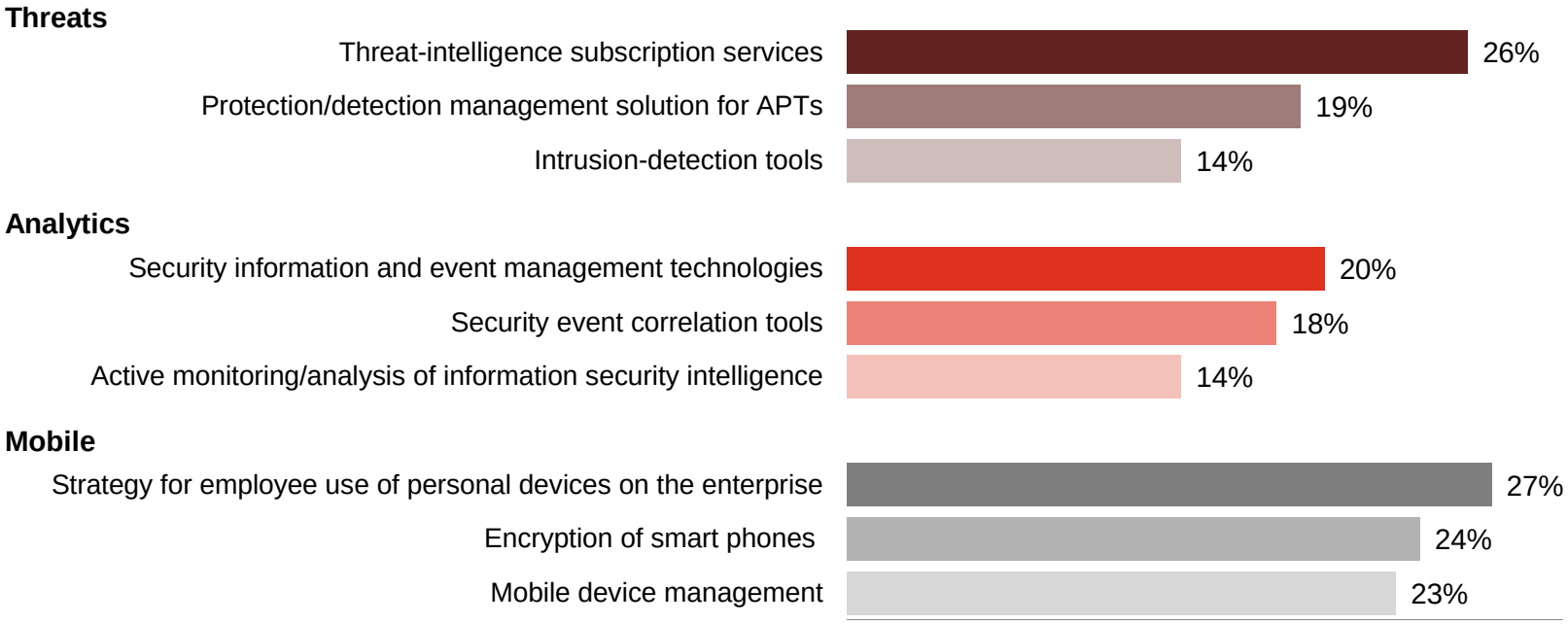


Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?"
Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and organizations are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Effective security also demands that organizations align policies and spending with business objectives.

This year, more technology respondents say security spending and policies are aligned with business objectives. This suggests they are starting to understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

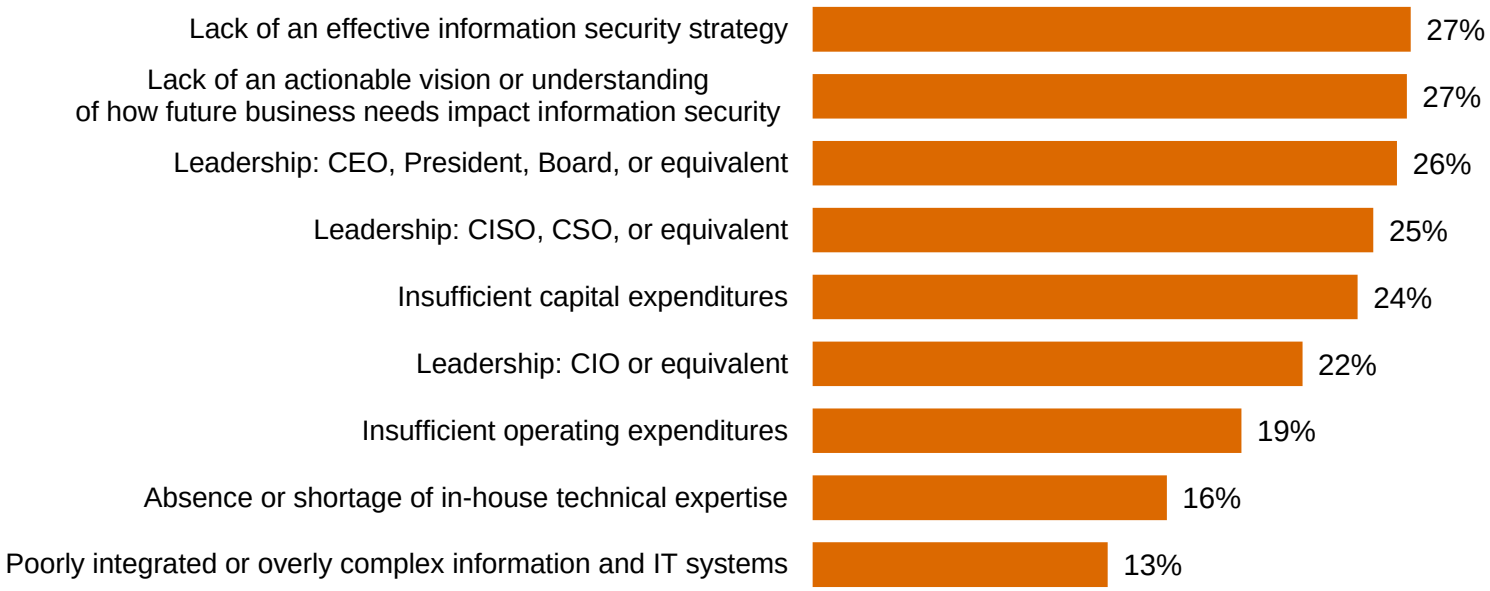
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

An effective strategy, informed vision, and committed leaders are needed to advance security.

An effective approach requires a strategy informed by the potential impact of future business needs on information security—and the support of the C-level executives.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are 10 key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
+1 949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
+1 646.471.5731
mark.a.lobel@us.pwc.com

US Technology Contacts

Thomas Archer
Partner
+1 408.817.3836
thomas.archer@us.pwc.com

Mickey Roach
Partner
+1 214.756.1635
mickey.roach@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

Telecommunications

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders can bypass perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents evolve in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives in the global telecommunications industry are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising, confidence is high, and the number and cost of detected incidents are down.

But while many telecommunications companies have raised the bar on security, their adversaries have done better.

Threats are constantly multiplying and evolving. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few companies have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that companies identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1	Methodology
Section 2	Confidence in an era of advancing risks
Section 3	Today's incidents, yesterday's strategies
Section 4	A weak defense against adversaries
Section 5	Preparing for the threats of tomorrow
Section 6	The future of security: Awareness to Action

Section 1

Methodology

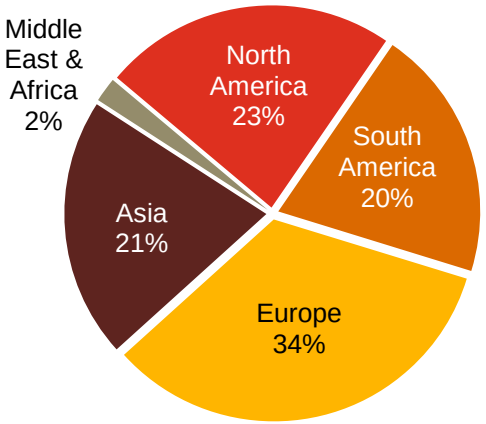
A global, cross-industry survey of business and IT executives

The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

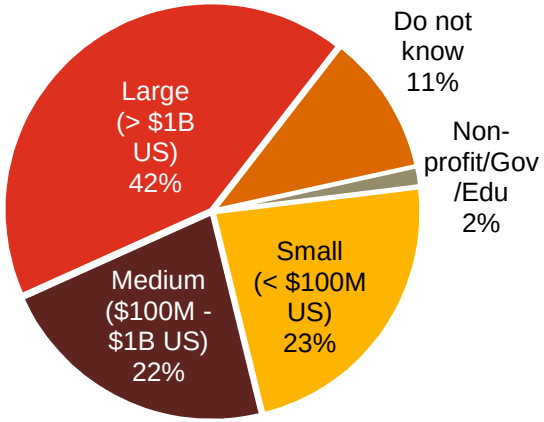
- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Survey included 456 respondents from the telecommunications industry
- Margin of error less than 1%; numbers may not add to 100% due to rounding

Demographics

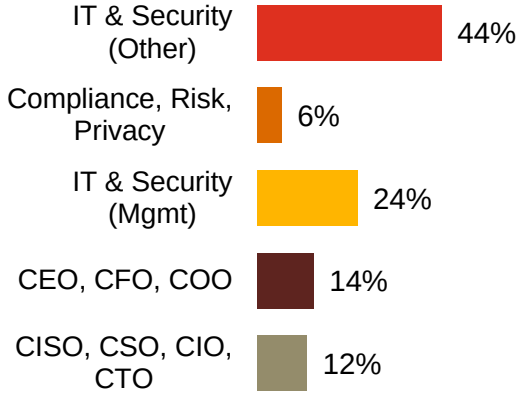
Telecom respondents by region of employment



Telecom respondents by company revenue size



Telecom respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

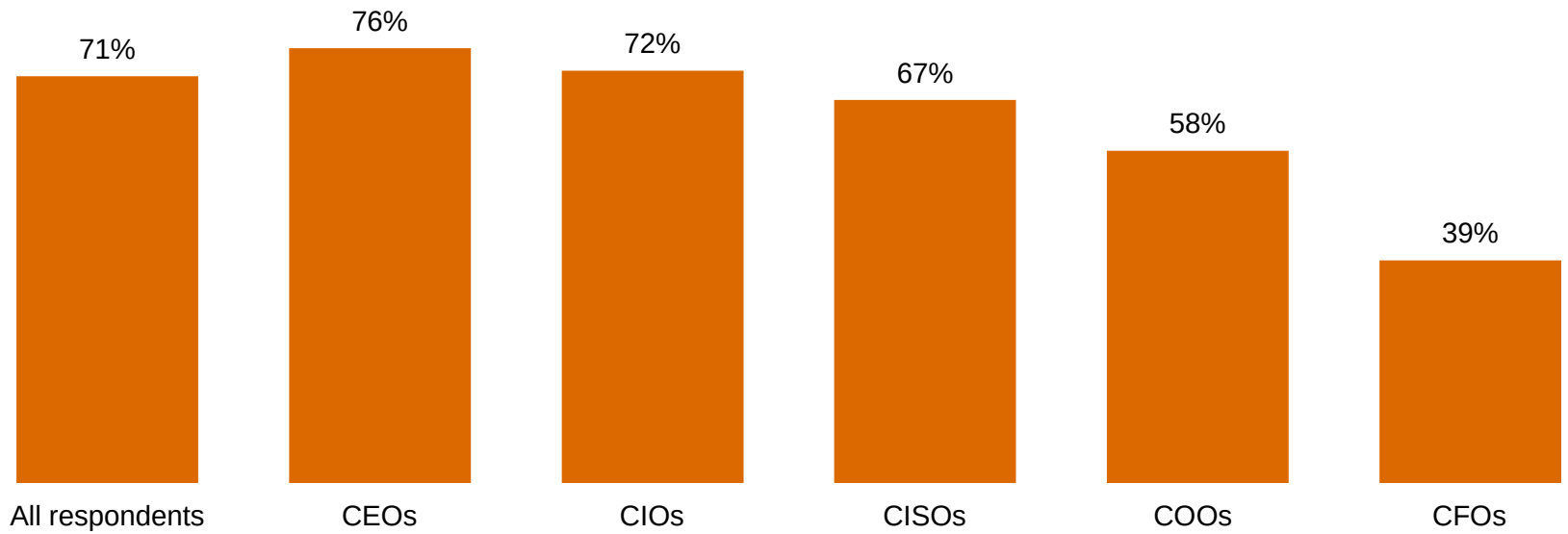
Section 2

Confidence in an era of advancing risks

71% of telecom respondents believe their security activities are effective, although some top executives are less confident.

While 76% of CEOs say they are confident in their security program, other top executives are less certain. Confidence among CFOs, for instance, has dropped sharply over last year.

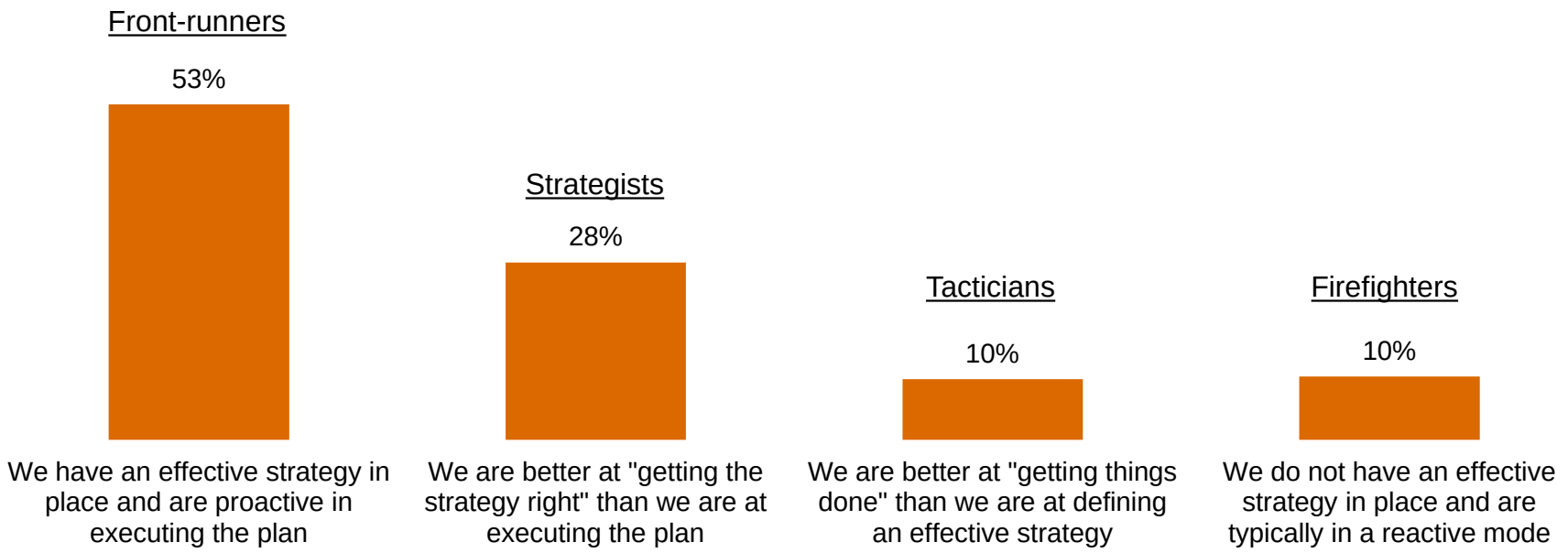
Executive confidence in effectiveness of security activities (somewhat or very confident)



Question 39: “How confident are you that your organization’s information security activities are effective?” (Respondents who answered “Somewhat confident” or “Very confident.”) Question 1: “My job title most closely resembles”

53% of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

More than half of telecom respondents say they have an effective strategy in place and are proactive in executing the plan, a slight increase over last year. More than one in four (28%) say they are better at getting the strategy right than executing the plan.



Question 27: "Which statement best characterizes your organization's approach to protecting information security?" (Numbers reported may not reconcile exactly with raw data due to rounding.)

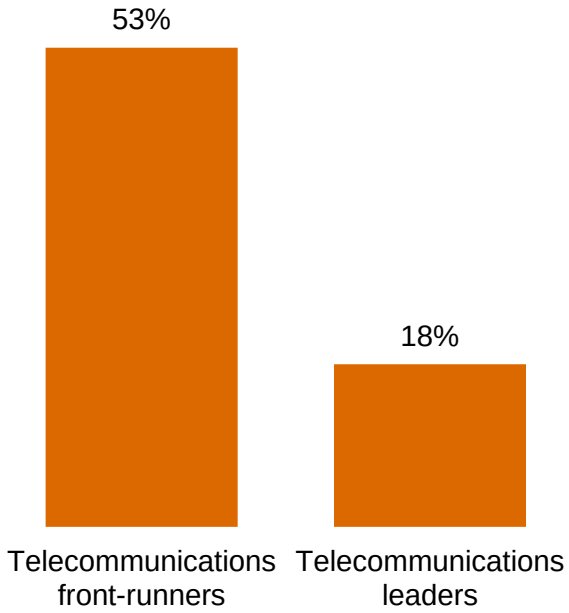
But closer scrutiny reveals far fewer real leaders than front-runners.

We measured telecommunications respondents' self-appraisal against four key criteria to filter for leadership.

To qualify, organizations must:

- Have an overall information security strategy
- Employ CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

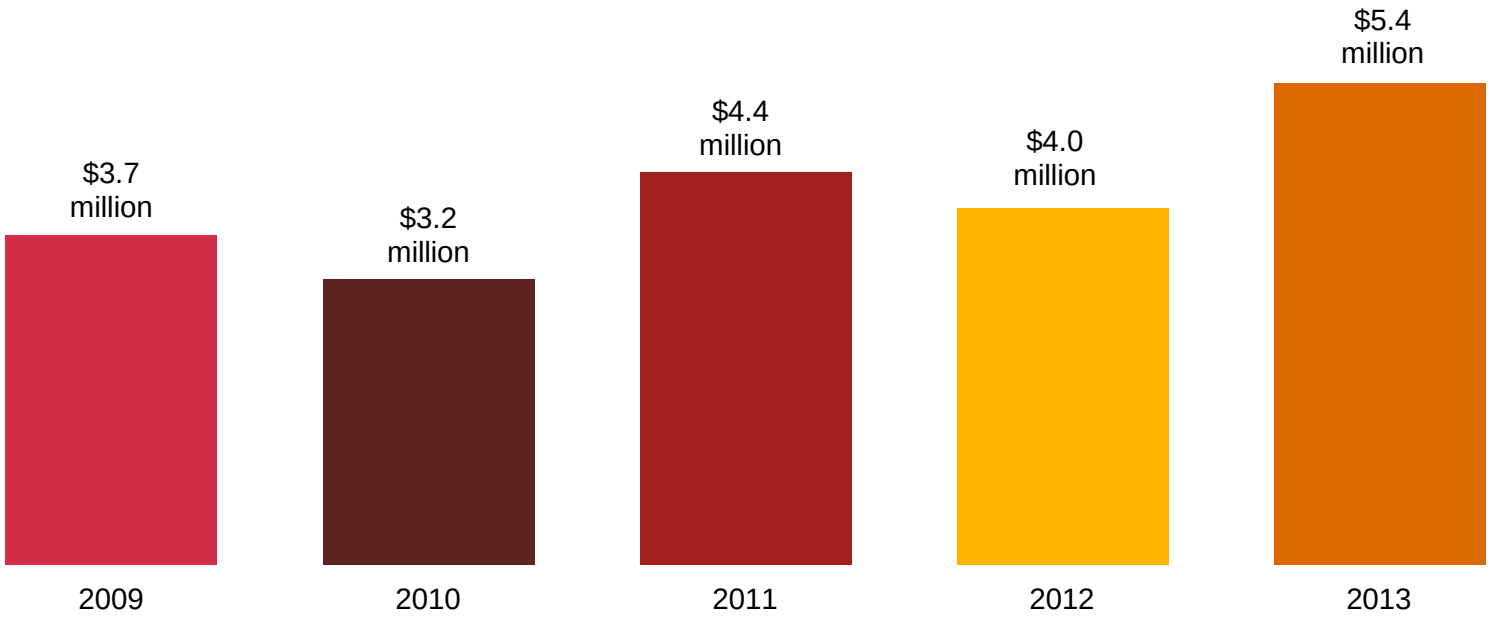
Our analysis shows there are significantly fewer real leaders than self-identified front-runners.



Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Information security budgets increase significantly.

Security budgets average $5.4 million this year, a gain of 35% over 2012. Telecom companies understand that today's elevated threat landscape demands a substantial boost in security investment.

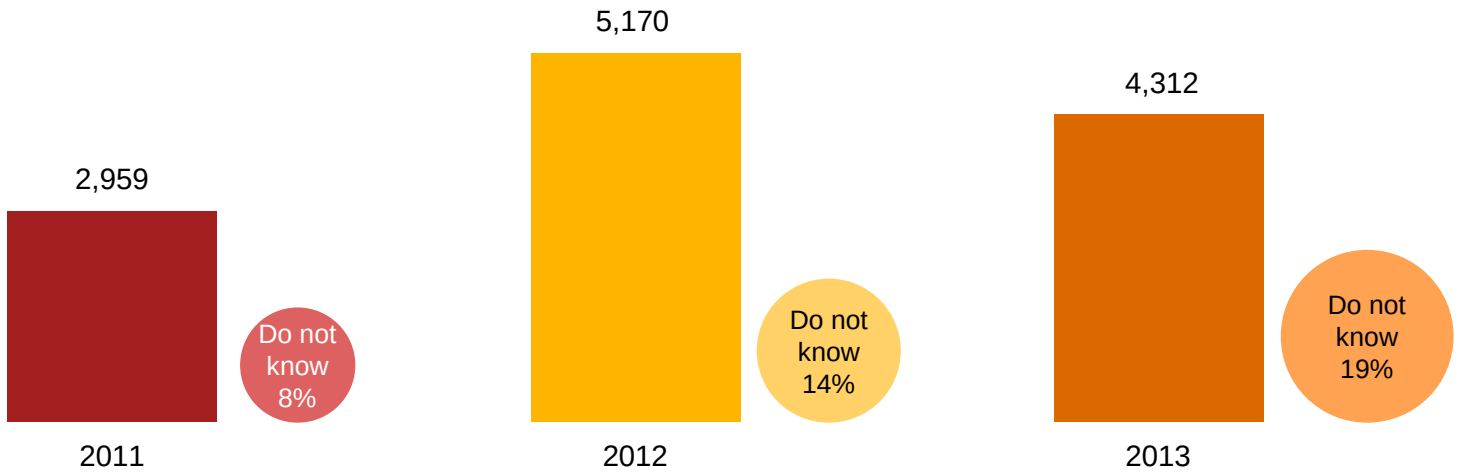


Question 8: "What is your organization's total information security budget for 2013?"

Among telecom respondents, detected security incidents and average financial losses have dropped significantly.*

Telecom respondents detected 17% fewer security incidents in the past 12 months. Despite the costs and complexity of responding to incidents, financial losses associated with security incidents decreased 34% over last year.

Average number of security incidents in past 12 months



* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months? Question 22A: "Estimated total financial losses as a result of all security incidents.

