UBM

December 2015

2016 Cybersecurity Trend Report

INSIDE

SPONSORED BY

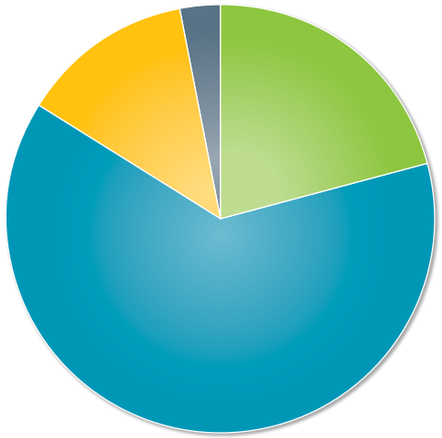
Hewlett Packard Enterprise

1512000

Introduction

Commercial and governmental organizations are under an unrelenting barrage of cyberattacks from skilled, well-organized adversaries. The loud, opportunistic attacks of the past, which were designed to steal as much data as quickly as possible with no concern the attack would be noticed, have been replaced by sophisticated attack campaigns that use stealth and persistence to harvest data, take over systems, disrupt operations, and create a vast array of mayhem.

Because of this, incident detection and response capabilities have become as important to an organization as preventing as many attacks as possible at the network edge. Businesses and governments alike can no longer rely solely on perimeter security technologies to keep them safe. Also vital for protection are application-level controls, data monitoring tools, and capabilities for correlating and analyzing security intelligence from multiple sources for the often-hidden markers of malicious activity.



- Extremely confident **21%**
- Somewhat confident **63%**
- Not very confident..... **13%**
- Almost certain to get breached **3%**

↑ Figure 1. How confident are you in your organization's ability to withstand a malicious attack over the next 12 months?

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

An October 2015 UBM Tech survey of 185 business technology professionals at medium and large companies examined how enterprises are responding to these rapidly evolving threats. We asked organizations to self-assess their readiness to combat cyberthreats and identify their biggest security concerns. We looked at how enterprises are spending IT security budgets and evaluated their attitudes toward the use of application security tools, as well as data monitoring and security information and event management controls.

The results show that many organizations are apprehensive about their ability to deal with current and emerging threats and are either planning to increase spending on nonperimeter security tools or have done so. A resounding 63% admitted to being only somewhat confident about stopping a cyberattack, while 16% confessed to being not very confident or almost certain of getting breached.

Only 21% admitted to being extremely confident of their organization's ability to withstand a malicious attack. Given the massive data breaches at organizations like Target, Anthem, and a host of other large, well-protected organizations and government entities over the last two years, even that number is surprisingly high. It suggests that some organizations have what security analysts describe as an overly optimistic view of their ability to stop threats.

In addition, consider that:

- Concerns over phishing attacks, insider abuse, and advanced persistent threats appear to be driving increased spending on application security, data security, and security information and event management.
- Despite questions about the effectiveness of perimeter security technologies, organizations are not scaling back on their use of firewalls, antivirus tools, and intrusion-detection and -prevention systems. Instead, a majority of the responds say their organizations will actually increase spending on such products in the next 12 months.
- Lack of budget and lack of management buy-in continue to be major obstacles to security spending despite the obvious concern about the growing costs and reputational impact of data breaches.

In this report, we will examine the overall security trends that are driving the need for change, as well as plans and strategies around application security, network security, and data security. ■

Security-Level Trends

An October 2015 global study of 252 companies in seven countries conducted by the Ponemon Institute[1] in conjunction with HPE Security shows that the number of cyber-attacks against organizations continues to increase in frequency and sophistication.

Organizations on average spent more per breach in 2015 than they did in 2014. The annualized cost to detect, respond to, and mitigate a breach globally was around $7.7 million—1.9% higher than in 2014. For U.S. companies, the average annualized costs were much higher, at around $15 million on an annualized basis.

The study also found that the average cost of a data breach was around $21,155 per day. So the longer an attack remained undetected, the higher the cost was to the breached organization. On average, organizations took around 46 days to resolve a cyberattack, which meant they spent around $973,000 just during the attack remediation phase.