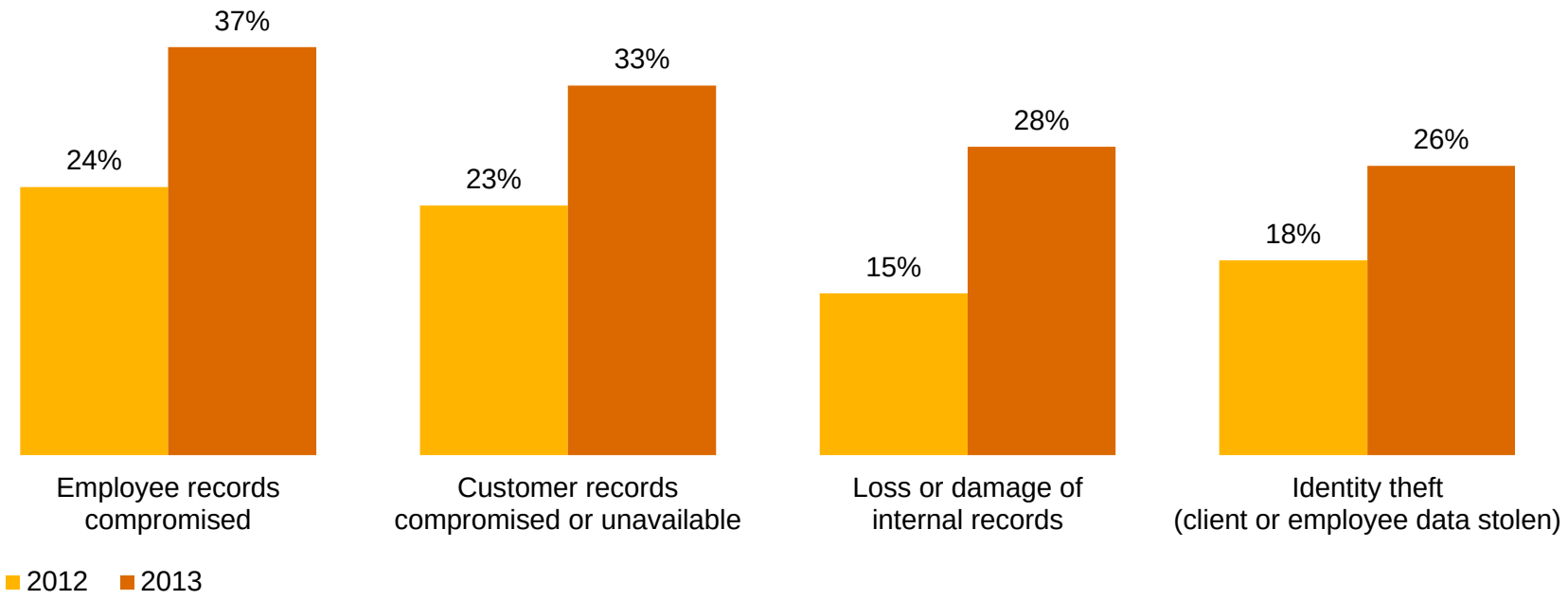
Section 3

Today's incidents, yesterday's strategies

Telecom respondents reported increases in data loss as a result of security incidents.

Compromise of employee and customer information increased substantially over last year, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records almost doubled.

Impact of security incidents

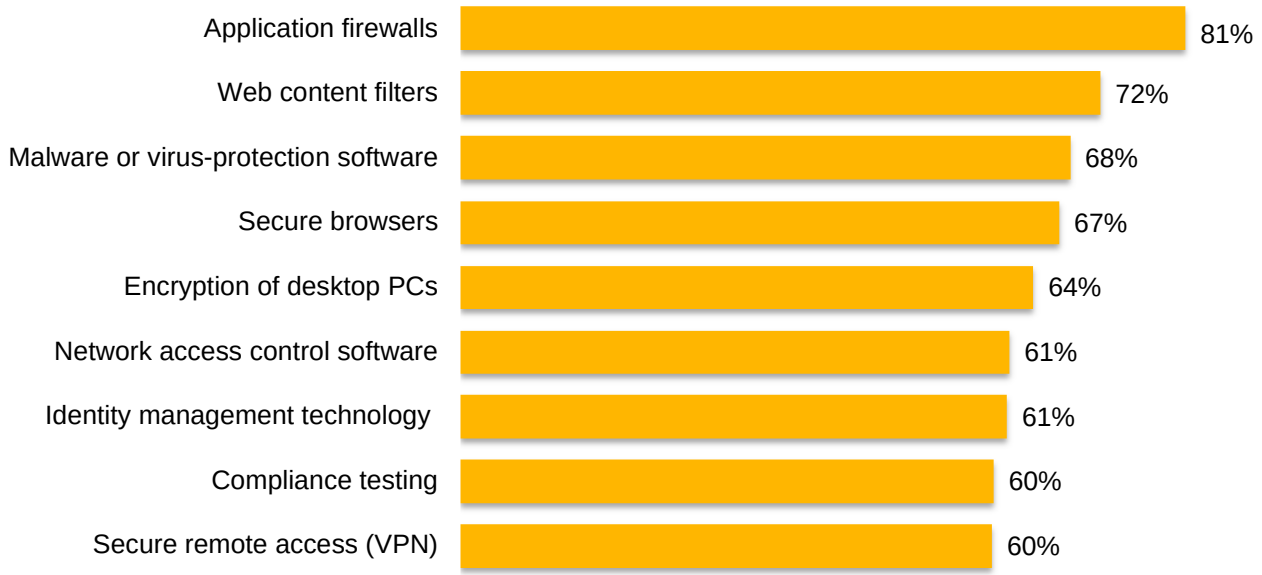


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Most respondents have deployed traditional security tools, yet they may not be effective in stopping today's threats.

Deployment of "block and tackle" security programs is at an all-time high. But they may not comprehensively block today's incidents, suggesting these products and services are ineffective because they are built on outdated security models.

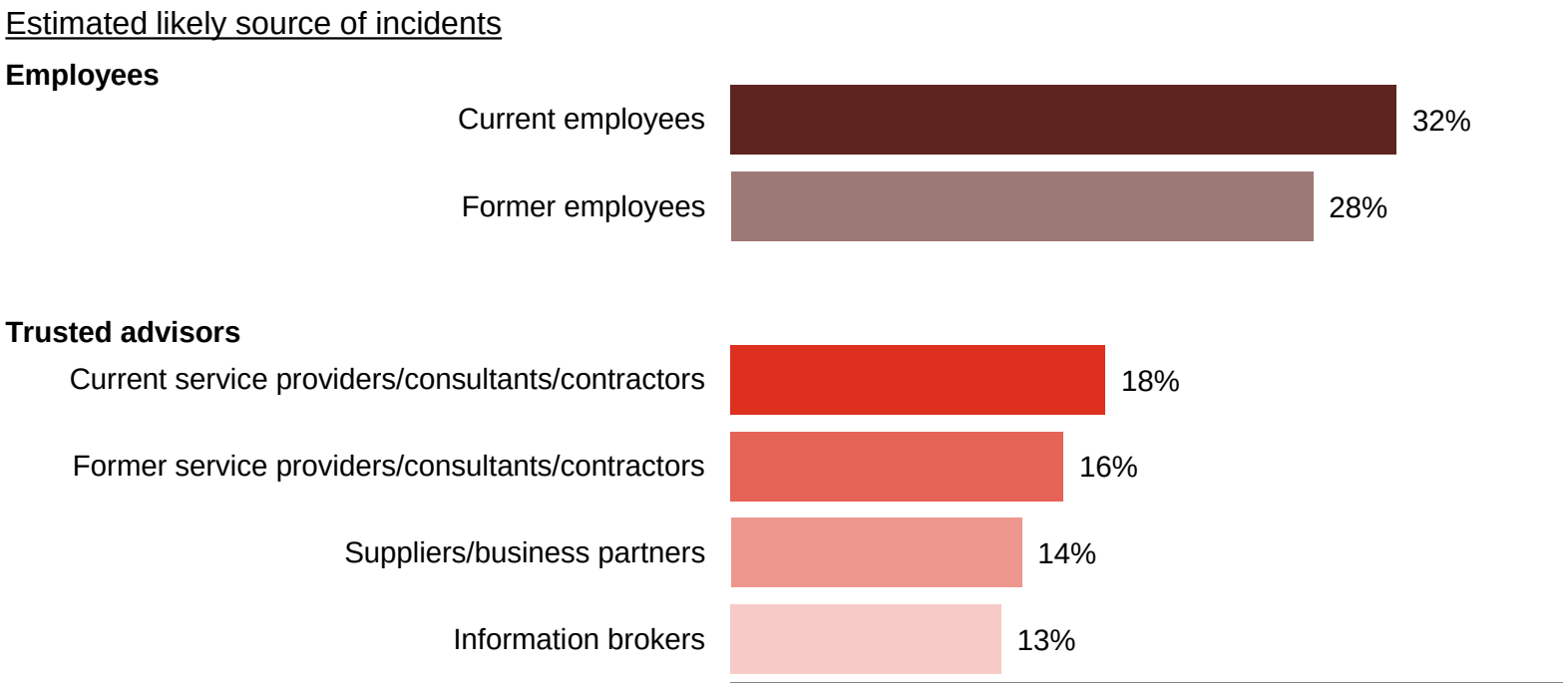
Information security safeguards and processes currently in place



Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most telecom respondents.

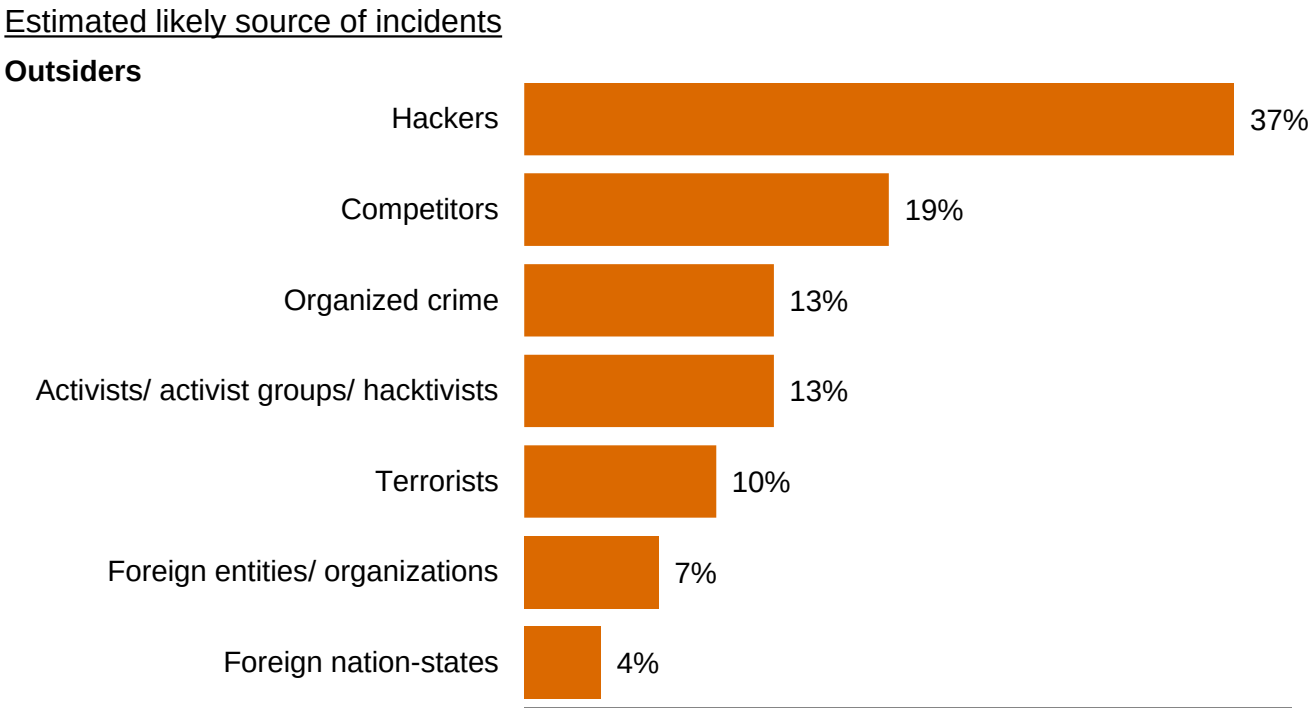
It's the people you know—current and former employees, as well as other insiders—who are most likely to perpetrate security incidents.



Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, telecoms are more likely to be hit by other outsiders.

Only 4% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger, attributed to 37% of incidents.



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

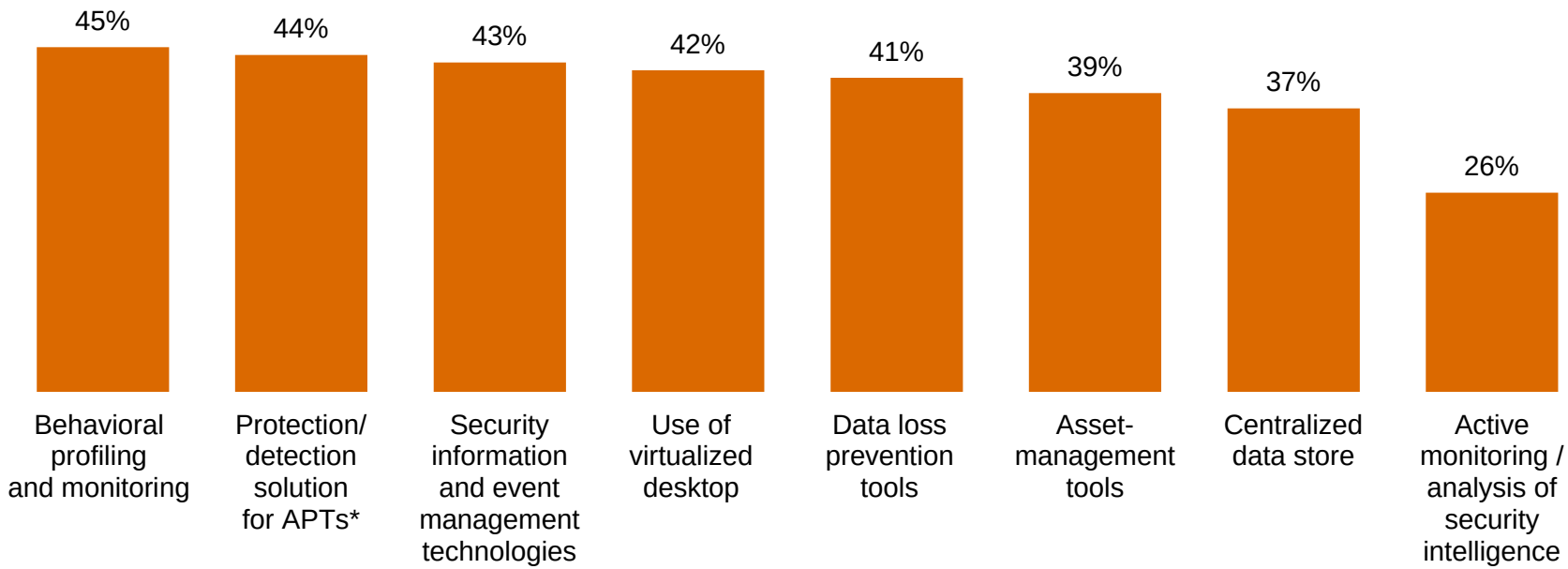
Section 4

A weak defense against adversaries

Many companies have not implemented technologies and processes that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place



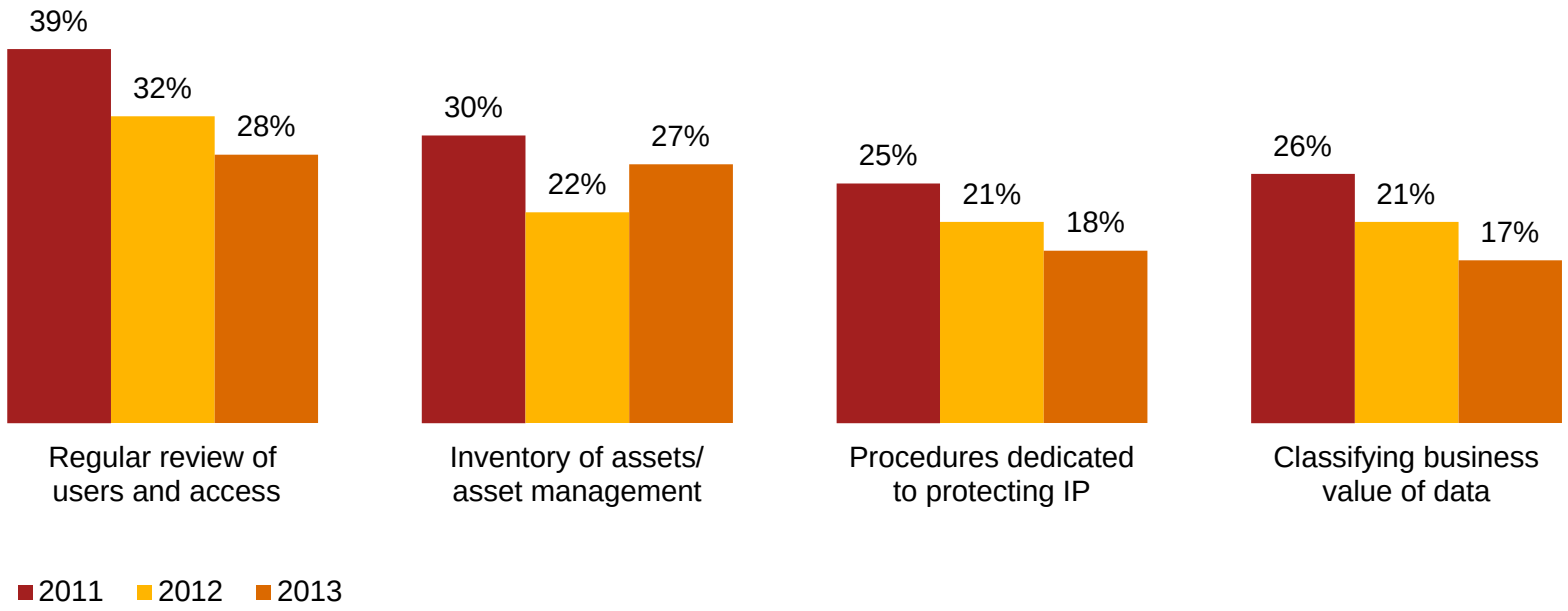
*Advanced persistent threats (APTs)

Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "Which technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

Despite the potential consequences, many telecom companies do not adequately safeguard high-value information.

It is imperative that companies identify, prioritize, and protect their "crown jewels." But implementation of basic policies to safeguard intellectual property (IP) is declining among telecom respondents.

Have policies to help safeguard IP and trade secrets

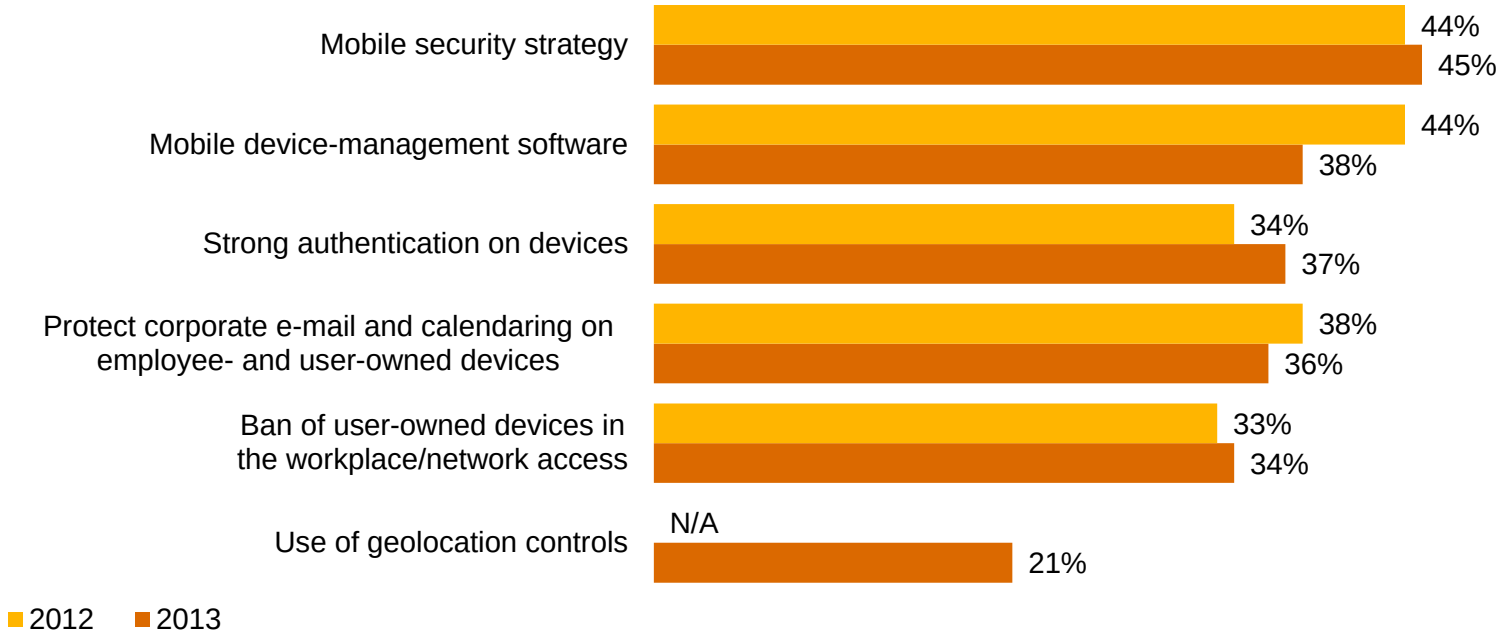


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet telecom respondents' efforts to implement mobile security programs do not show significant gains over last year, and continue to trail the growing use of mobile devices.

Initiatives launched to address mobile security risks

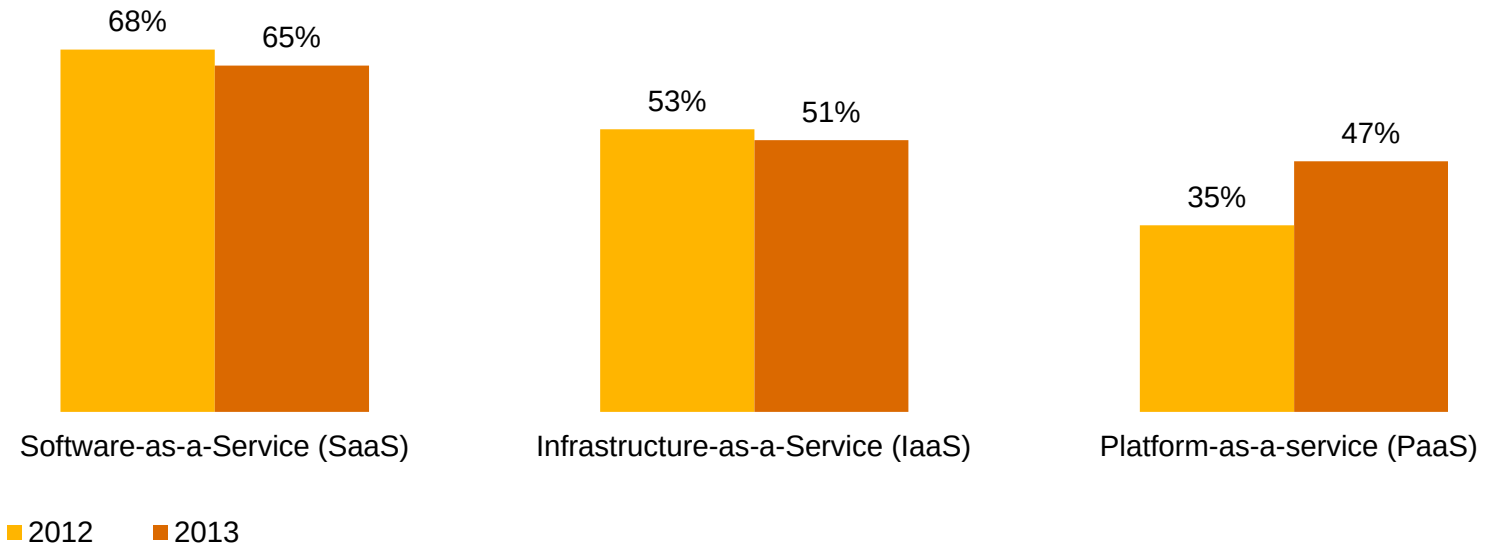


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Half of telecom respondents use cloud computing, but they often do not include cloud in their security policies.