Contrary to popular perception about external attackers causing the most damage, the costliest crimes were caused by insiders. Denial-of-service attacks and web application attacks were close behind in terms of costliest attacks.

The data revealed that unlike the mass attacks of a few years ago, a growing number of current attacks against organizations are stealthy, highly targeted, and carried out by organized cybercrime gangs.

With many advanced persistent threat (APT) campaigns, attackers have shown a tendency to use spear-phishing emails and other social engineering tricks to acquire login credentials belonging to legitimate users, which they then use to gain an initial foothold on an enterprise network.[2] Threat actors have been known to conduct extensive surveillance to gather information about victims in order to target them more effectively.

Previous APT attacks have shown that once attackers gain access to a system, they use sophisticated malware to move laterally across the network until they gain access to systems containing customer, financial, and other valuable data. Unlike the smash-and-grab raids of the past, many of the attacks have emphasized persistence and stealth during the data exfiltration stage, which can last for months.

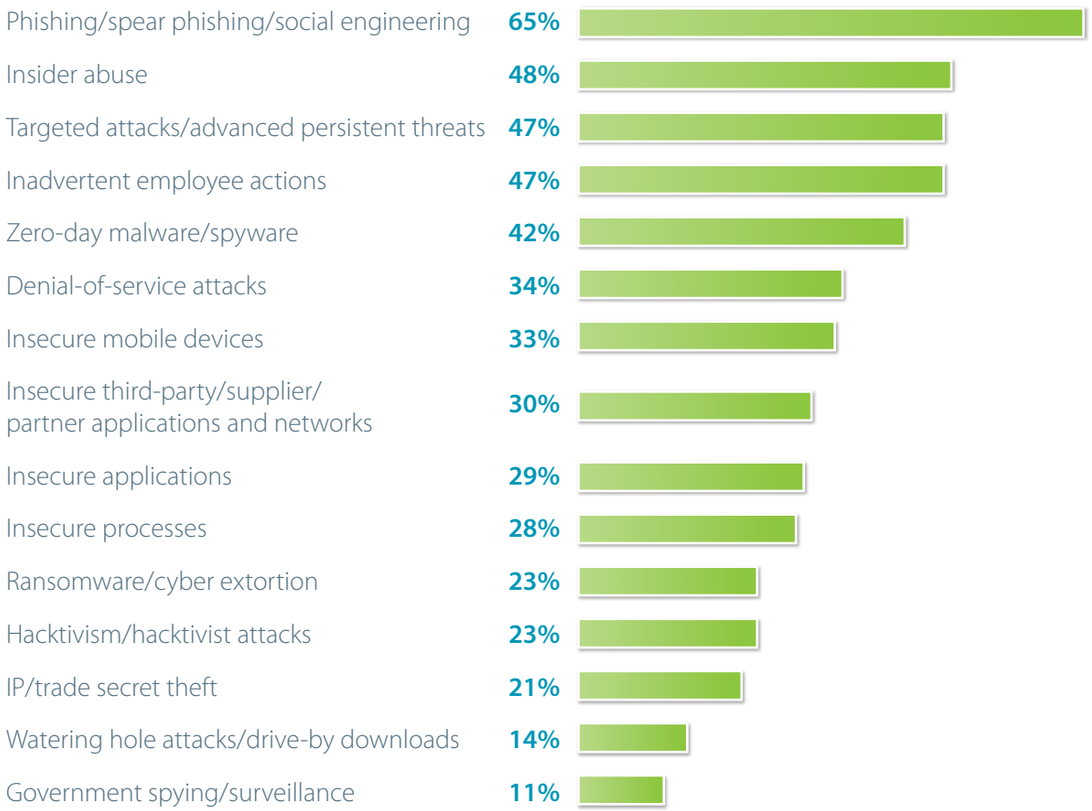


Figure 2. What do you see as the biggest security threats to your organization?

Note: Multiple responses allowed

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

The results of the UBM survey reflect a growing awareness of the problem, with 65% of respondents identifying phishing and social engineering as their biggest security concern. Nearly half (47%) identified APTs and targeted attacks as a major concern, while 42% cited zero-day threats as a problem. Other major concerns included insider abuse, inadvertent employee actions, and denial-of-service attacks.