While 50% of telecom respondents report using cloud services—and 57% say the technology has improved security—only 20% include provisions for cloud in their security policy. Among telecoms, SaaS remains dominant but PaaS shows strong growth.

Type of cloud service used



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

23% of respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey, we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves business performance and enables quick adaption to market changes.[1]

Reasons for not collaborating on information security

[1] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

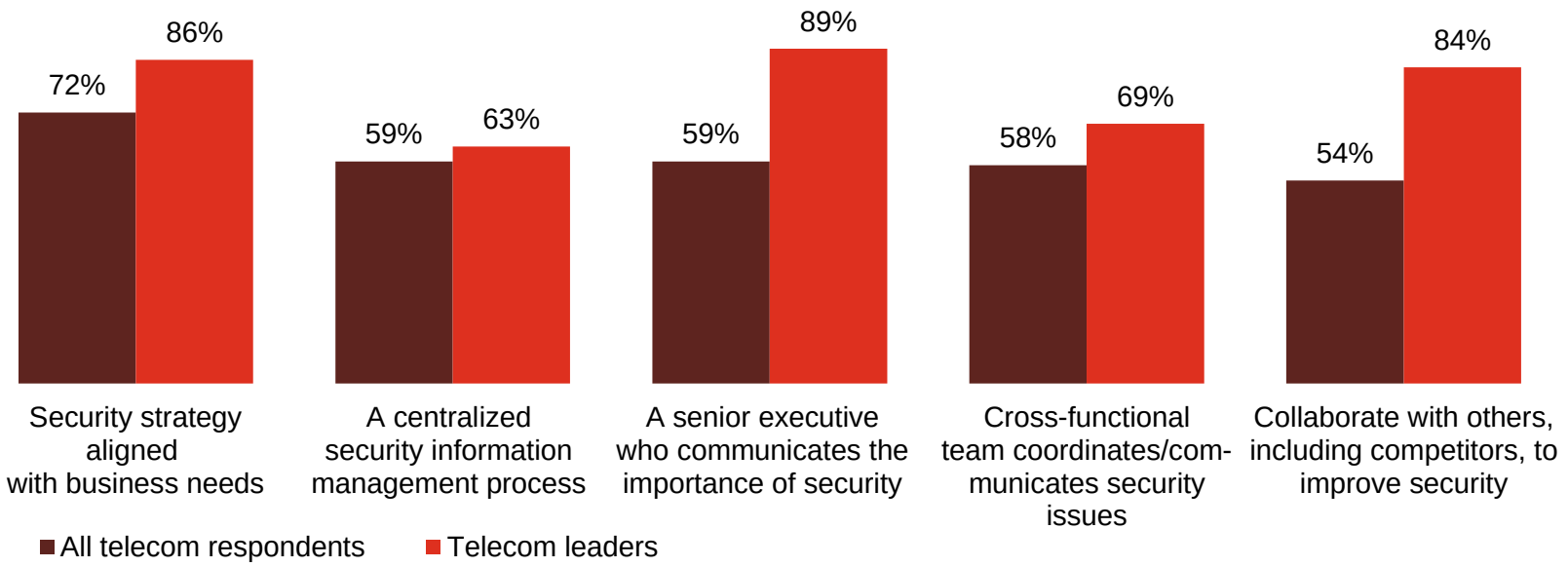
Section 5

Preparing for the threats of tomorrow

Telecom leaders are enhancing capabilities in ways that show security is a business imperative—not just an IT challenge.

Aligning security with business needs, collaborating with others, and improving communications show telecom leaders, in particular, are rethinking the fundamentals of security.

Security policies and safeguards currently in place: All respondents vs. leaders



Question 14: "What process information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?" Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?"

Many companies have invested in technology safeguards to secure their ecosystems against today's evolving threats.

Telecom leaders are more likely to have implemented many of these technologies. But given today's elevated threat landscape, *all* telecom companies—not just leaders— should strongly consider implementation of these safeguards.

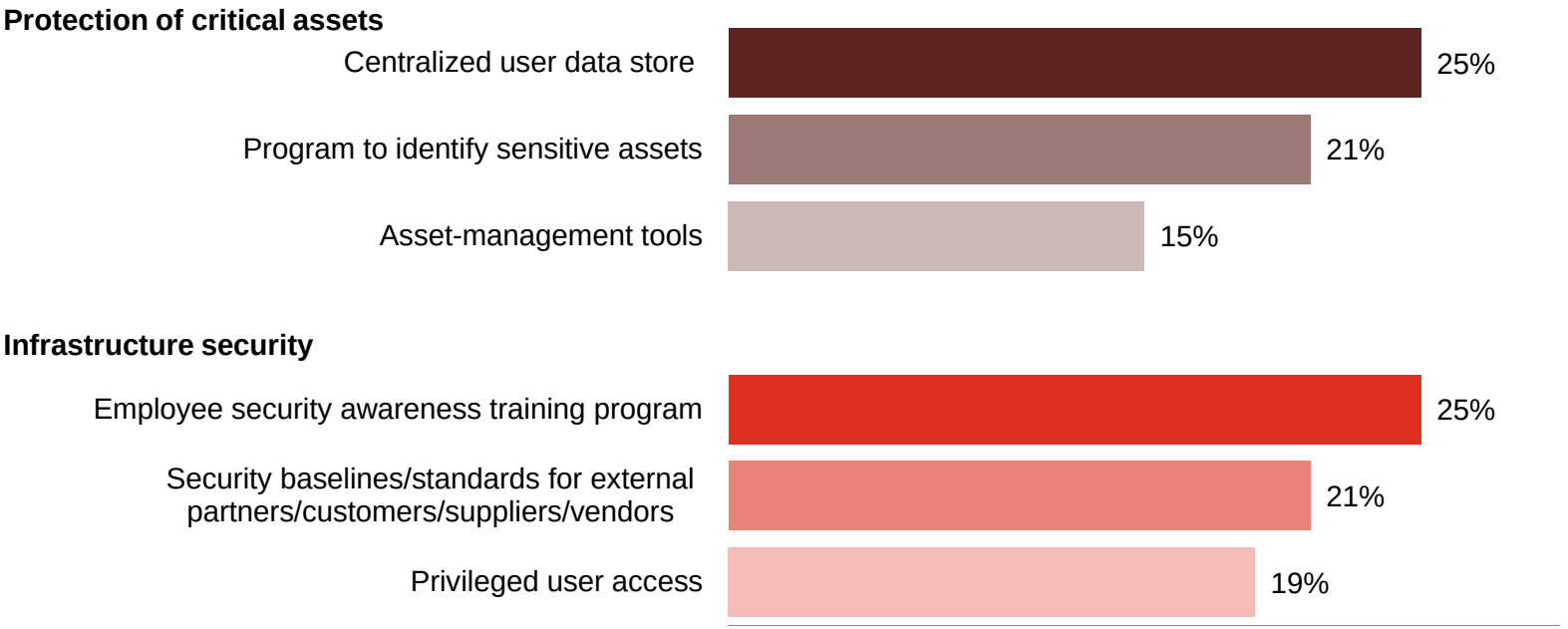
Technology safeguards currently in place	All telecom respondents	Telecom leaders
Malicious code detection tools	76%	86%
Intrusion detection tools	68%	72%
Privileged user access	65%	72%
Patch management tools	64%	72%
Asset management tools	60%	68%
User activity monitoring tools	60%	65%
Security information and event management technologies	57%	62%
Behavioral profiling and monitoring	55%	64%
Code analysis tools	53%	62%
Federated identity management	53%	64%

Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

What business imperatives and processes will telecom respondents prioritize this year?

Some of the highest priorities cited by telecom respondents include technologies that can help the organization protect its most valuable assets and gain strategic advantages.

Safeguards not in place but a top priority over the next 12 months

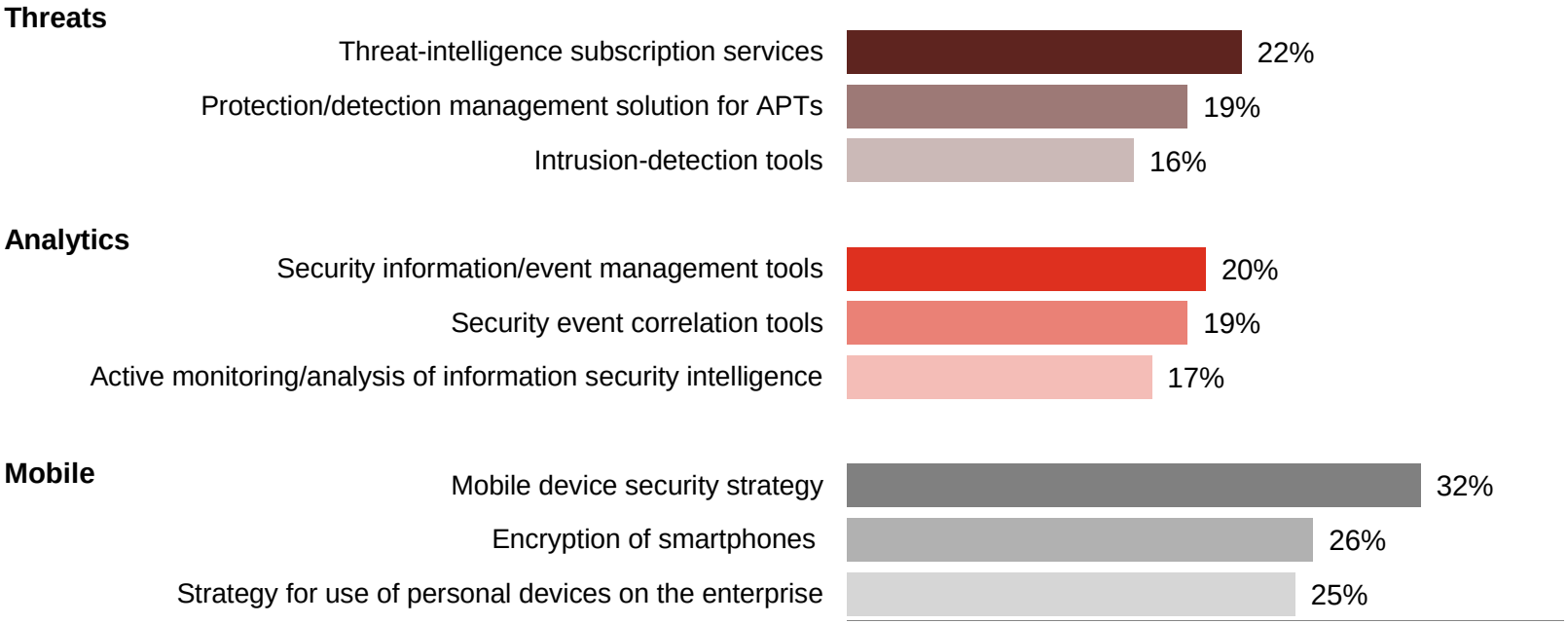


Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and telecom respondents are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Effective security demands that telecom companies align security spending and policies with business objectives.

Most telecom respondents say security spending is aligned with business objectives. In other words, they are starting to understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

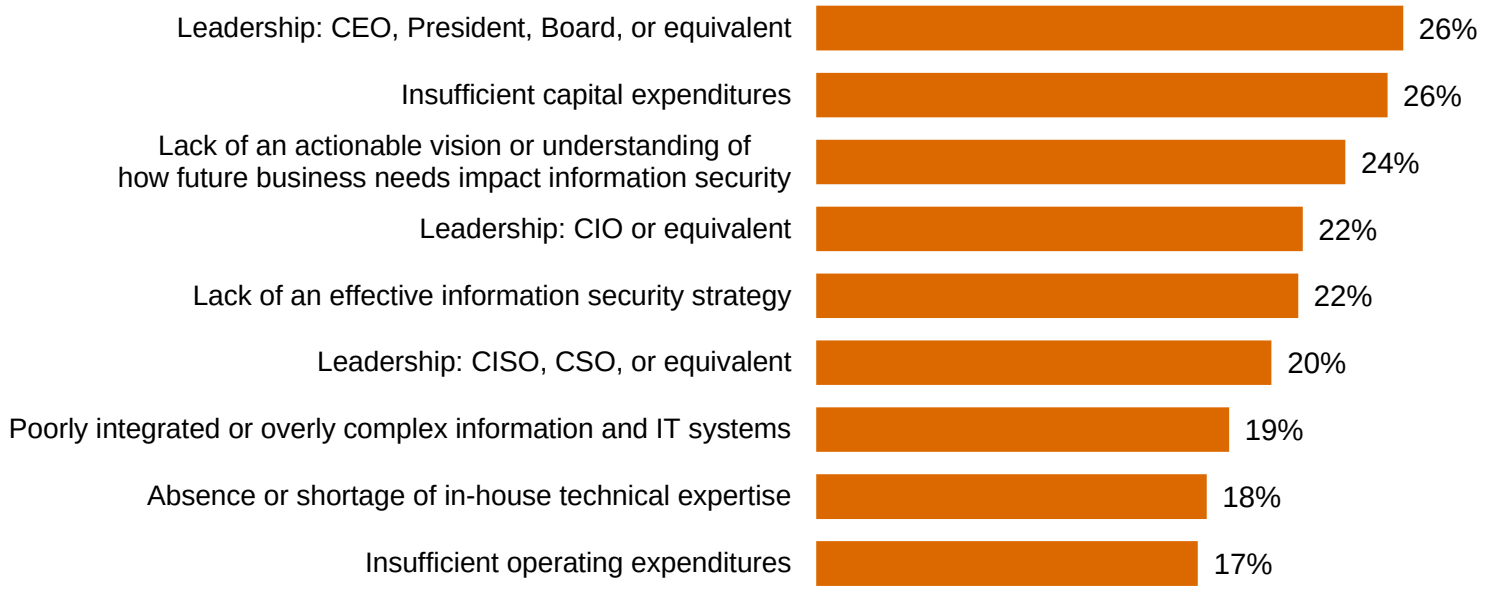
Level of alignment with organization's business objectives (somewhat or completely aligned)

Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?" Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?"

Committed leadership, more money, and an informed vision are needed to advance security.

These are critical because an evolved approach to security requires the support of informed top executives and an adequate budget that is aligned with business needs.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

US IT Security, Privacy & Risk Contacts

Gary Loveland
Principal
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

US Telecommunications Contacts

Ron Haas
Partner
214.754.4520
ronald.d.haas@us.pwc.com

Joseph Tagliaferro
Director
973.236.4226
joseph.tagliaferro@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data and benchmark your organization.

PwC

www.pwc.com/security

Defending yesterday

Key findings from The Global State of Information Security® Survey 2014

Advisory Services
Security

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

pwc

Methodology

The Global State of Information Security® Survey 2014 is a worldwide study by PwC, CIO magazine, and CSO magazine. It was conducted online from February 1, 2013, to April 1, 2013. Readers of CIO and CSO magazines and clients of PwC from around the globe were invited via e-mail to take the survey. The results discussed in this report are based on the responses of more than 9,600 executives including CEOs, CFOs, CISOs, CIOs, CSOs, vice presidents, and directors of IT and information security from 115 countries. Thirty-six percent (36%) of respondents were from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa. The margin of error is less than 1%. All figures and graphics in this report, unless otherwise noted, were sourced from survey results.

Table of contents

The heart of the matter

While information security risks have evolved and intensified, security strategies—historically compliance-based and perimeter-oriented—have not kept pace.

The result? Today, organizations often rely on yesterday's security strategies to fight a largely ineffectual battle against highly skilled adversaries who leverage the threats and technologies of tomorrow.

These sophisticated intruders are bypassing outdated perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives. Compounding matters, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through interconnected digital channels.

These factors have combined to make information security progressively more complex and challenging. It has become a discipline that demands pioneering technologies and processes, a skill set based on counterintelligence techniques, and the unwavering support of top executives. A key tenet of this new approach is an understanding that an attack is all but inevitable, and safeguarding all data at an equally high level is no longer practical.

The Global State of Information Security® Survey 2014 aims to measure and interpret how global organizations implement practices to combat today's highly skilled adversaries. This year's survey indicates that executives are elevating the importance of security. They are heeding the need to fund enhanced security activities and believe that they have substantially improved technology safeguards, processes, and strategies.

But while organizations have raised the bar on security, their adversaries have done even more. This year's survey shows that detected security incidents have increased 25% over the previous year, while the average financial costs of incidents are up 18%.

The survey also reveals that many organizations have not deployed technologies that can provide insight into ecosystem vulnerabilities and threats, identify and protect key assets, and evaluate threats within the context of business objectives. And for many companies, security is not yet a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

Put simply, few organizations have kept pace with today's escalating risks—and fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," **says Gary Loveland, PwC Principal.** *"What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."*

In this new model of information security, knowledge is power. Seize it.

An in-depth discussion

As digital technologies become universal, they have transformed the business environment.

Today, organizations are increasingly interconnected, integrated, and interdependent. They employ technology and ubiquitous connectivity to share an unprecedented volume of information assets with customers, service providers, suppliers, partners, and employees. These sophisticated technologies enable organizations to perform business tasks with a velocity and degree of efficiency that are unprecedented.

But this evolved business ecosystem also imperils organizations by putting them at the mercy of adversaries who would exploit these technologies and processes to disrupt operations and even destroy businesses. As a result, security threats have become a critical business risk to global organizations.

The traditional reactive approach to information security strategy, which typically relegates security to an IT challenge, remains commonplace.

But it is no longer effective, nor is it defensible.

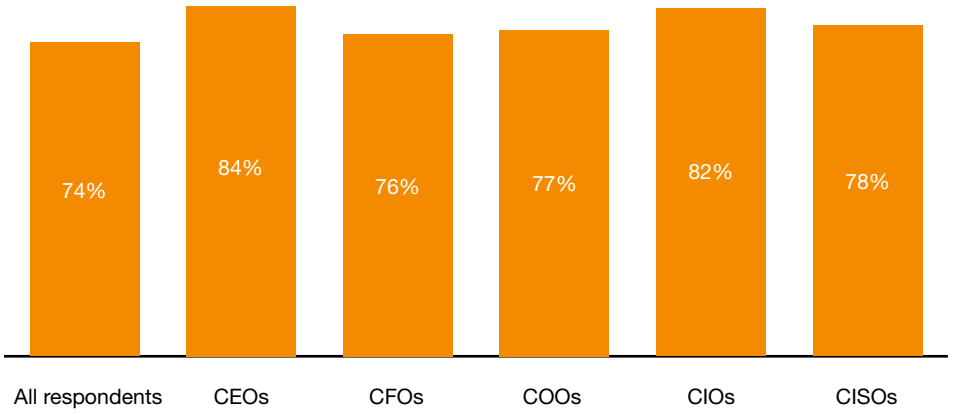
Today's new world of security risks demands that organizations treat information security threats as enterprise risk-management issues that can critically threaten business objectives. Safeguarding all data at the highest level is no longer realistic or even possible.

Against this backdrop, we asked business, security, and IT executives to tell us how they are addressing information security imperatives, and how well their privacy and information security safeguards are aligned with business objectives. The results of The Global State of Information Security® Survey 2014 show that most executives across industries worldwide are confident in their organization's information security practices.

Strong confidence in today's security practices

It is striking that, even in a climate of escalating and evolving risks, executives remain highly confident in their organization's security capabilities and activities. Globally, 74% of respondents say their security activities are effective. (Figure 1) And this optimism is strongest at the top of the org chart. For instance, 84% of CEOs say they are confident in their security program, and 78% of CISOs—those with direct responsibility for security—report confidence. Among executives, CFOs are the least confident. A regional view shows that respondents from South America (81%) and Asia (76%) report the highest levels of trust in their security programs.

Figure 1: Confidence in security activities (somewhat or very confident)



More than

80%

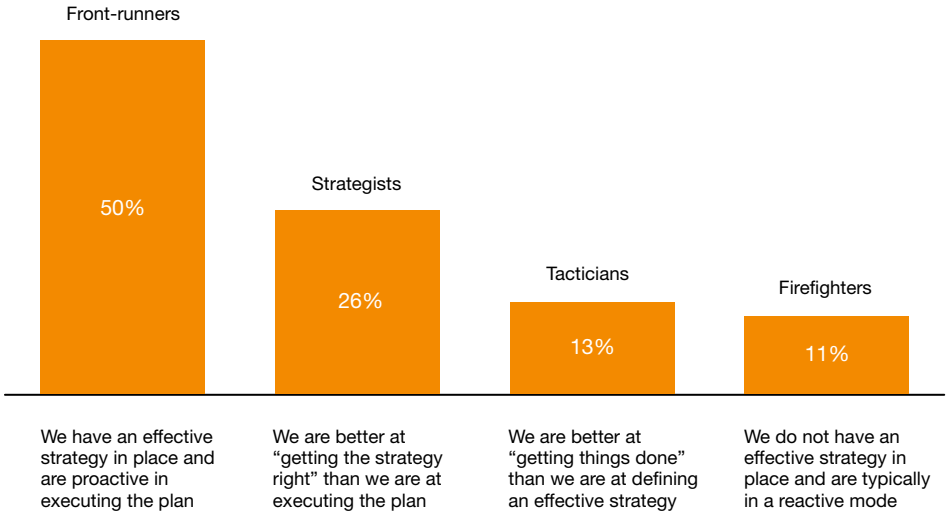
say security spending and policies are aligned with the business.

Another measure of confidence can be gleaned from how well executives perceive their organization's security program to be aligned with business strategy and overall spending. By that count, optimism is equally robust. More than 80% of respondents say security spending and policies are aligned with business objectives, an increase over last year for both categories. These levels of confidence suggest respondents understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

Optimism also extends to how respondents rank their overall security strategy and their ability to proactively execute that strategy. We asked respondents to tell us how they rate their security approach, and results show they rank themselves higher than the past two years.

We label those who report they have an effective strategy in place and are proactive in executing the plan Front-runners, since they exhibit two key attributes of leaders. Among this year's respondents, 50% say they have the attributes of a Front-runner, a 17% jump over last year. (Figure 2) About one in four (26%) say they get strategy right but may not successfully execute the plan, a category we call Strategists. Those who consider themselves better at "getting things done" than defining effective strategy—Tacticians—account for 13% of respondents. And the group that we call Firefighters, which do not have a strategy in place and are typically in a reactive mode, comprise 11% of respondents.

Figure 2: How respondents characterize their approach to information security



Are Front-runners really leaders?

Self-assessments are, by their very nature, biased. So we took a closer look at the data and created a series of requirements that define "true leaders" on the basis of reported capabilities rather than self-perception. To qualify as leaders, respondents must:

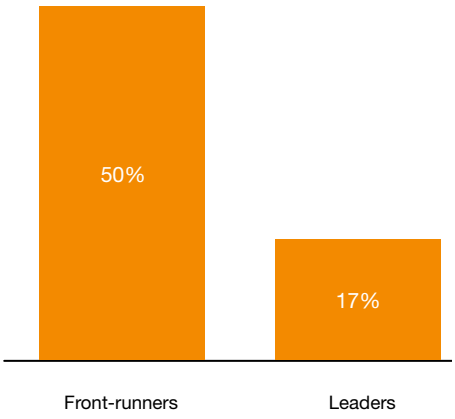
- Have an overall information security strategy.
- Employ a chief information security officer (CISO) or equivalent who reports to top leadership: the CEO, CFO, COO, CRO, or legal counsel.
- Have measured and reviewed the effectiveness of their security measures within the past year.
- Understand exactly what type of security events have occurred in the past year.

Filtering for these qualities shows that Front-runners are not necessarily leaders. Based on these criteria, only 17% of all survey respondents rank as true leaders. (Figure 3) We also found that, compared with Front-runners, real leaders detect more security incidents, have a better understanding of what types of security incidents occur and the source of those incidents, and report lower average financial losses as a result of security incidents.

Real leaders detect more security incidents, have a better understanding of what types of security incidents occur and the source of those incidents, and report lower average financial losses as a result of security incidents.

Regionally, leaders are most likely to be based in Asia Pacific (28%) and North America (26%), followed by Europe (24%), South America (21%), and the Middle East and Africa (1%). Industries most represented among leaders include technology (16%), financial services (11%), and retail and consumer (9%).

Figure 3: Front-runners vs. leaders



Another cause for optimism: Budgets are rising

If most respondents see themselves as highly competent in their information security practices, those who control the company purse strings also appear to be optimistic about the security function—or perhaps they understand that today's elevated threat landscape demands a boost in security investment. Either way, substantial increases in security funding are a good sign for security efforts. While budgets vary significantly across industries and by company size, overall respondents say security budgets average $4.3 million this year, a 51% gain over 2012. Despite this increase, however, information security budgets represent only 3.8% of the total IT spend this year, a relatively small investment.

Average information security budgets have increased

51%

over last year.

But what about the future? Optimism is high there, too. Almost half (49%) of respondents say that security spending over the next 12 months will increase, up from 45% last year. Regionally, respondents from South America (66%) and Asia Pacific (60%) expect that security investments will rise. Only 38% of North America respondents forecast an uptick in security spending, making them the least sanguine on spending.

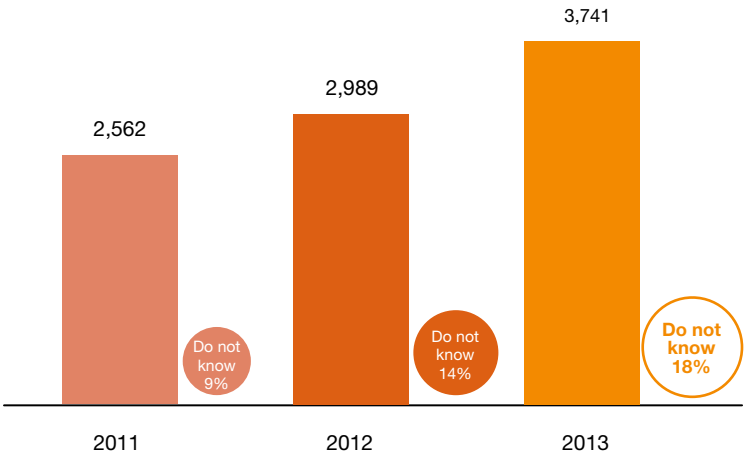
Today's incidents, yesterday's strategies

It has been all but impossible to ignore the barrage of news reports about increasingly sophisticated—and often successful—security breaches over the past year. Given the sometimes sensational, and often click-driven nature of news reporting, it's only natural to question the accuracy of reports concerning cyber intrusions.

The results of this year's survey corroborate some—but not all—of the reporting concerning security incidents.

One fact is indisputable: Security incidents are increasing. (We define a security incident as any adverse incident that threatens some aspect of computer security.) Survey respondents report a 25% jump in detected incidents over last year. (Figure 4) This would seem to validate the headlines trumpeting elevated security threats. On the other hand, an increase in detected incidents could also mean that organizations are getting better at identifying incidents.

Figure 4: Average number of security incidents in past 12 months



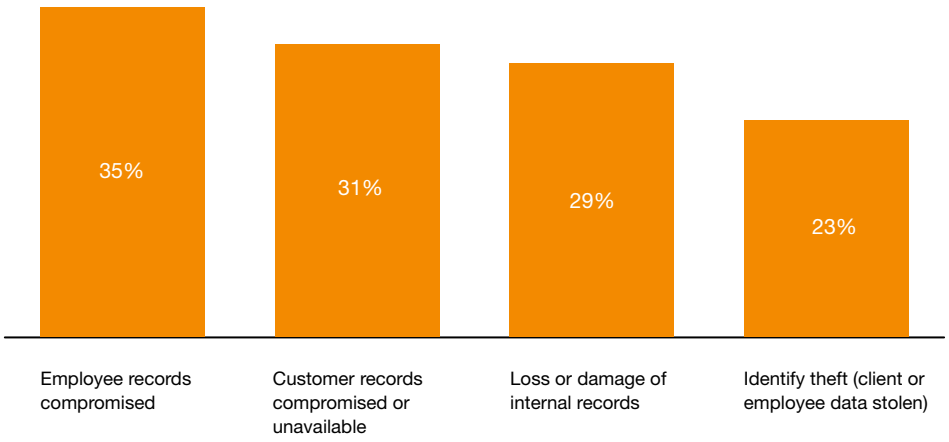
"Incidents are increasing not only because there are more threats out there, but also because some companies have invested in new technologies to better detect them," **says Mark Lobel, PwC Principal.** *"In that regard, increased detection of security incidents should be seen as a positive development."*

But the number of respondents who do not know the frequency of incidents continues to climb year over year—it's now at 18% —and that would seem to contradict the notion that organizations are becoming more adept at detecting intrusions. This finding, in fact, is more likely to suggest that old security models in use may be broken or ineffective.

The increase in incidents combined with a concurrent rise in the volume of business data being shared digitally results in an unsurprising finding: Proliferating data loss. This year, 24% of respondents reported loss of data as a result of security incidents, a hike of 16% over 2012.

Delving into the types of data exploited reveals some interesting findings. Compromise of employee records (35%) and customer records (31%) led the pack of data impacted. (Figure 5) Year after year, survey respondents tell us that employee and customer data are the most valuable information they hold—so presumably their security efforts would center on protecting these types of data. Yet the fact that employee and customer data are the most likely types of information to be siphoned off suggests that current data-protection efforts are not effective or focused on the right risks.

Figure 5: Impact of security incidents



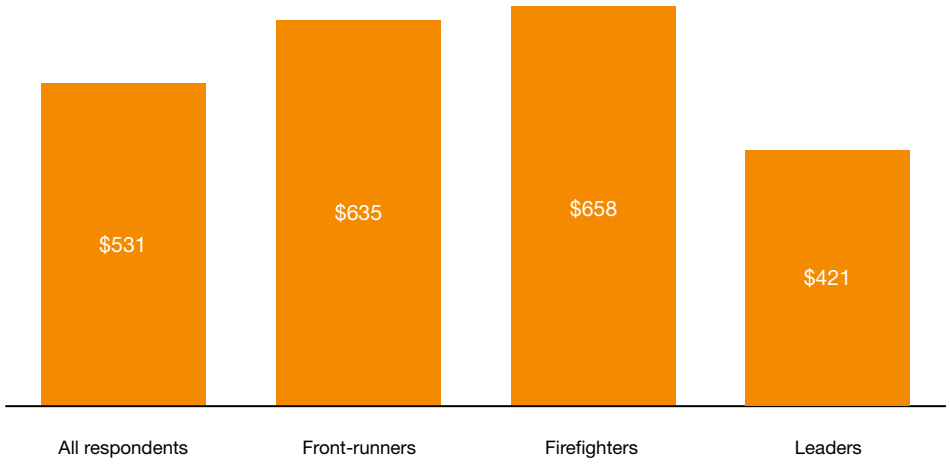
Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

The compounding costs of loss

It would seem logical that, as the number of security incidents rise, so too would the financial costs. And so it is: We found that average financial losses associated with security incidents rose 18% over last year.

"Overall, the costs and complexity of responding to incidents are increasing," **says Shane Sims, PwC Principal.** *"This includes the cost to investigate; the cost to understand business risks and contain incidents; the cost to manage notification to regulators, customers, and consumers; and the cost of litigation. Also, the cost of remediation is rising because more records across more jurisdictions are being impacted, and security controls have not kept pace with the ever-changing threat landscape."*

Figure 6: Average cost per security incident



Parsing the data a bit more, we discovered that financial losses are accelerating sharply among respondents that report high-dollar value impact. Case in point: The number of respondents who report losses of $10 million-plus has increased 51% since 2011. We expect certain industries that have historically been proactive in investing in security initiatives would report lesser losses, but surprisingly, this wasn't the case. Industries reporting losses of $10 million or more included pharmaceuticals (20%), financial services (9%), and technology (9%).

Overall, the average cost of intrusions on a per-incident basis is $531. (Figure 6) Respondents we identified as leaders report the lowest cost per-incident, at

an average of $421—no surprise there. What we didn't expect to see is that self-identified Front-runners spend is $635 per incident—almost as much firefighters, those who are, by their own assessment, the least prepared to run an effective security program. This calls into question the real-world efficacy of Front-runners.

Insiders, outsiders, and hackers

As noted, headlines don't always reflect boots-on-the-ground reality in combatting threats. While high-profile incidents such as highly sophisticated intrusions attributed to advanced persistent threats (APTs) make for tantalizing copy, this type of incident is quite rare.

Indeed, reality is much more prosaic. Most respondents attribute security incidents to everyday insiders like current employees (31%) or former employees (27%). (Figure 7) Many see these insider threats as far more significant than headline-making, but infrequent, threats.

Figure 7: Estimated likely source of incidents

Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

"I see the insider threat looming larger in my windshield than in the past," **says Michael A. Mason, chief security officer for Verizon Communications, adding that Verizon defines insiders as anyone who has access to Verizon's data.** *"And it's important to note that insider threats are not necessarily a 'bad guy' with bad intentions; it could be a good employee doing righteous work in an insecure manner. Our problems are more human than technological."*

Given the prevalence of employee risks, it is surprising that many organizations are not prepared to handle common insider threats. A separate survey co-sponsored by PwC, the 2013 US State of Cybercrime Survey, finds that one-third of US respondents do not have an incidence response plan for dealing with insider security incidents.[1] And among those that do have a response plan for internal incidents, only 18% of respondents describe the effort as extremely effective.

"One reason why organizations do not have effective plans in place for internal threats is that many classes of insiders, such as partners and suppliers, are invited within network perimeters and a certain level of trust is assumed," **says John Hunt, PwC Principal.** *"Businesses should understand that trust in advisors should not be implicit."*

Among external risk factors, it's important to note that some high-profile threat actors—hackers, in particular—do deliver on their risk potential. Consider this: 32% of survey respondents attribute security incidents to hackers, an increase of 27% over last year.

And what of high-publicity incidents such as attacks by foreign nation-states that employ APTs to exfiltrate information? Survey respondents say intrusions backed by foreign nation-states account for only 4% of detected incidents.

It's not a big concern for many companies, Verizon included. "Worrying about advanced persistent threats is, in some ways, like worrying about catching a cold while working in an anthrax factory," Mason says.

While APTs may present a remote risk potential, keeping abreast of rapidly evolving cyber threats is a priority for many large organizations, including Cablevision Systems Corporation, a multiple system operator (MSO) whose properties include cable TV, an Internet service provider, and a high-circulation daily newspaper.

"Like most MSOs, we are attuned to and follow the published reports denoting an increase in the detection of state-sponsored and cyber-terrorist activities, specifically as they relate to utilities and communication companies as targets," says Jennifer Love, senior vice president of security operations. "We use information from various sources, including the industry and government, to identify risks and guide decisions."

A weak defense against adversaries

To combat today's risks, organizations should be able to achieve ongoing insight and intelligence on ecosystem vulnerabilities and dynamic threats. Activities and investments should be driven by the best available knowledge about information assets, ecosystem threats, and vulnerabilities—and evaluated within the context of business activity.

For many, this represents a significant shift in thinking and planning. So it's not entirely surprising that many survey respondents report they have not implemented technologies and processes that provide insight into current risks. For instance, 52% of respondents have not deployed behavioral profiling and monitoring tools, and fewer (46%) do not employ security information and event-management technologies. Asset-management tools are critical to safeguarding data assets, yet are not in place for 39% of respondents we surveyed. Even established technologies that can be essential to protecting sensitive information are under-utilized. Most notably, we found 42% of respondents do not use data loss prevention tools.

[1] *2013 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

As data proliferates and is shared among more partners, suppliers, contractors, and customers, it is increasingly critical that businesses understand the risks associated with sharing data with third parties. What's more, organizations should ensure that third parties meet or beat their requirements for data security.

So it is worrisome to find that, in the US, many respondents do not have policies and tools to assess security risks of third parties, according to a separate survey co-sponsored by PwC.[2] For instance, only 20% say they evaluate more than once a year the security of third parties with which they share data or network access. Indeed, 22% say they do not evaluate third parties at all, while 35% say they evaluate third parties once a year or less. Similarly, only 22% of respondents say they conduct incident-response planning with third-party supply chain partners, while 52% never conduct incident-response planning for third party supply chains.

As noted, today's elevated and evolving threat environment requires that organizations understand that it is no longer practical—or, indeed, possible—to protect all information with equal priority. In a new model of security, businesses should identify and prioritize the information that really matters.

The information that really matters will vary by organization and by industry, of course. These "crown jewels" may include intellectual property (IP) such as product designs, marketing plans, executive communications, and business strategies. A more general definition can be stated as any information that could render significant hardship to the business if lost, stolen, or compromised.

Figure 8: Have policies to safeguard IP and trade secrets

Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Non-tangible assets such as IP now account for 80% of the value associated with S&P 500 firms, according to Ocean Tomo, the Intellectual Capital Merchant Banc™ firm.[3] And as the value of IP increases, so does its appeal to cyber criminals.

Despite the increasing value of IP and the potential consequences of its loss, this year's survey finds that many respondents do not adequately identify and safeguard their high-value information. For instance, only 17% of respondents classify the business value of data and only 20% have implemented procedures dedicated to protecting IP. (Figure 8) Slightly more (26%) maintain an inventory of assets and asset management. Survey results show that, in some industries, inclusion of policies to protect IP is actually declining.

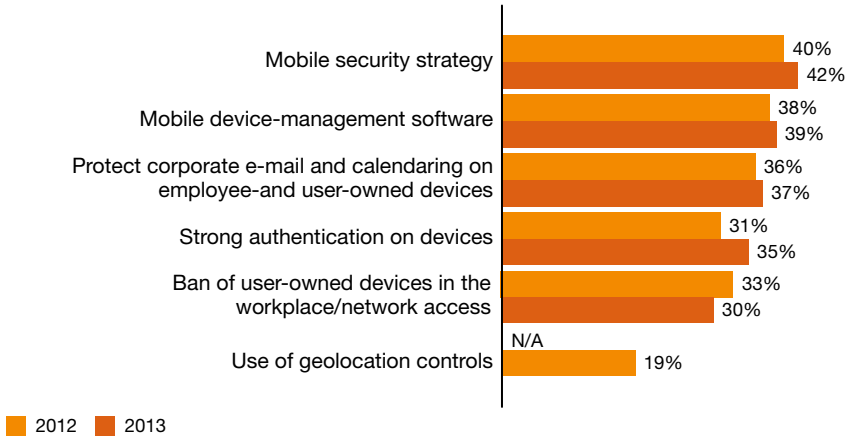
Another key risk to data security is the surge in the use of mobile devices such as smartphones and tablets, as well as the "bring your own device" (BYOD) trend. While the use of mobile devices to share and transmit data continues to increase, deployment of mobile security

[2] *2013 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

[3] Ocean Tomo, *Ocean Tomo's Annual Study of Intangible Asset Market Value*, April 2011

policies lags the proliferating use of smartphones and tablets. In fact, survey respondents indicate that efforts to implement mobile security programs do not show significant gains over last year and in some cases are actually declining. (Figure 9) For instance, only 42% say they have a mobile security strategy in place, and fewer (39%) say their organization has deployed mobile device management (MDM) software, a critical tool for automated management of a fleet of smartphones.

Figure 9: Initiatives launched to address mobile security risks



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Only ***18%*** *of respondents say they have policies governing cloud services.*

Cloud computing has been around for more than a decade, and is commonplace—if not quite mainstream—in the corporate ecosystem. Almost half (47%) of respondents use some form of cloud computing, a healthy gain of 24% over the year before. Among those who use cloud services, 59% of respondents report that their security posture has improved.

So it is a bit surprising to learn that many organizations have not seriously addressed the security implications of cloud services. For instance, among survey respondents that use cloud services, only 18% say they have policies governing the use of cloud.

"A lack of policies for cloud computing represents a serious security gap for businesses," says Joshua McKibben, PwC Director. "The proliferation of data being shared, in combination with the increase in the use of mobile devices, creates an environment in which cloud services are more widely used—and potentially abused—by employees. At the same time, it is essential that businesses ensure that third-party cloud providers agree to follow security practices."

Advanced persistent threats, as noted, get more than their share of press, and that could account for the increase in those who seem to be taking APTs seriously. For instance, 54% of overall survey respondents say they have protection/detection management solution technology in place. Among industries, a higher percentage of aerospace and defense (61%), public sector (58%), and pharmaceuticals (58%) respondents say they have deployed an APT solution.

According to the 2013 US State of Cybercrime Survey, APT tools are most likely to include malware analysis, inspection of outbound traffic, rogue device scanning, and analysis and geolocation of IP traffic.[4]

[4] *2013 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

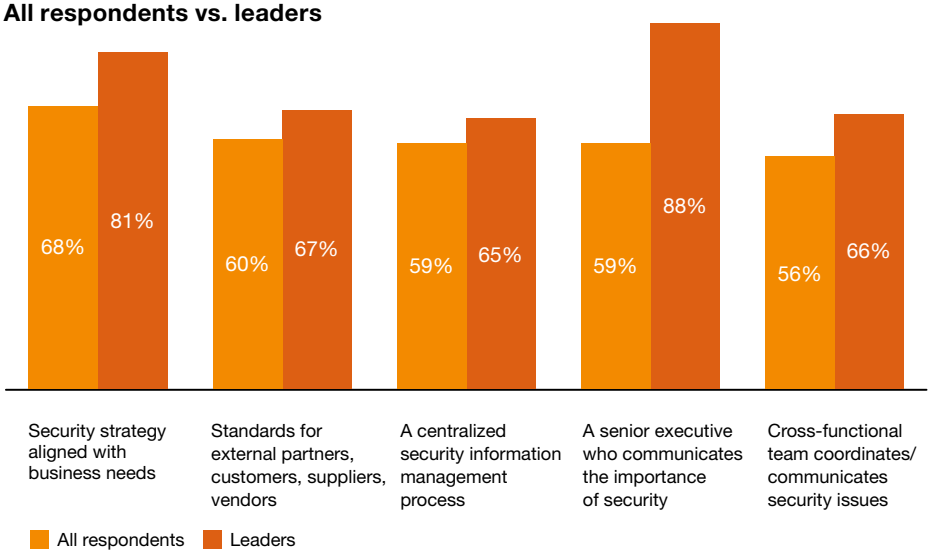
Preparing for the threats of tomorrow

Today, adversaries are constantly sharpening and evolving their capabilities to exploit new vulnerabilities. Addressing these threats will require that organizations approach activities and investments with best-available knowledge about information assets, ecosystem threats, and vulnerabilities. These activities should be evaluated within the context of business activity.

This year's survey indicates that those we define as leaders are enhancing their capabilities to do just that by implementing policies that elevate security to a top business imperative—not just an IT challenge. How so?

Leaders are aligning security with business needs, setting standards for external partners, and, in general, rethinking the fundamentals of security. (Figure 10) For instance, 88% of leaders have a senior executive who communicates the importance of information security across the enterprise. Another forward-thinking policy is to designate a cross-functional team that coordinates and communicates security issues, which 66% of leaders employ.

Figure 10: Security policies and safeguards currently in place—All respondents vs. leaders



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

"These types of policies demonstrate a new commitment to security, one that focuses on the involvement of top executives and the board to ensure that the company designs and implements an effective security program," **says Joe Nocera, PwC Principal.** *"It also underscores the need to raise security awareness among employees and third parties that handle sensitive data."*

"At Cablevision, the C-suite and board readily embrace security initiatives," **says Jennifer Love, SVP of security operations.** *"Our executives and board understand the importance of information security and express a keen interest in understanding what threats we face and what we are doing to mitigate our vulnerabilities."*

Policy and executive support are just a start, however. A measure of real intent can be gauged by whether companies have also deployed technologies to execute these policies.

Leaders are more likely to have deployed tools that provide a real-time analysis of suspicious activity logged on network hardware and applications. For instance, 66% of leaders say they have implemented security information and event management (SIEM) technologies. Similarly, 66% of leaders say they have deployed event correlation tools, which aggregate and correlate information from disparate tools like vulnerability and intrusion monitoring systems. Vulnerability scanning solutions, in place at 71% of leaders, assess networks and applications for weaknesses.

While our focus is on leaders who have implemented the technologies above, it's just as important to stress that, given today's elevated threat landscape, all organizations should strongly consider implementation of these safeguards when applicable.

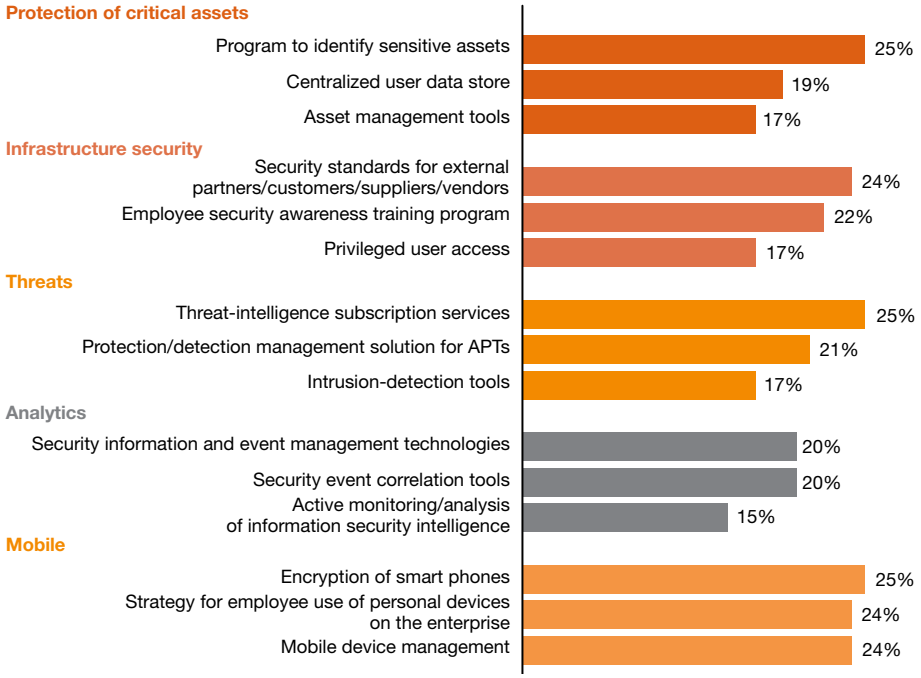
Another example can be found in employee security awareness and training programs. Employee awareness is critical to the success of any security program, and 60% of respondents say they have an employee security awareness training program in place. Because adversaries often target employees with social engineering schemes, 100% of respondents should implement an effective employee-training program.

"We see a lot of attacks that target what is in the employee's hands," **says Susan Mauldin, chief security officer for Equifax, the global consumer credit-reporting agency.** *"Because of this, our employee training and awareness is role-based and targets high-risk groups such as call-center employees, privileged users, and executives, with current training exercises focusing on targeted phishing attacks."*

To gauge respondents' priorities in preparing for the threats of tomorrow, we looked at priorities for implementation of process and technology safeguards over the next 12 months. We were interested in five categories in particular: protection of critical assets, infrastructure security, security threats, analytics, and mobile device security.

Effective security today requires that organizations identify and prioritize protection of "crown jewels." Twenty-five percent (25%) of respondents say they will prioritize over the next 12 months deployment of a program to identify sensitive assets, and 17% say they will prioritize asset management tools. (Figure 11) These types of solutions provide a key way to understand, value, and manage an organization's sensitive data.