Somewhat surprisingly, only 24% of those who responded to the UBM survey admitted their organizations have suffered a data breach in the past 12 months. Fifty-six percent said they have not experienced a data breach, while 20% said they didn't know whether they have been breached.

The relatively high proportion of respondents who said their organizations have not suffered a data breach is significant because it suggests one of two things: The organizations are either doing an exceptionally good job preventing cyberattacks, or they don't yet realize that they have been breached.

While enterprises clearly want to be able to respond as quickly as they can to a data breach, it's taking longer and longer for many to detect intrusions. For instance, it takes financial services companies up to 98

days on average to detect a breach. The dwell time—the period between intrusion and breach discovery—is even longer for retailers, at around 197 days.[3]

Results from the UBM survey reflected this trend, with 50% of the respondents saying their organizations would take several days to several weeks to detect an intrusion, 8% saying it could take months, and 4% saying they'd never know.

The numbers highlight the need for enterprises to have more robust capabilities for detecting and responding to intrusions. Most organizations see perimeter tools as being vital to their ability to defend against attacks. But there appears to be a growing trend among security administrators and managers about the need for tools that can help them mitigate the fallout of an intrusion, should one occur.

In the coming year, most organizations surveyed plan to increase spending on application security, data security, and information security. For instance, 45% of respondents said they expect to spend more on application security in the next 12 months, while another 30% expect spending to remain the same.

A similar proportion (43%) of respondents said their organizations would increase spending on data security tools for database activity monitoring, data loss prevention, encryption, and tokenization, while 33% planned to keep their spending at current levels.

The heightened awareness for incident detection and response was also reflected in the survey results pertaining to security information and event management tools. Some 42% of the organizations surveyed already use SIEM tools to correlate and analyze threat data from multiple sources, while another 14% plan to implement the capability in the next 12 months. Similarly, 45% use tools to monitor DNS and NetFlow, and 17% will do so in the coming year. ■

[1] *https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf*
[2] *http://www.infosecurity-magazine.com/news/91-of-apt-attacks-start-with-a-spear-phishing/*
[3] *http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches*

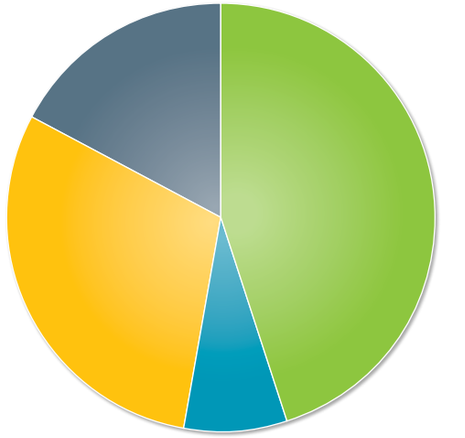


Figure 3. Over the next 12 months, do you expect your organization to spend more or less money on application security products and processes?

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

Application Security Trends

Web applications continue to provide an attractive target for malicious attackers looking for an entry point to enterprise systems and data. Well-understood vulnerabilities like SQL injection, cross-site scripting, command injection, and cryptographic errors continue to be rampant in web applications despite a heightened awareness of the threat they pose to enterprise security. Some of these issues, like SQL injection and cross-site scripting flaws, have been around almost as long as the web itself but continue to pose major problems for organizations.

A full 48% of web applications in 2014 that HPE reviewed for its Cyber Risk Report 2015[4] had cross-frame scripting vulnerabilities, 47% had a privacy violation error, while 45% were prone to cookie security issues. The HPE report also showed that 68% of all reported web application vulnerabilities resulted from inadequate input validation.

Over the years, threat actors have looked for and exploited these vulnerabilities with devastating effects. Common attacks have included those that redirect website visitors to malicious sites, escalate privileges, send malicious code and scripts, read data from databases, or modify database data.

The situation could get worse. Data gathered by Verizon for its 2015 Data Breach Investigations Report[5] showed that organized crime groups attacked web applications more frequently than any other threat actor.

Concerns over web application security have pushed organizations like the PCI Security Standards Council to require covered entities to implement specific controls for mitigating the risk posed by vulnerable applications.