Figure 11: Safeguards not in place but a top priority over the next 12 months



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

To enhance infrastructure security, almost one in four (24%) respondents say they will implement security standards for external partners, suppliers, vendors, and customers. This is critical as more organizations open their networks, applications, and data to third parties. What's more, technologies such as virtualization and cloud services have amplified the potential for compromise by a privileged inside user. Consequently, monitoring and managing privileged users is now a key challenge; we found that 17% of respondents plan to add privileged user access management tools over the next 12 months.

Other priorities focus on technologies that can help gain a better understanding of threats as well as improve security for mobile devices. For the first time, we asked respondents if they plan to add threat-intelligence subscription services as a means to obtain third-party assistance and early warnings about threat-intelligence risks and zero-day vulnerabilities. And many are: 49% of respondents say they currently use threat-intelligence subscription services, and among those that do not, 25% said implementation of these services would be a priority over the next 12 months.

At Equifax, top priorities include hardening employee devices in ways that will enable the financial services company to better understand threat actors. "We are taking a look at hardware that is used by employees and are basically sandboxing the environment to shield the computers from viruses and malware," Mauldin says. "This addresses risk, but it also helps us determine what types of threats are incoming and who is looking at Equifax as a target."

Given the soaring interest in Big Data, we also wondered whether organizations plan to leverage analytics as a means to improve security. It's a strategy that is gaining favor: Twenty percent (20%) of respondents say they will prioritize security information and event-management tools, and an equal number say security event-correlation technologies are a top priority.

"These types of technologies can help organizations detect patterns and anomalies in activity that can provide insight and intelligence on cyber threats facing the business," says Prakash Venkata, PwC Managing Director. "Armed with this insight, business leaders can anticipate and dynamically react to changes in their companies' cyber threat profile."

Another front-burner issue is mobile device security. Almost one in four respondents say they plan to prioritize encryption of smartphones, add mobile device management (MDM) solutions, and implement a strategy for the use of personal devices on the enterprise network.

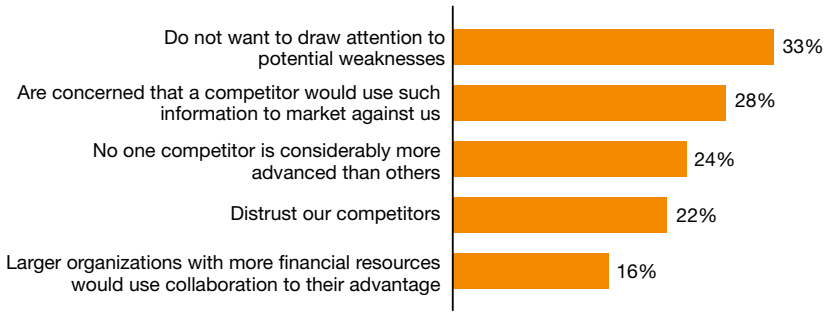
In the past year, sharing information about security threats—even among competitors—has emerged as a powerful offensive tool. We believe that collaboration can enable a business to more quickly adapt to market changes. In PwC's 5th Annual Digital IQ Survey,[5] we found that firms with collaborative C-suites intertwine business strategy and IT, which often improves the performance of a business.

So we were curious how global respondents, many of whom operate in an increasingly competitive environment, would view collaboration with others to improve security and share knowledge of threats. Many organizations see the merits of collaboration: We found that 50% of respondents say they collaborate with others, and among leaders, that number rises to 82%.

Equifax provides an example. "We participate in FS ISAC (the Financial Services Information Sharing and Analysis Center)," CSO Mauldin says. "This is very important to us because many government agencies also participate in FS ISAC, and it provides a proactive way to learn about evolving threats." Equifax participates in several other industry groups, and also collaborates with peers.

Among the 28% of respondents that do not collaborate, primary reasons for not sharing information include concerns about accentuating weaknesses, worries that a competitor might use information to its favor, and frank distrust of competitors. (Figure 12) Finally, 22% of respondents do not know if their organization collaborates with others.

Figure 12: Reasons for not collaborating on information security



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

[5] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013

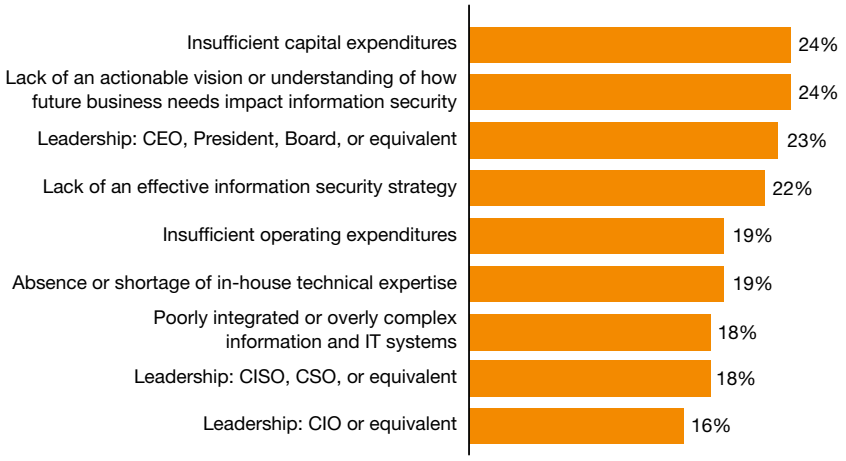
Obstacles to advancing security

While most security stakeholders agree that action should be taken to improve information security, there appears to be little consensus about the challenges of doing so. We asked respondents to identify the greatest obstacles to better security. The answers revealed a wide range of diverging opinions and, in some cases, finger pointing.

Overall, survey respondents say the most significant obstacles include insufficient capital funding, inadequate understanding of how future business needs will impact information security, committed leadership, and a lack of an effective security strategy. (Figure 13) Given the upward tick in security budgets this year, concern about funding may take care of itself. But it is troubling that deeply fundamental issues such as the understanding and alignment of security with future business needs and the efficacy of security strategies are among top concerns. Respondents are also very likely to point to executive leadership, the CEO in particular, as a top impediment to improved security.

And who or what do CEOs blame? Interestingly, chief executives overwhelmingly named themselves as obstacle No. 1. CFOs, meanwhile, point to CEOs as the leading hindrance, followed by the CIO, CISO, and CSO. Ask CISOs, the executives directly responsible for information security, and they'll put insufficient funding (both capital and operating) at the top of the list, followed by a lack of in-house technical expertise. CIOs flag a lack of strategy and vision, along with leadership of CEOs and security executives.

Figure 13: Greatest obstacles to improving information security



Note: Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

"This lack of clarity on obstacles to effective security shows, in part, that businesses have not engaged in sufficient dialogue around security. In this dialogue, employees, executives, and third parties all understand their role in information security, key priorities, and the biggest risks," **says David Burg, PwC Principal.** *"Building and sustaining a culture of security awareness will also require the full support of top executives, including the CEO and board. This must be an ongoing discussion."*

The global cyber-defense race

For several years, Asia Pacific has taken the lead in investment in security technologies, processes, and spending. As a result, the region pulled ahead of others in developing and implementing effective security programs. (Figure 14)

And it still holds the top spot. In fact, 28% of those whom we identify as leaders are from Asia Pacific, which represents only 21% of overall total respondents.

But Asia Pacific's high ranking in security practices is being vigorously challenged by South America. For the first time, South America seems poised to take the lead in information security investments, policies, and safeguards. The continent leads in key factors like security spending and employment of a CISO to oversee security, and is neck and neck with Asia Pacific in many others.

Nonetheless, Asia Pacific remains very strong in security spending and leading practices. Europe and North America, on the other hand, lag in many aspects, including employment of a CISO, inclusion of key policies such as backup and recovery/business continuity, and collaboration with others. North America exhibits some key strengths, such as requiring third parties to comply with privacy policies and employee awareness and training, but is behind in many other measures.

Figure 14: Security practices by region

	South America	Asia Pacific	Europe	North America
Security spending will increase over the next 12 months	66%	60%	46%	38%
Have an overall security strategy	75%	79%	77%	81%
Employ a Chief Information Security Officer	75%	74%	68%	65%
Have a senior executive who communicates the importance of security	68%	69%	51%	55%
Measured/reviewed effectiveness of security policies and procedures in past year	70%	69%	53%	49%
Have policy for backup and recovery/ business continuity	58%	55%	45%	47%
Require third parties to comply with privacy policies	55%	58%	55%	62%
Employee security awareness training program	54%	63%	55%	64%
Have procedures dedicated to protecting intellectual property (IP)	20%	24%	17%	21%
Have intrusion-detection technologies in place	64%	67%	63%	67%
Inventory of where personal data are collected, transmitted, and stored	53%	60%	52%	64%
Collaborate with others to improve security and reduce risks	66%	59%	45%	42%

Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Asia Pacific—Still the pacesetter

Asia Pacific remains the pacesetter in security spending and practices. Security investment is strong: Average security budgets have increased 85% over last year, and at 4.3%, Asia Pacific reports the highest IS budget as a percent of overall IT spending. Respondents are optimistic on the future IS spend, with 60% saying their security budget will increase over the next 12 months. However, average financial losses due to security incidents are up 28% over last year.

Average security budgets have increased

85%

in Asia Pacific.

Asia Pacific matches South America in key policies like employing a CISO to oversee the security program. The region is also highly likely to have adopted progressive new security measures, such as having a senior executive who communicates the importance of security (69%) and collaborating with others to enhance

security (59%). It is also most likely to deploy intrusion-detection technologies (67%) and have an inventory of where personal data is collected, transmitted, and stored (60%) when compared to South America.

Yet a year-over-year comparison reveals that Asia Pacific is beginning to stall in implementation of certain security policies and technologies. For instance, the number of respondents who report they have a policy for backup and recovery/business continuity is down over last year, and other key policies such as employee training and procedures dedicated to protecting IP are essentially static.

China comprises 33% of Asia Pacific respondents in this survey, followed by India (31%) and Japan (17%). By most measures, China eclipses other countries in security practices and policies. For instance, 60% of respondents from China use behavioral profiling and monitoring, 73% have centralized user data storage, and 72% employ vulnerability scanning tools, all higher than adoption rates of other countries. Sixty-two percent (62%) of Asia Pacific respondents have protection/detection management solutions for APTs and 66% have implemented SIEM technologies, results that outstrip other nations. What's more, no country has implemented security policies for mobile devices, BYOD, and social media at a higher rate than China. For instance, 71% of respondents from China have a policy in place for the use of personal devices on the enterprise network, compared with 64% in the US and 54% in India. In comparison with China, India is making solid overall gains in security programs and policies but it lags China on almost all counts.

South America: A new powerhouse from the south

South America shows solid gains in security spending, policies, and technologies. By many measures, the region matches—and sometimes surpasses—Asia Pacific.

For instance, information security budgets have jumped 69% over last year, and 66% of South America respondents say security spending will increase over the next 12 months. Security budgets comprise 4.1% of the overall IT spend, higher only in Asia Pacific. South America respondents are most likely to employ a CISO (75%) and to have a policy for backup and recovery/business continuity (58%). The continent leads in collaborating with others (66%) and is essentially tied with Asia Pacific in progressive policies such as having a senior executive who communicates the importance of security (68%). Average total financial losses due to security incidents are up modestly (4%) compared with last year.

75% *of South America respondents say their organization employs a CISO.*

Respondents from Brazil comprise the largest percentage of South America respondents (48% of the total), followed by Mexico (30%), and Argentina (21%). Brazil ranks high in many measures—behavioral profiling and monitoring (57%) and use of vulnerability scanning tools (63%), for instance—but generally lags China and the US.

South America is not without weaknesses. For instance, the percentage of respondents who say their organization has a policy for employee security awareness training is comparatively low at 54%, as is those who have an inventory of locations where personal data are collected, transmitted, and stored (53%).

Financial losses due to security incidents in Europe increased

28%

over last year.

Europe: Falling behind in funding and safeguards

Unlike other regions, investment in information security is down slightly (3%) over last year in Europe, and the continent continues to lag in adoption of key security safeguards.

In addition to a slight degradation of security investments, only 46% of European respondents believe security spending will increase over the next 12 months. While the number of detected security incidents is down 22% over last year, average financial losses due to security incidents shows a 28% increase.

Implementation of important policies, including backup and recovery/ business continuity (45%) and security awareness training and communications (21%), are comparatively low in Europe. Also lacking is the number of respondents who say they collaborate with others (45%) and those who have a mobile security policy (38%).

North America: Lagging and leading

Investment in security is soaring in North America, as is the number of detected security incidents. And while adoption of key policies remains low, North America leads in some important areas.

Average security budgets are up 80% over last year, although the outlook for future spending in the coming year is the lowest among all regions: Only 38% of North America respondents say security spending will increase over the next 12 months. The number of detected security incidents jumped 117% over 2012, while the average financial losses due to security incidents increased 48%.

North America leads other regions in some key practices, including having an overall security strategy (81%), requiring third parties to comply with privacy policies (62%), and employee security awareness training (64%). It also is most likely to inventory, collect, transmit, and store personal data (64%) and to use intrusion-detection technologies (67%). On the downside, North America is behind other regions in collaborating with others (42%) and employment of a CISO (65%). North American respondents are also least likely to

In North America, detected incidents increased

117%

over last year.

have reviewed the effectiveness of their security practices within the past year.

The US, which comprises 84% of North America respondents, ranks high in strategies for cloud computing (52%), mobile device security (60%), social media (58%), and BYOD (64%), second only to China in most factors.

What this means for your business

One thing is certain: yesterday's security defenses are not effective against today's rapidly evolving threats.

The results of The Global State of Information Security® Survey 2014 capture information security at an uncertain juncture, simultaneously poised on the threshold of change and stalled at the inertia of the status quo. Respondents demonstrate progress in deploying important new security safeguards on one hand, and inattention to key strategies like protection of intellectual property on the other. A renewed commitment to investing in security alongside an uncertain direction on how to improve practices.

Given the enormous changes and challenges wrought by today's evolving threat ecosystem, it's not entirely surprising that the way forward is ambiguous.

One thing is certain: Yesterday's security defenses are not effective against today's rapidly evolving threats. And the risks of tomorrow—uncertain at best and perilous at worst—will demand a completely new model of information security.

We suggest an evolved approach to what security can be, one that is driven by knowledge of threats, assets, and adversaries. One in which security incidents are seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels.

We call this model Awareness to Action. At its most basic, this approach comprises four key precepts:

- **Security is a business imperative:** Effective security requires that you understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem. An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.
- **Security threats are business risks:** You should view security risks as organizational threats. It is critical to anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks. Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security policies and practices.
- **Protect the information that really matters:** Effective security requires that you understand and adapt to changes in the threat environment by identifying your most valuable information. Know where these "crown jewels" are located and who has access to them at all times, and proficiently allocate and prioritize your organization's resources to protect its most valuable information.
- **Gain advantage from Awareness to Action:** In this new model of information security, all activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring. You should create a culture of security that starts with commitment of top executives and cascades to all employees and third parties. Engage in public-private collaboration with others for enhanced threat intelligence.

We can help you understand the implications of this new approach to information security and apply the concepts to the unique needs of your business, your industry, and your threat environment. Let us show you how to effectively combat the security threats of today and plan for those of tomorrow.

For more information, please contact:

Gary Loveland
Products & Services Industries
949 437 5380
gary.loveland@us.pwc.com

John Hunt
Public Sector
703 918 3767
john.d.hunt@us.pwc.com

Mark Lobel
Products & Services Industries
646 471 5731
mark.a.lobel@us.pwc.com

Dave Burg
Forensic Services
703 918 1067
david.b.burg@us.pwc.com

Joe Nocera
Financial Services Industry
312 298 2745
joseph.nocera@us.pwc.com

Dave Roath
Risk Assurance Services
646 471 5876
david.roath@us.pwc.com

Peter Harries
Health Industries
213 356 6760
peter.harries@us.pwc.com

Or visit: www.pwc.com/gsiss2014 to explore the data for your industry and benchmark your organization.

www.pwc.com/security

Defending yesterday

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

Key findings from The Global State of Information Security® Survey 2014

September 2013

pwc

Threats advance faster than security

While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders can bypass perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical.

Incidents increase in a new world of risk

The results of The Global State of Information Security® Survey 2014 show that executives are heeding the need to fund enhanced security activities and have substantially improved technology safeguards, processes, and strategies. Budgets are rising and confidence continues to climb.

But while many organizations have raised the bar on security, their adversaries have done better.

This year's survey shows that detected security incidents have increased, as has the cost of breaches. And hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured. Many executives are hesitant to share security intelligence with others, forgoing a powerful offensive tool against targeted, dynamic attacks.

Gain advantages with an evolved approach to security

If few organizations have kept pace with today's escalating risks, fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," says Gary Loveland, a principal in PwC's security practice. "What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."

This evolved approach requires that organizations identify their most valuable assets and prioritize protection. Security incidents should be seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. And it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

In this new model of information security, knowledge is power. Seize it.

Agenda

Section 1

Methodology

A global, cross-industry survey of business and IT executives

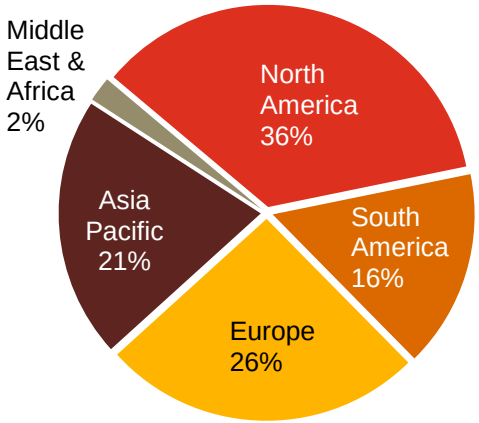
The Global State of Information Security® Survey 2014, a worldwide study by PwC, *CIO* magazine, and *CSO* magazine, was conducted online from February 1, 2013 to April 1, 2013.

- PwC's 16th year conducting the online survey, 11th with *CIO* and *CSO* magazines
- Readers of *CIO* and *CSO* magazines and clients of PwC from 115 countries
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-nine percent (39%) of respondents from companies with revenue of $500 million+
- Thirty-six percent (36%) of respondents from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa
- Margin of error less than 1%; numbers may not add to 100% due to rounding

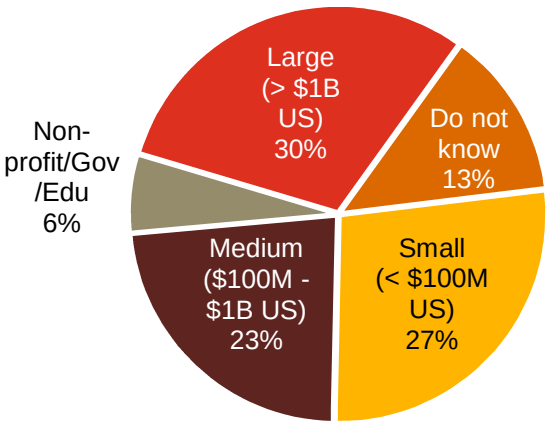
Demographics

30% of respondents work for large organizations (more than $1 billion in revenue), an increase of 22% over last year.

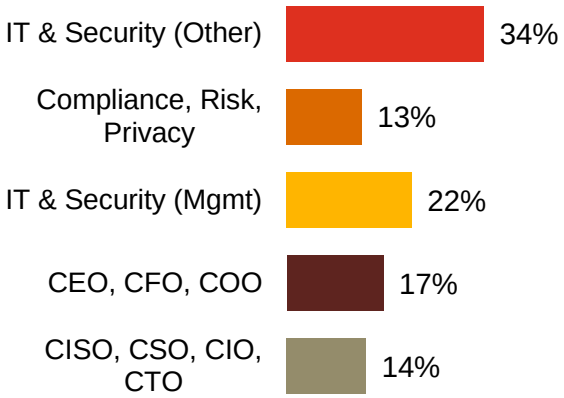
Respondents by region of employment



Respondents by company revenue size



Respondents by title



(Numbers reported may not reconcile exactly with raw data due to rounding)

Survey response levels by industry

Number of responses this year	
Technology	1,226
Financial Services	993
Retail & Consumer	820
Public Sector	694
Industrial Products	671
Telecommunications	456
Healthcare Providers	398
Entertainment & Media	221
Automotive	209
Aerospace & Defense	193
Power & Utilities	143
Oil & Gas	107
Pharmaceutical	74

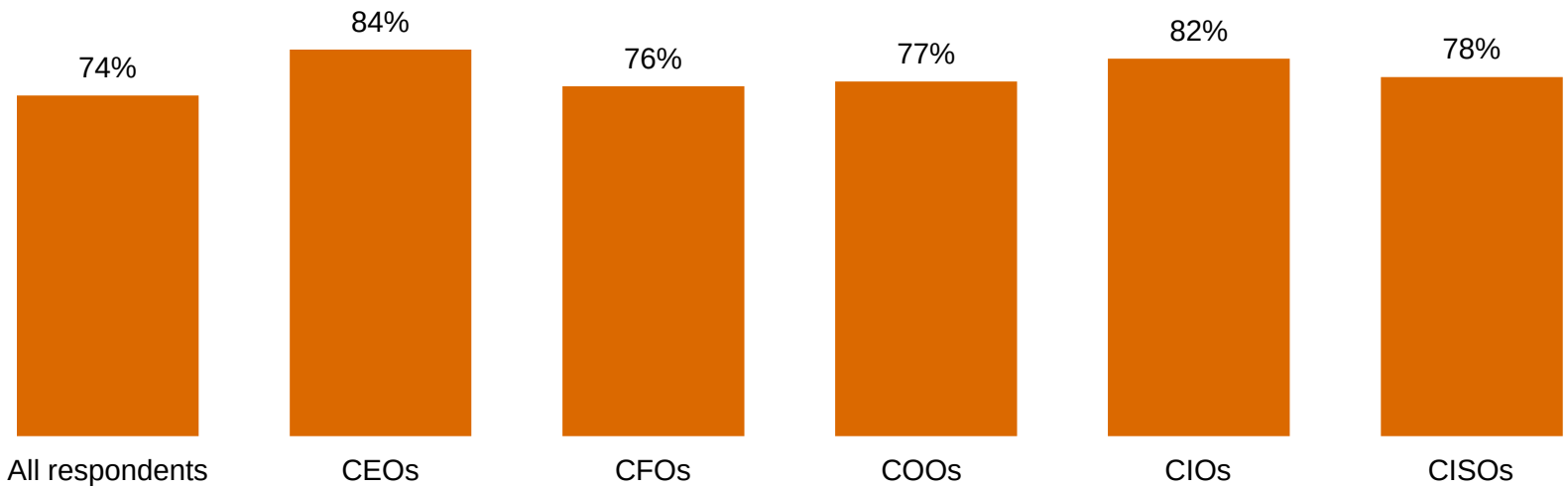
Section 2

Confidence in an era of advancing risks

Confidence is high: 74% of respondents believe their security activities are effective, with top execs even more optimistic.

In the C-suite,* 84% of CEOs say they are confident in their security program. Note that CFOs are the least confident among executives.

Executive confidence in effectiveness of security activities (somewhat or very confident)

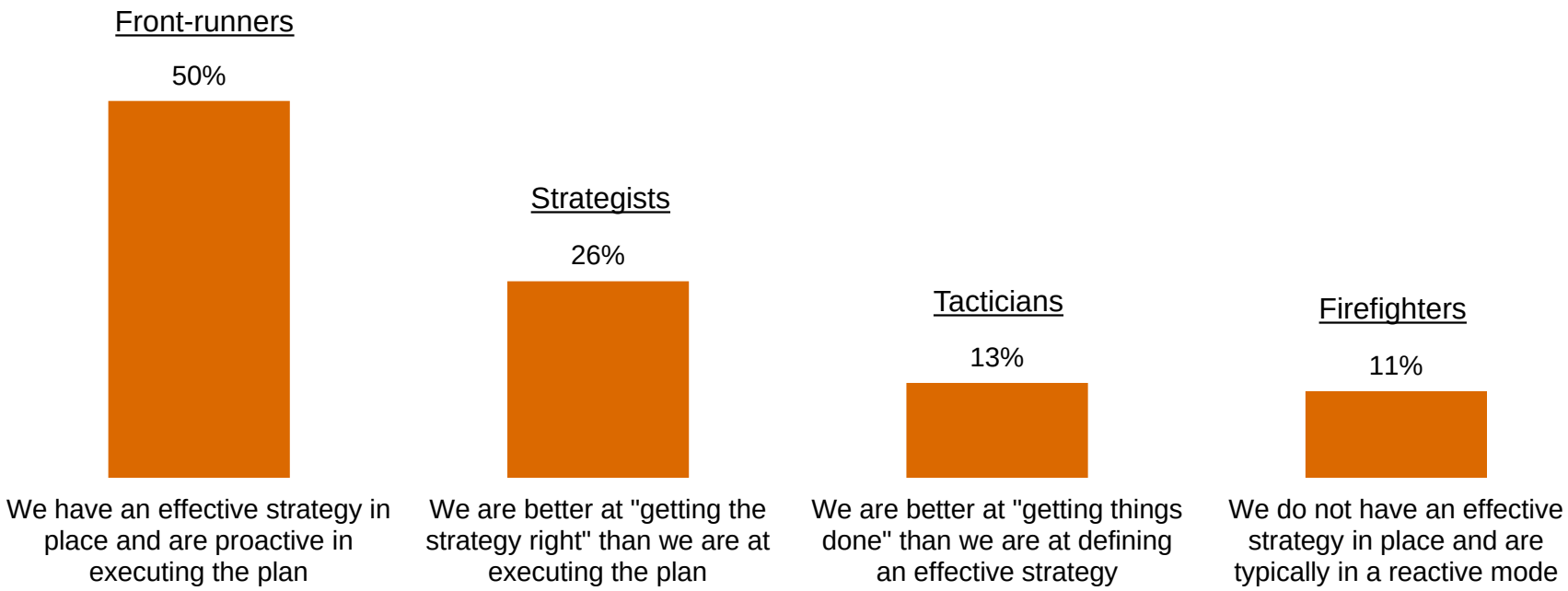


* CEOs, CFOs, and COOs

Question 39: “How confident are you that your organization’s information security activities are effective?” (Respondents who answered “Somewhat confident” or “Very confident.”) Question 1: “My job title most closely resembles”

Half of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices.

50% say they have an effective strategy in place and are proactive in executing the plan, a 17% increase over last year. About one in four (26%) say they are better at getting the strategy right than executing the plan.



Question 27: "Which statement best characterizes your organization's approach to protecting information security?"

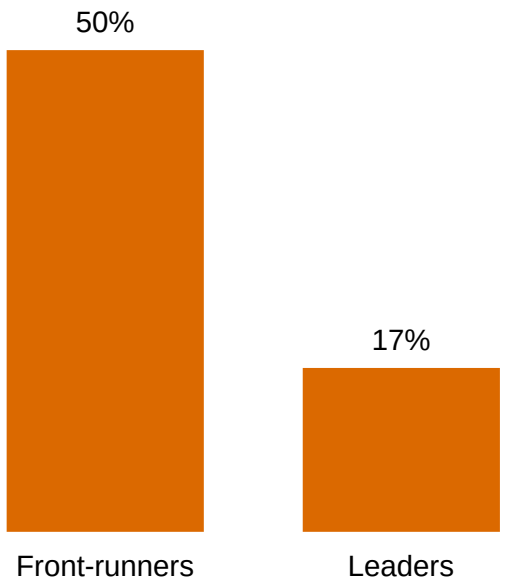
But closer scrutiny reveals far fewer real leaders than front-runners.

We measured respondents' self-appraisal against four key criteria to filter for leadership.

To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are still significantly fewer real leaders than self-identified front-runners.

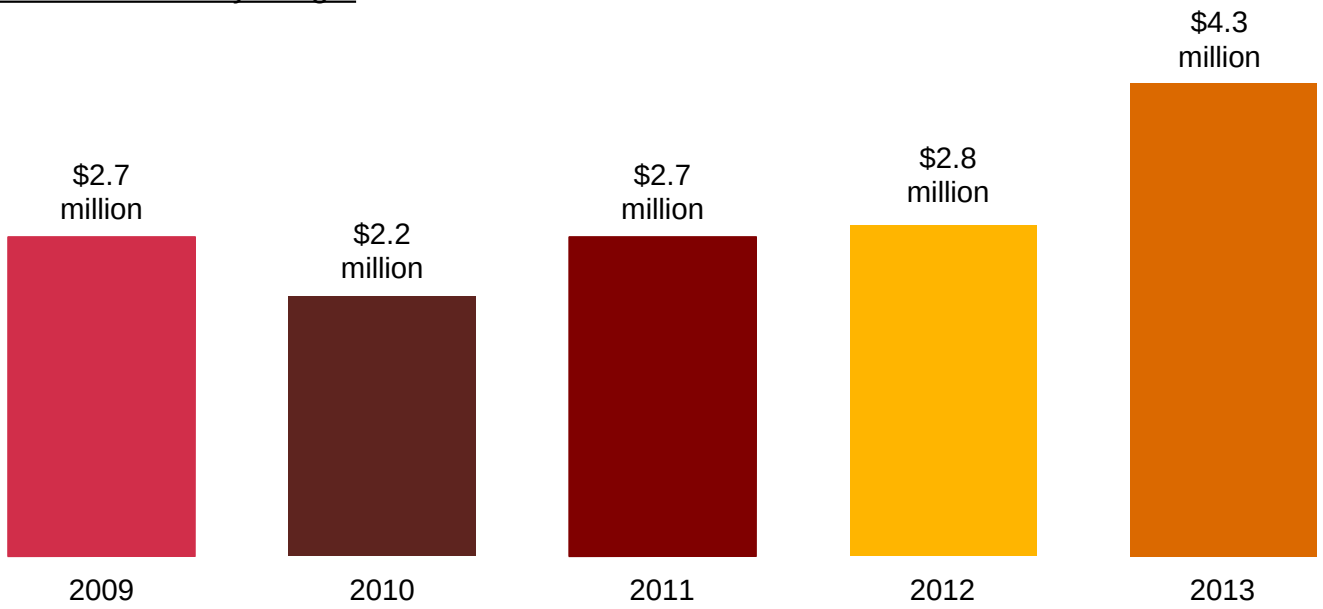


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Information security budgets increase significantly.

Security budgets average $4.3 million this year, a gain of 51% over 2012. Organizations understand that today's elevated threat landscape demands a substantial boost in security investment.

Average information security budget



Question 8: "What is your organization's total information security budget for 2013?"

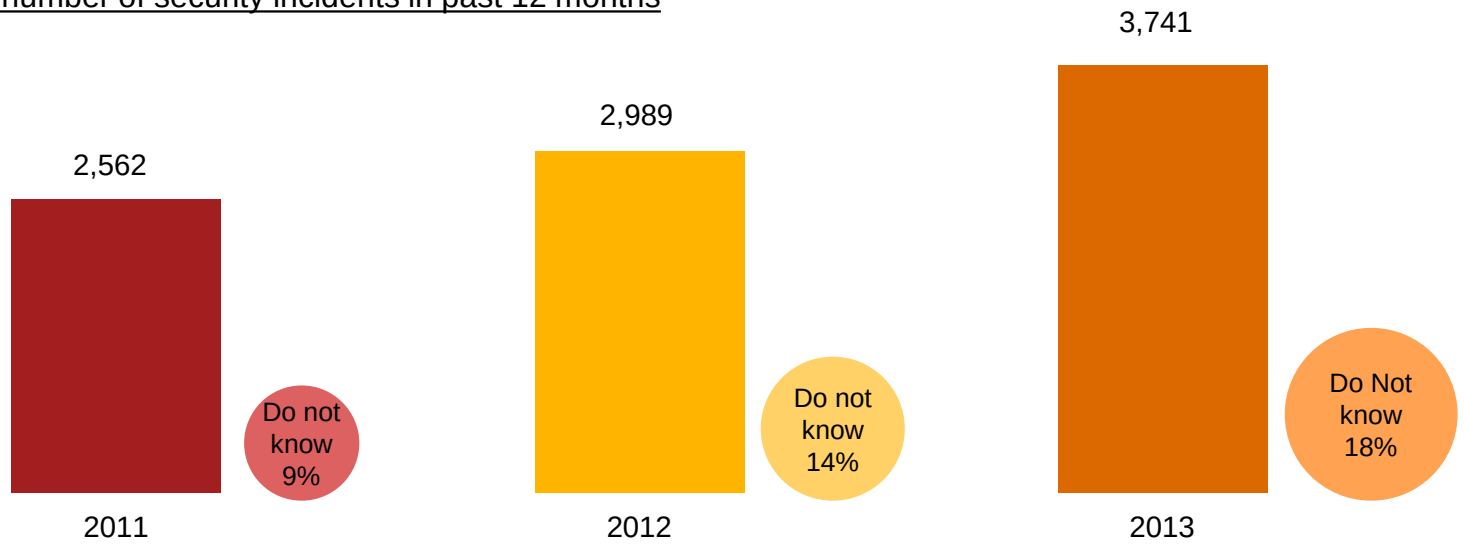
Section 3

Today's incidents, yesterday's strategies

*Respondents are detecting more security incidents.**

The number of incidents detected in the past 12 months increased by 25%, perhaps an indication of today's elevated threat environment. It is troubling that respondents who do not know the number of incidents has doubled over two years. This may be due to continued investments in security products based on outdated models.

Average number of security incidents in past 12 months



* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months?"

A US-only survey shows that, even when in place, security technologies and policies often do not prevent incidents.

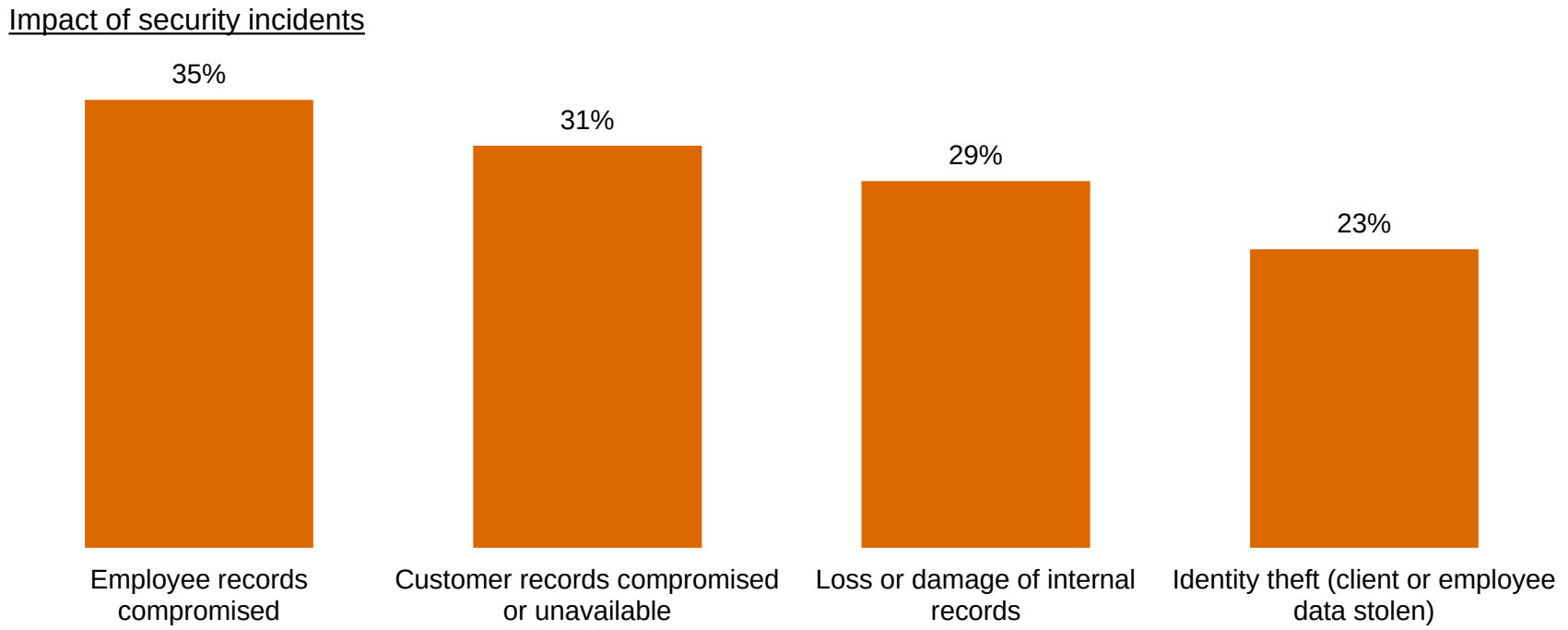
Respondents to the 2013 US State of Cybercrime Survey,[1] co-sponsored by PwC, say security incidents increased 33%, despite implementation of security practices. For many, existing security technologies and policies are simply not keeping pace with fast-evolving threats.

Security technologies and policies in place (US only)	
Use policy-based network connections to detect and/or counter security incidents	68%
Inspect inbound and outbound network traffic	61%
Use account/password management in an attempt to reduce security incidents	60%
Have an acceptable-use policy	55%
Use malware analysis as a tool to counter advanced persistent threats (APTs)	51%
Use data loss prevention technology to prevent and/or counter security incidents	51%
Use security event management to detect and/or counter security incidents	50%
Use cyber-threat research in an attempt to reduce security incidents	25%
Do not allow non-corporate-supplied devices in the workplace/network access	17%

[1] *2013 US State of Cybercrime Survey*, co-sponsored by *CSO* magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

Employee and customer data continue to be easy targets.

Compromise of employee and customer records remain the most cited impacts, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records jumped more than 100% over last year.

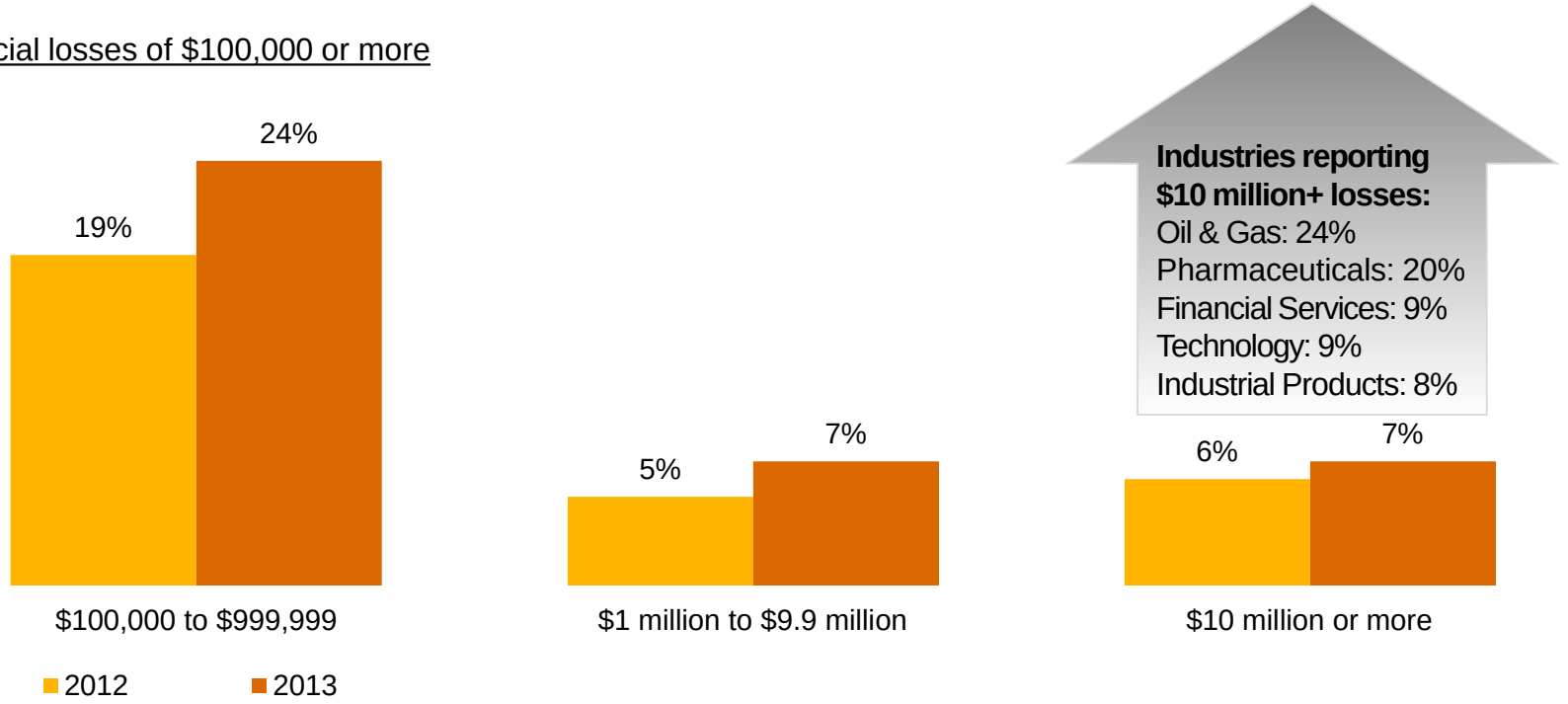


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

The financial costs of incidents are rising, particularly among organizations reporting high dollar-value impact.

Average losses are up 18% over last year, which is not surprising given the costs and complexity of responding to security incidents. Big liabilities are increasing faster than smaller losses: Respondents reporting losses of $10 million-plus is up 51% from 2011.

Financial losses of $100,000 or more

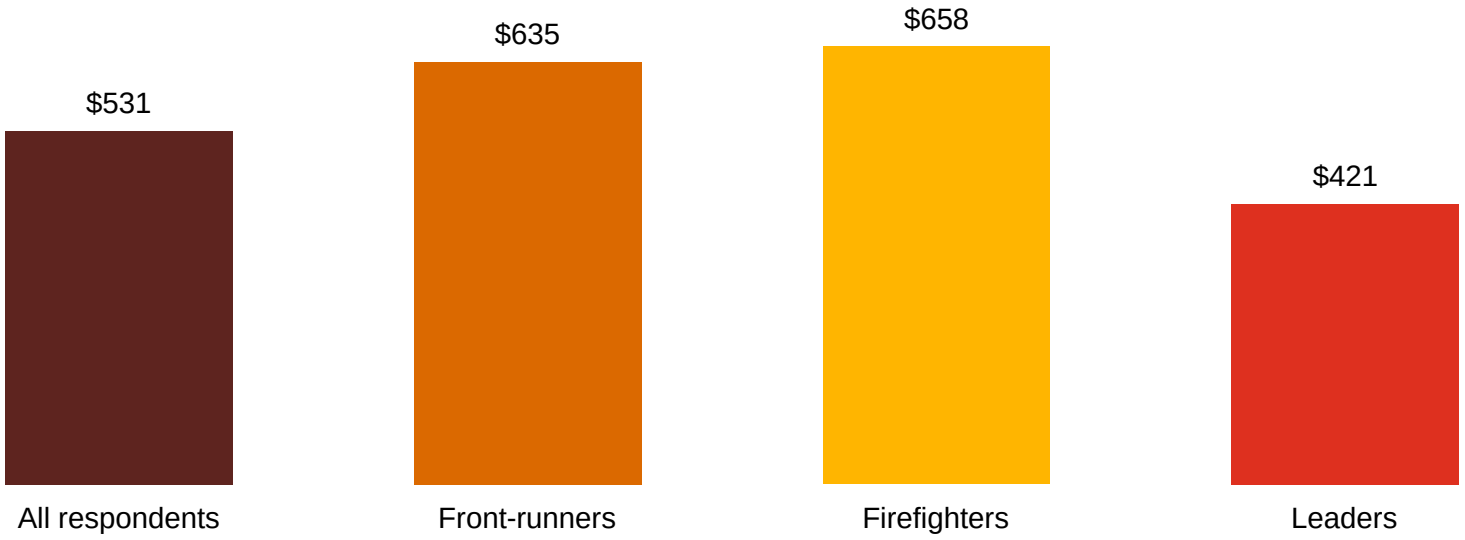


Question 22A: “Estimated total financial losses as a result of all security incidents”

Organizations that identify as front-runners report a high cost per security incident; leaders claim the lowest cost.

Front-runners spend almost as much per incident as firefighters—those least prepared to run an effective security program.

The average cost per security incident

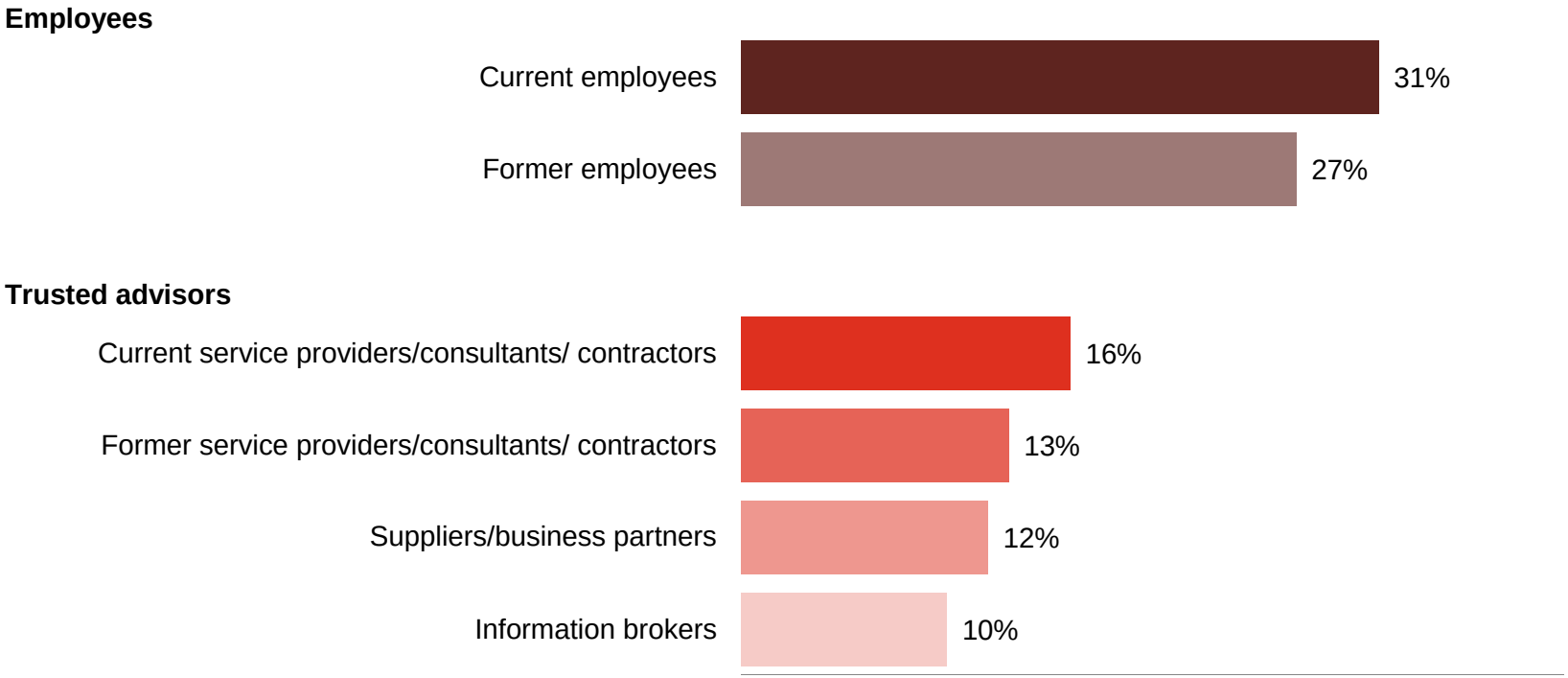


Question 18: “What is the number of security incidents detected in the past 12 months?” Question 22A: “Estimated total financial losses as a result of all security incidents”

Insiders, particularly current or former employees, are cited as a source of security incidents by most respondents.

It's the people you know—current or former employees, as well as other insiders—who are most likely to perpetrate security incidents.

Estimated likely source of incidents

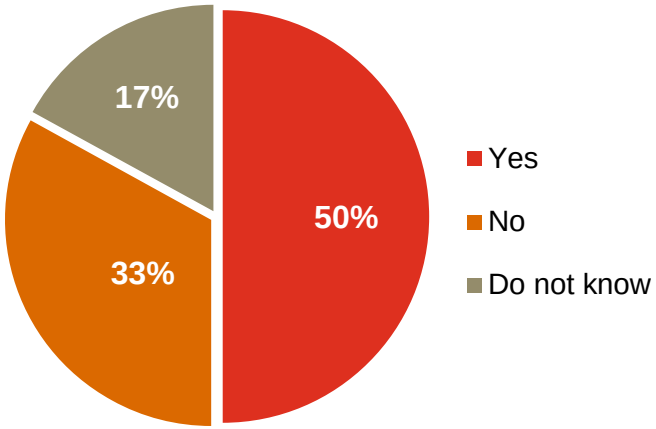


Question 21: "Estimated likely source of incidents" (Not all factors shown.)

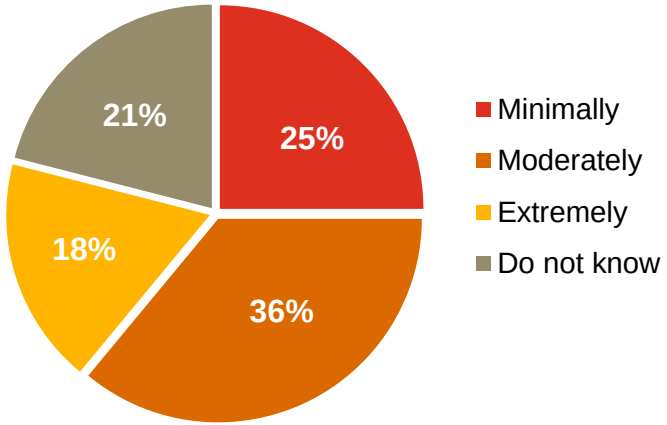
Yet many organizations do not have plans for responding to insider threats, and those that do are not highly effective.

The 2013 US State of Cybercrime Survey[2] shows that many organizations have not implemented effective strategies for responding to in-house adversaries.

Organization has a formal plan for responding to insider security incidents



Organization is effective in reporting, managing, and intervening cyber threats with internal employees

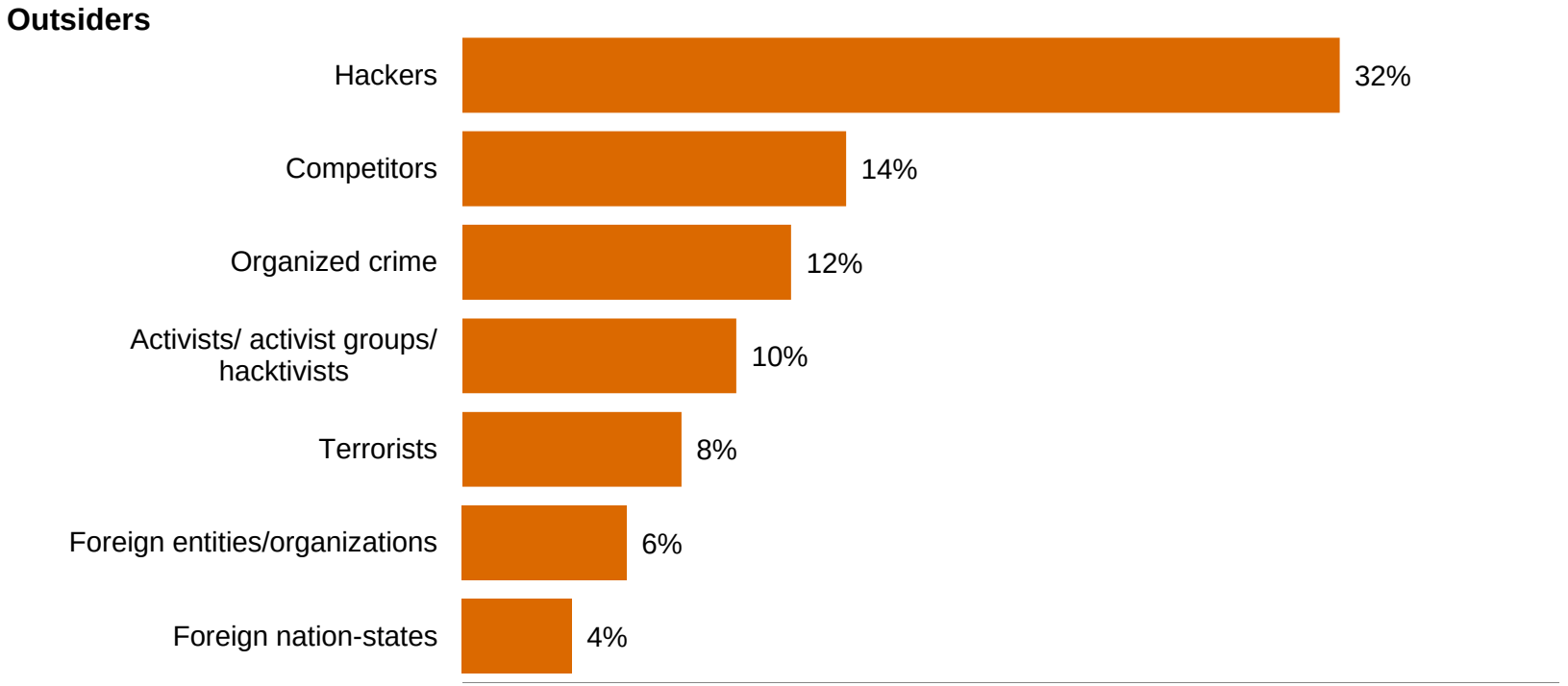


[2] *2013 US State of Cybercrime Survey*, co-sponsored by *CSO* magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

While attacks backed by nation-states make headlines, your organization is more likely to be hit by other outsiders.

Only 4% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger.

Estimated likely source of incidents



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

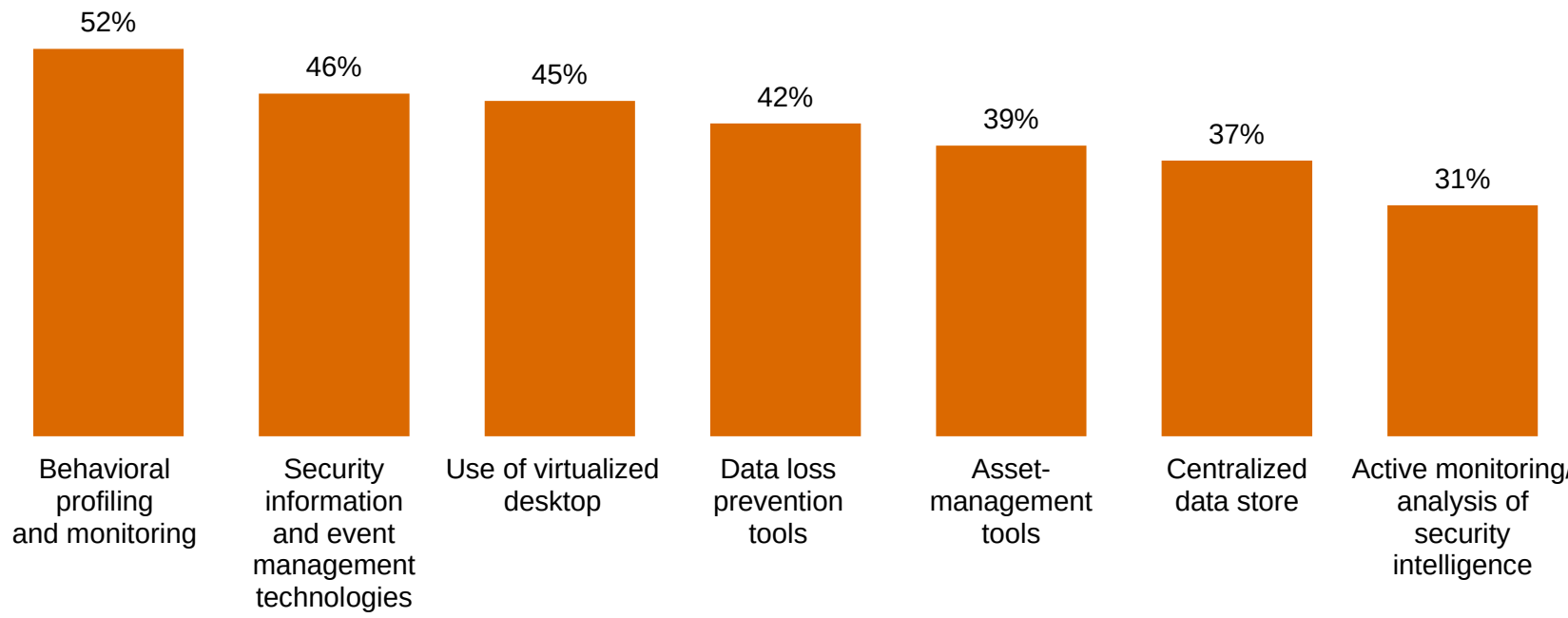
Section 4

A weak defense against adversaries

Many organizations have not implemented technologies and processes that can provide insight into today's risks.

Security safeguards that monitor data and assets are less likely to be in place. These tools can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

Respondents who answered security safeguards ARE NOT currently in place



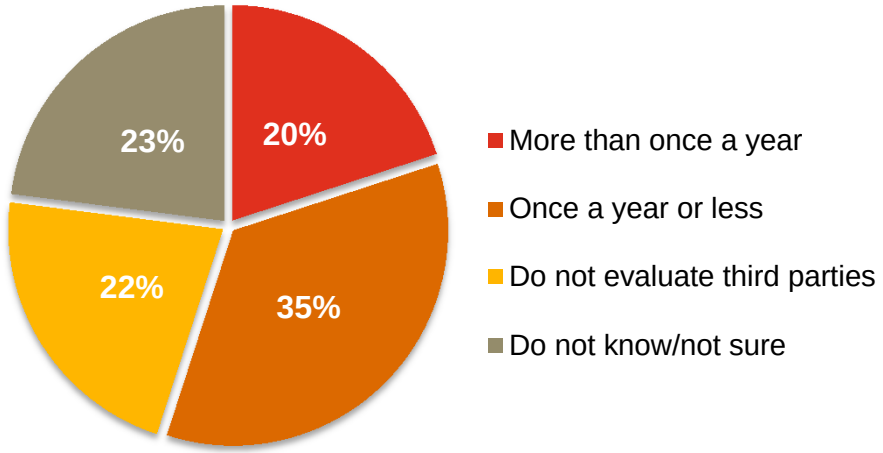
Question 14: "What process information security safeguards does your organization currently have in place?" Question 15: "Which technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

In the US, many organizations lack an understanding of risks associated with third parties.

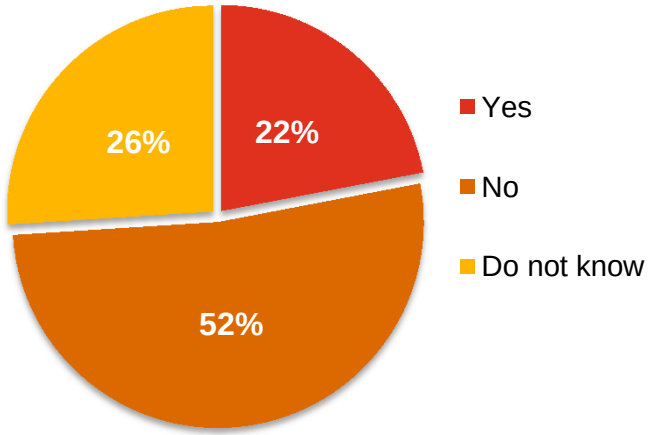
The 2013 US State of Cybercrime Survey[3] found that many respondents do not have policies and tools to assess security risks of third parties. More than ever, company leaders should not view cybersecurity as simply a technology problem; it is now a risk-management issue.

Does your organization:

Evaluate the security of third parties with which the organization shares data or network access?



Conduct incident response planning with third-party supply chain?

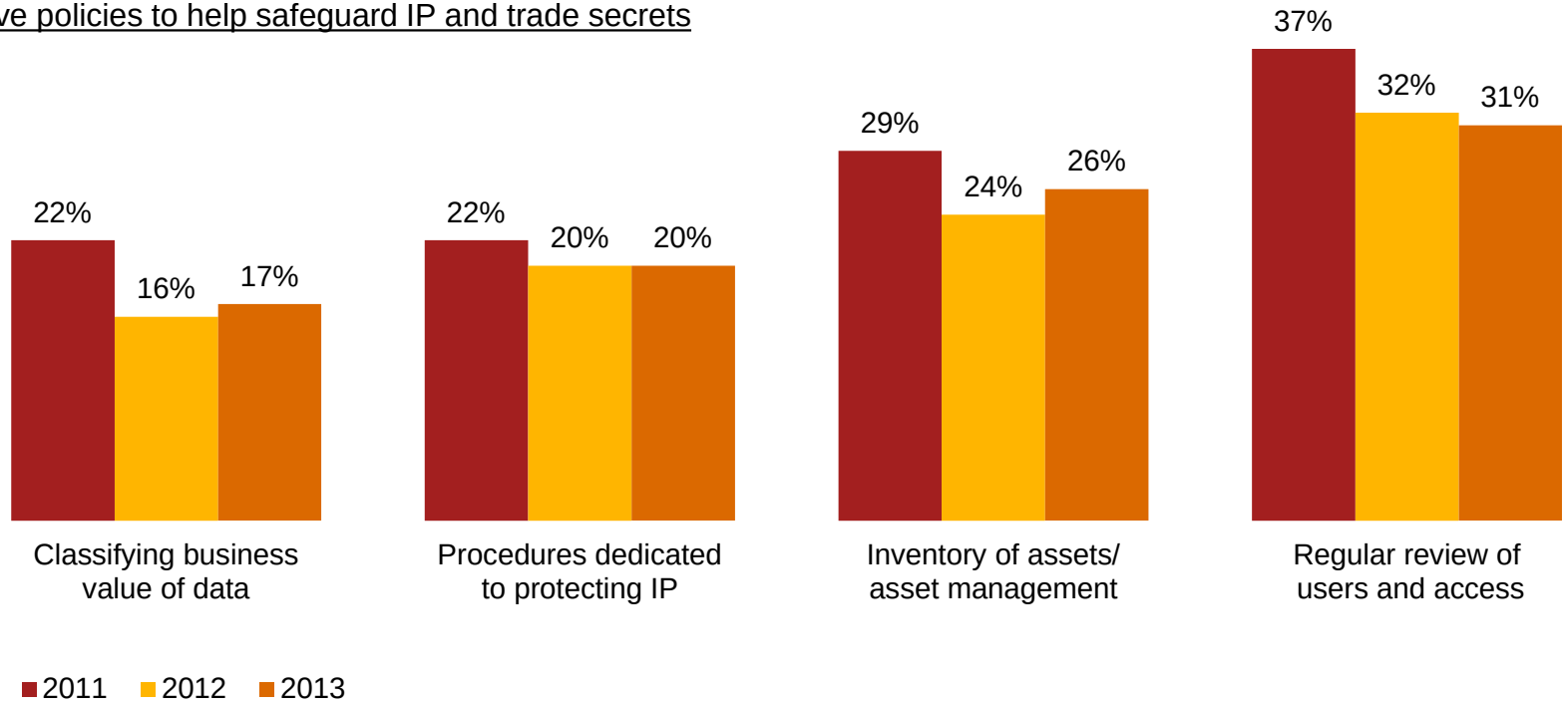


[3] *2013 US State of Cybercrime Survey*, co-sponsored by *CSO* magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

Despite the potential consequences, many respondents do not adequately safeguard their high-value information.

It is imperative that organizations identify, prioritize, and protect their "crown jewels." Many, however, have not yet implemented basic policies necessary to safeguard intellectual property (IP).

Have policies to help safeguard IP and trade secrets

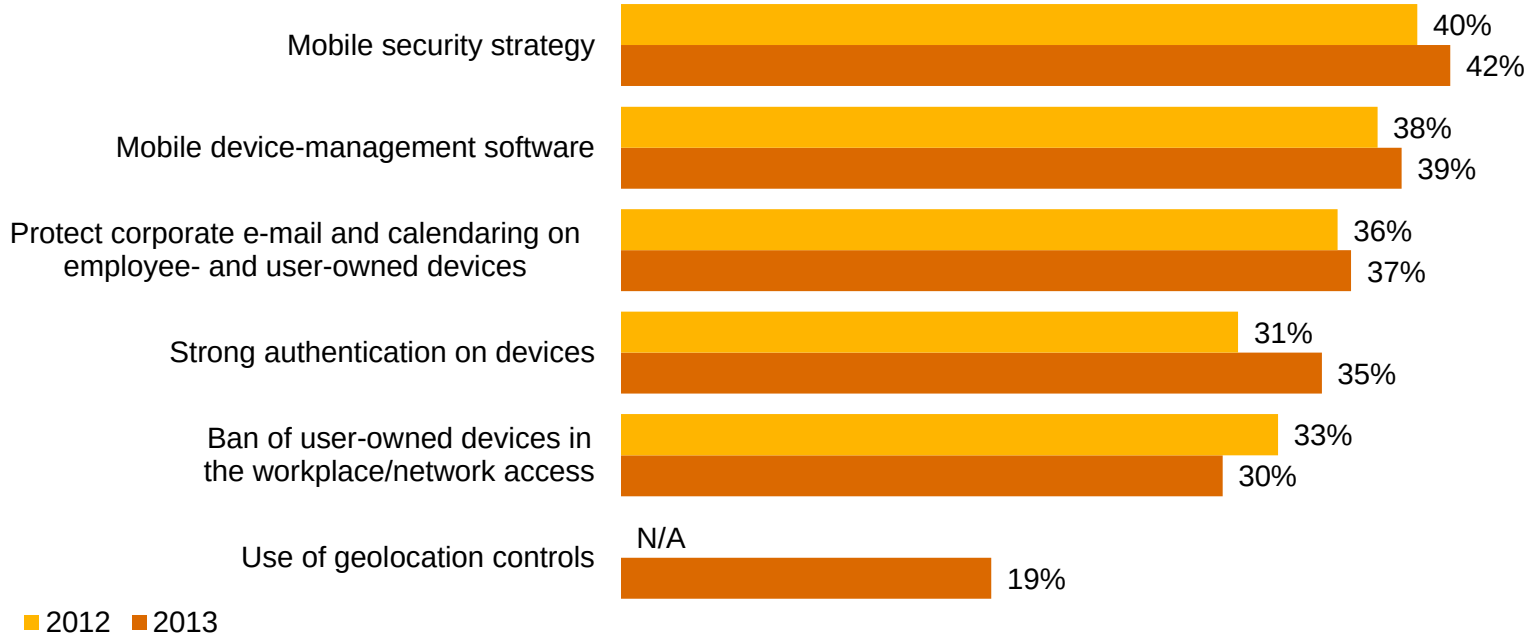


Question 32: "Which of the following elements, if any, are included in your organization's security policy?" (Not all factors shown.)

Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace with use.

Smart phones, tablets, and the "bring your own device" trend have elevated security risks. Yet efforts to implement mobile security programs do not show significant gains over last year, and continue to trail the proliferating use of mobile devices.

Initiatives launched to address mobile security risks

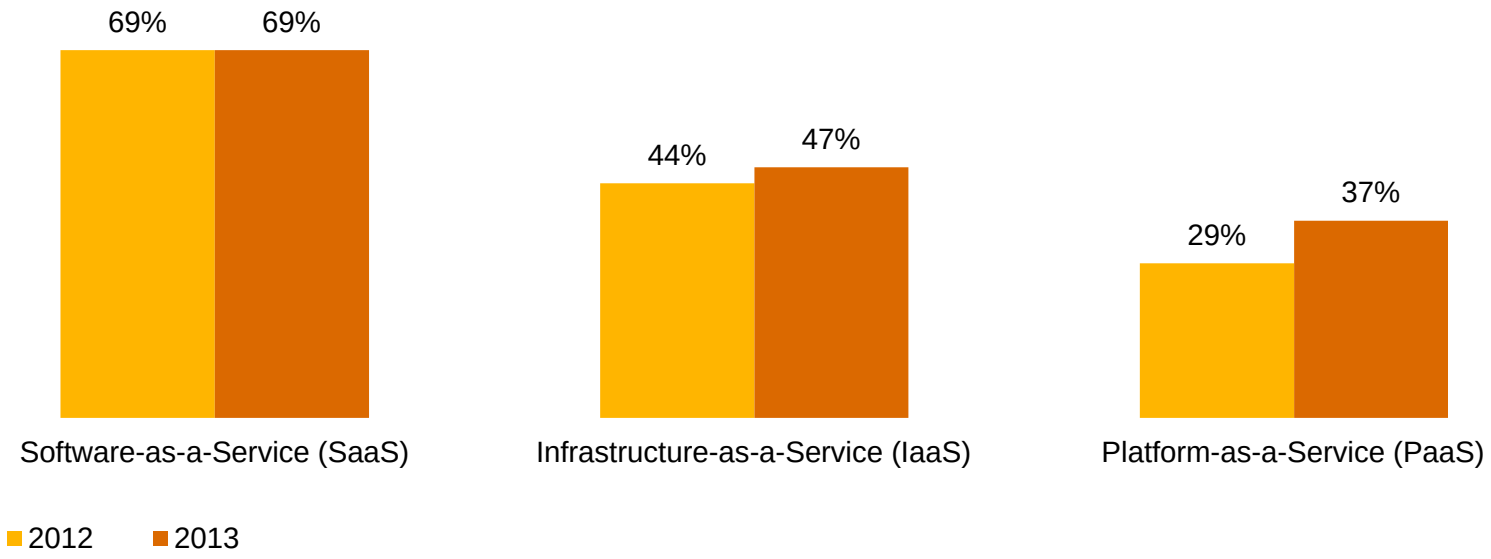


Question 16: "What initiatives has your organization launched to address mobile security risks?" (Not all factors shown.)

Almost half of respondents use cloud computing, but they often do not include cloud in their security policies.

While 47% of respondents use cloud computing—and among those who do, 59% say security has improved—only 18% include provisions for cloud in their security policy. SaaS is the most widely adopted cloud service, but PaaS shows strong growth.

Type of cloud service used



Question 32: “Which of the following elements, if any, are included in your organization’s security policy?” Question 42: “Does your organization currently use cloud services such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS)?” Question 42A: “What type of cloud service does your organization use?” Question 42C: “What impact has cloud computing had on your company’s information security?” (Not all factors shown.)

28% of respondents do not collaborate with others to improve security, forgoing a powerful offensive tool.

And that can impede security in today's interconnected world. In PwC's 5th Annual Digital IQ Survey,[4] we found that firms with collaborative C-suites intertwine business strategy and IT—and that often improves performance and enables quick adaption to market changes.

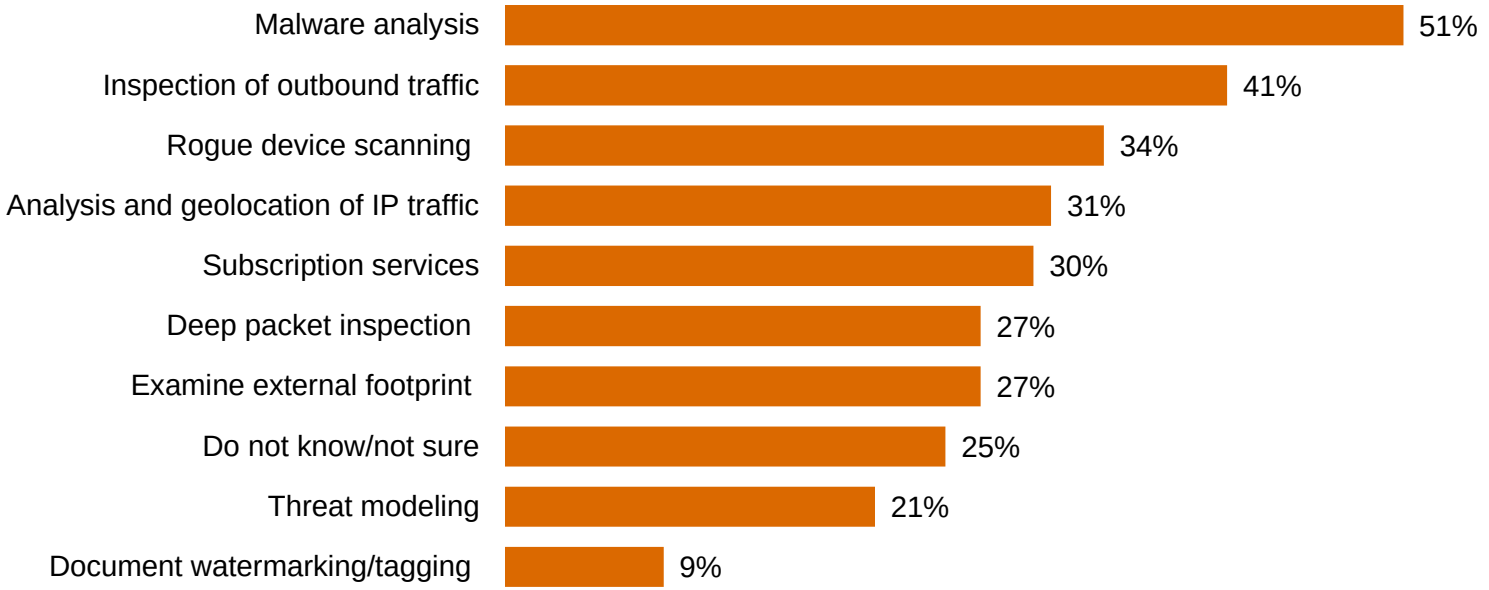
Reasons for not collaborating on information security

[4] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?" Question 41A: "Why doesn't your organization collaborate with others in the industry to improve security and reduce the potential for future risks?" (Not all factors shown.)

In the US, sophisticated threat-intelligence tools necessary to combat advanced persistent threats are largely absent.

Advanced persistent threats require a new information-protection model that focuses on continuous monitoring of network activity and high-value information. The 2013 US State of Cybercrime Survey[5] found that the majority of US organizations lack these capabilities.

Activities and techniques used to counter advanced persistent threats



[5] *2013 US State of Cybercrime Survey*, co-sponsored by *CSO* magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

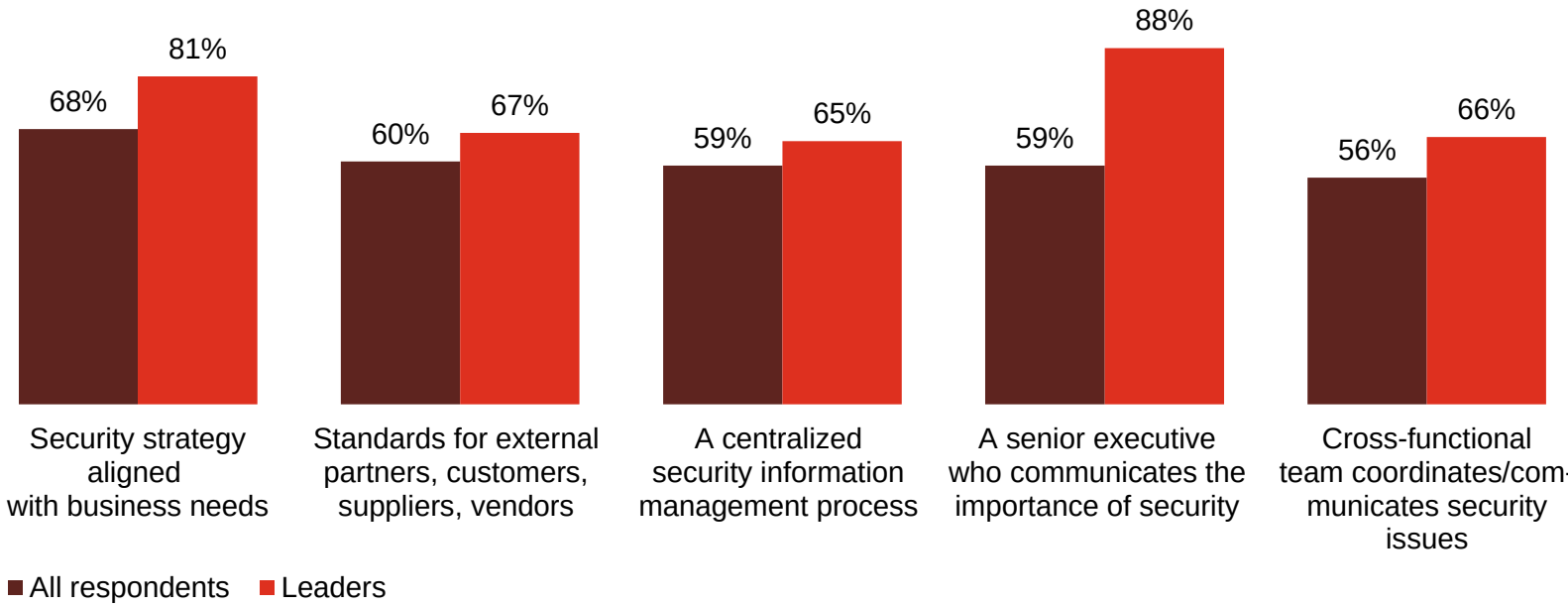
Section 5

Preparing for the threats of tomorrow

Leaders are enhancing capabilities in ways that show security is now a business imperative—not just an IT challenge.

Aligning security with business needs, setting standards for external partners, and better communications show leaders, in particular, are rethinking the fundamentals of security.

Security policies and safeguards currently in place: All respondents vs. leaders



Question 14: "What process information security safeguards does your organization currently have in place?" (Not all factors shown.) Question 29: "Does your organization have a senior executive (CEO, CFO, COO, etc.) who proactively communicates the importance of information security to the entire organization?"

Many organizations have invested in technology safeguards to secure their ecosystems against today's evolving threats.

Leaders are more likely to have implemented these technologies. But given today's elevated threat landscape, *all* organizations should strongly consider implementation of these safeguards.

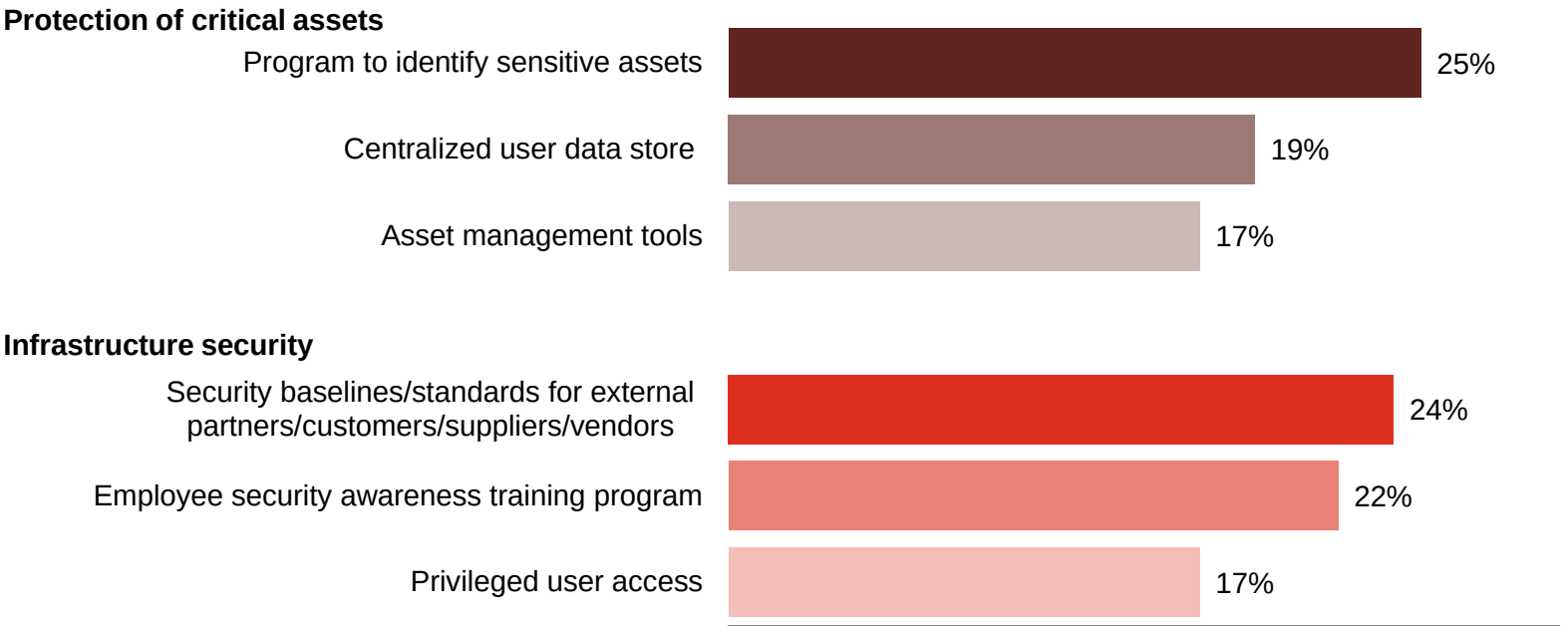
Technology safeguards currently in place	All Respondents	Leaders
Malicious code detection tools	74%	88%
Vulnerability scanning tools	62%	71%
Data loss prevention tools	58%	67%
Mobile device malware detection	57%	67%
Security event correlation tools	57%	66%
Virtualized desktop interface	55%	65%
Code analysis tools	54%	64%
Protection/detection management solution for APTs	54%	66%
Security information and event management technologies	54%	66%

Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

What business imperatives and processes will respondents invest in?

Some of the highest priorities include technologies that can help the organization protect its most valuable assets and gain strategic advantages.

Safeguards not in place but a top priority over the next 12 months

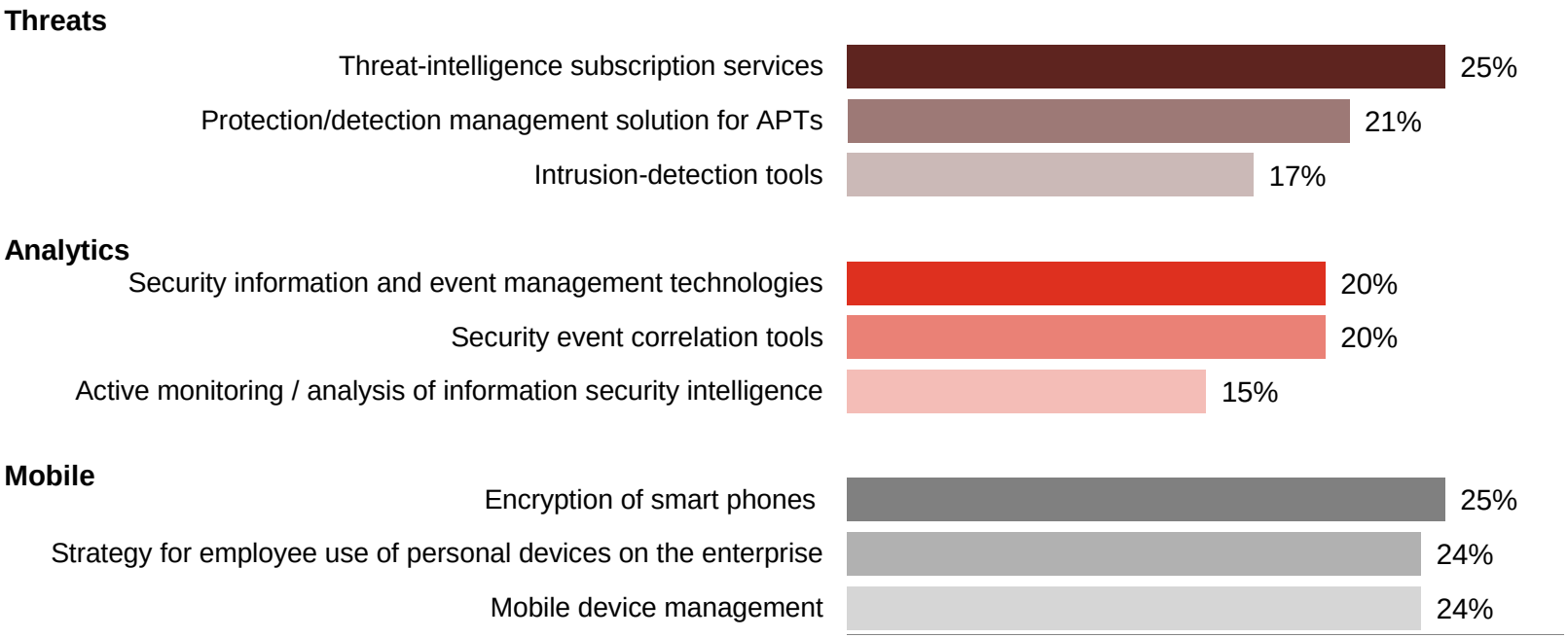


Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and organizations are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.

Safeguards not in place but a top priority over the next 12 months



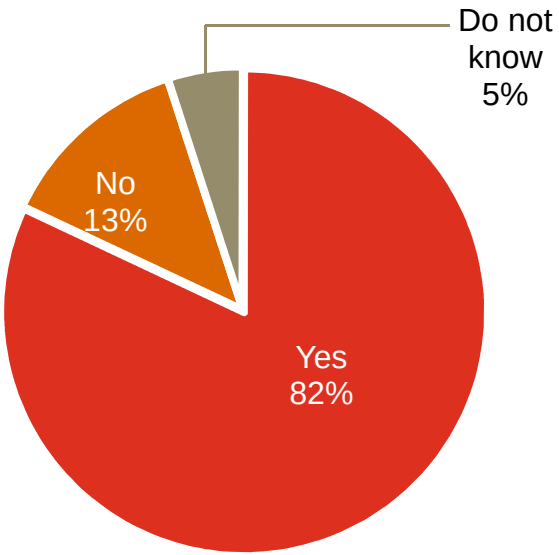
Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?”
Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Global leaders are likely to see the potential benefits of collaboration and information sharing.

Many leaders realize that public-private partnerships can be an effective way to gain intelligence about fast-changing security threats.

Formally collaborate on information security with others in the industry (leaders)

82% of **leaders** collaborate



Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?"

Effective security demands that organizations align information security with business strategy and objectives.

More respondents say security spending and policies are completely aligned with business objectives. In other words, they are starting to understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

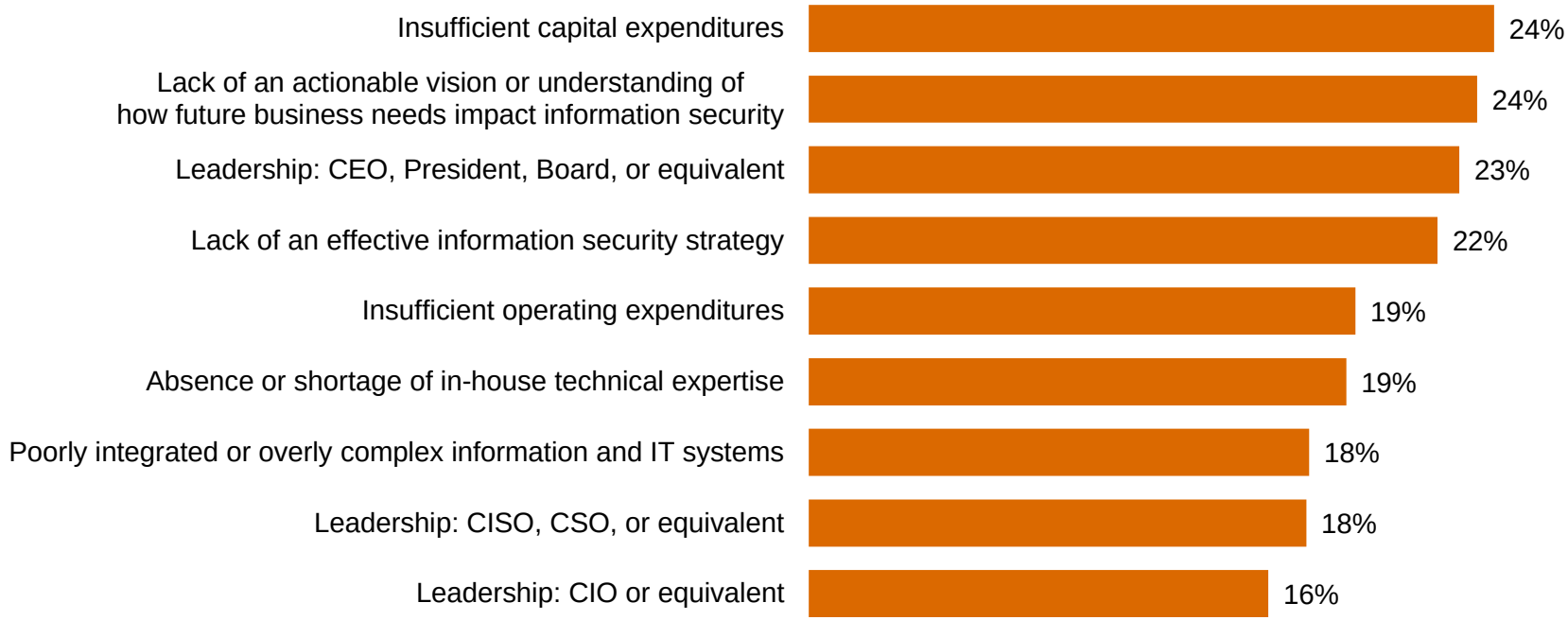
Level of alignment with organization's business objectives (somewhat or very aligned)

Question 33: "In your opinion, how well are your company's security policies aligned with your company's business objectives?" Question 34: "In your opinion, how well is your company's spending aligned with your company's business objectives?"

More money and committed leadership are needed to overcome obstacles to advancing security.

These are critical because an evolved approach to security requires the support of top executives and an adequate budget that is aligned with business needs.

Greatest obstacles to improving the strategic effectiveness of the company's IS function



Question 28: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?"

Section 6

The global cyber-defense race

South America is poised to take the lead in information security investment, safeguards, and policies.

Asia Pacific remains very strong in security spending and leading practices, while Europe and North America lag in many aspects.

	South America	Asia Pacific	Europe	North America
Security spending will increase over the next 12 months	66%	60%	46%	38%
Have an overall security strategy	75%	79%	77%	81%
Employ a Chief Information Security Officer	75%	74%	68%	65%
Have a senior executive who communicates the importance of security	68%	69%	51%	55%
Measured/reviewed effectiveness of security policies and procedures in past year	70%	69%	53%	49%
Have policy for backup and recovery/business continuity	58%	55%	45%	47%
Require third parties to comply with privacy policies	55%	58%	55%	62%
Employee security awareness training program	54%	63%	55%	64%
Have procedures dedicated to protecting intellectual property (IP)	20%	24%	17%	21%
Have intrusion-detection technologies in place	64%	67%	63%	67%
Inventory of where personal data are collected, transmitted, and stored	53%	60%	52%	64%
Collaborate with others to improve security and reduce risks	66%	59%	45%	42%

(Not all factors shown.)

China has the advantage in implementation of technology safeguards to protect against today's dynamic threats.

Russia also shows solid progress in deployment of safeguards that monitor data and assets, while the US leads Brazil—and India plays catch-up.

	China	Russia	US	Brazil	India
Centralized user data store	73%	68%	65%	64%	61%
Behavioral profiling and monitoring	60%	48%	44%	57%	48%
Encryption of smartphones	61%	51%	57%	52%	53%
Intrusion detection tools	65%	76%	67%	64%	68%
Vulnerability scanning tools	72%	60%	63%	63%	58%
Asset management tools	71%	60%	64%	59%	62%
Use of virtual desktop interface	64%	61%	56%	55%	52%
Protection/detection management solution for APTs	62%	56%	56%	54%	48%
Security information and event management (SIEM) technologies	66%	59%	57%	54%	48%

Question 15: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown.)

The fusion of cloud computing, mobility, personal devices, and social media is a unified challenge for all countries.

No country has fully addressed the potential impact of these four interconnected issues, but China and the US are setting the pace for implementation of security strategy.

	China	US	Russia	Brazil	India
Cloud security strategy	51%	52%	45%	49%	47%
Mobile device security strategy	64%	57%	51%	49%	50%
Social media security strategy	59%	58%	47%	51%	50%
Security strategy for employee use of personal devices on the enterprise	71%	64%	56%	53%	54%

Question 14: “What process information security safeguards does your organization currently have in place?” (Not all factors shown.)

Section 7

The future of security: Awareness to Action

The fundamental safeguards you'll need for an effective security program.

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

Essential safeguards for effective security	
1	A written security policy
2	Back-up and recovery/business continuity plans
3	Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
4	Strong technology safeguards for prevention, detection, and encryption
5	Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
7	Ongoing monitoring of the data-privacy program
8	Personnel background checks
9	An employee security awareness training program
10	Require employees and third parties to comply with privacy policies

Beyond the fundamentals: A new approach to security for a new world.

Traditional security safeguards will only take you so far. Today's elevated risk landscape demands a new approach to security, one that is driven by knowledge of threats, assets, and adversaries. We call this model Awareness to Action.

Security is a business imperative

- You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
- An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.

Security threats are business risks

- CEOs, board members, and business executives should understand that security risks are organizational threats.
- You should anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks.
- Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Beyond the fundamentals: A new approach to security for a new world *(cont'd).*

Protect the information that really matters

- Understand and adapt to changes in the threat environment by identifying your most valuable information.
- Know where these "crown jewels" are located and who has access to them.
- Allocate and prioritize resources to protect your valuable information.

Gain advantage from Awareness to Action

- All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring.
- Create a culture of security that starts with commitment of top executives and cascades to all employees.
- Engage in public-private collaboration with others for enhanced threat intelligence.

For more information, please contact:

Gary Loveland
Products & Services Industries
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Products & Services Industries
646.471.5731
mark.a.lobel@us.pwc.com

Joe Nocera
Financial Services Industry
312.298.2745
joseph.nocera@us.pwc.com

Peter Harries
Health Industries
213.356.6760
peter.harries@us.pwc.com

John Hunt
Public Sector
703.918.3767
john.d.hunt@us.pwc.com

Dave Burg
Forensic Services
703.918.1067
david.b.burg@us.pwc.com

Dave Roath
Risk Assurance Services
646.471.5876
david.roath@us.pwc.com

Or visit www.pwc.com/gsiss2014 to explore the data for your industry and benchmark your organization.

PwC