PCI rules require all organizations that handle credit or debit card data to do application code reviews and, in many cases, implement a web application firewall for protecting web applications handling payment card data. The rules leave it largely up to the covered entities to decide if they want to do a manual source code review or use automated scanning tools to look for and remediate any web application vulnerabilities.

PCI rules also recommend that organizations put controls in place to detect and prevent tampering of session tokens and to automatically receive signature updates from application vendors.[6]

Multiple tools and approaches are available to enterprises to mitigate application security issues. Examples include penetration testing and dynamic scanning of production code, static vulnerability scans of code in development and testing, code reviews,

and runtime application self-protection tools.

Implementing a secure software development practice, where security is an integral part of the application development life cycle and not treated as an afterthought, can help mitigate common application security errors over the longer term.

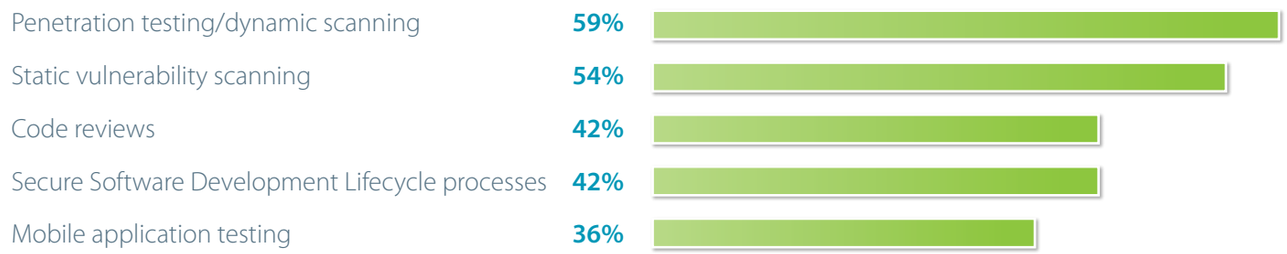
Responses to the UBM survey show that many organizations are already taking application security measures in one form or another. Only 14% of the respondents admitted to not taking any web application security precautions at all.

Dynamic scanning appears to be the most commonly used method for testing application security, with 59% of the respondents saying they have implemented the measures. Static vulnerability scanning is used by 54%, while code reviews and secure software development practices each garnered 42%.

The results of the UBM survey are somewhat similar to the results of a survey conducted by the SANS Institute on the continuous monitoring practices of enterprises.[7] That survey showed that 38% of organizations conduct web application vulnerability scans on a weekly or better basis, while 13% have implemented a continuous monitoring capability. When respondents were asked the top three categories of vulnerabilities they discovered most frequently as a result of these scans, they quite expectedly pointed to cross-site scripting, privilege escalation, and information disclosure flaws.

The numbers suggest that a fair number of organizations have implemented measures to address web application security issues. But many are lagging in their efforts. For example, if 59% in the UBM survey are doing penetration tests and dynamic scans, it calls into question why 41% of the respondents aren't taking such measures. Similarly, 58% are not doing either code reviews or secure software development. So while a majority of organizations in total are taking at least some measures to mitigate app security vulnerabilities, not many appear to have implemented multilayered protections around web apps.

Part of the problem could be budget. When



↑ Figure 4. Which of the following application-level security products and controls has your organization implemented?

Note: Multiple responses allowed

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

asked what proportion of their IT security budget is spent on application security, 37% in the UBM survey said less than 10% while 32% said the amount hovered between 10% and 20%. On the positive side, a substantial 45% said their organizations plan to spend more on application security in the next 12 months, while 30 percent expect their budgets to remain the same.

45%

The percentage of organizations that plan to spend more on application security in the next 12 months

In addition to limited budgets, a lack of management buy-in and skilled resources appear to be posing a big challenge to better web application security at many organizations. A relatively high 58% of survey respondents said their efforts to launch new application security initiatives or improve upon existing ones were being hampered by a lack of support from management. Fifty-five percent blamed the situation on a lack of skilled manpower.

It's actually somewhat surprising that this number isn't even higher. A recent Forbes study[8] on the cybersecurity industry's market size and employment statistics showed that more than 200,000 cybersecurity jobs in the US are currently unfilled because of a dearth of security skills. By 2019, the number of unfilled jobs is expected to reach a staggering 1.5 million. ■

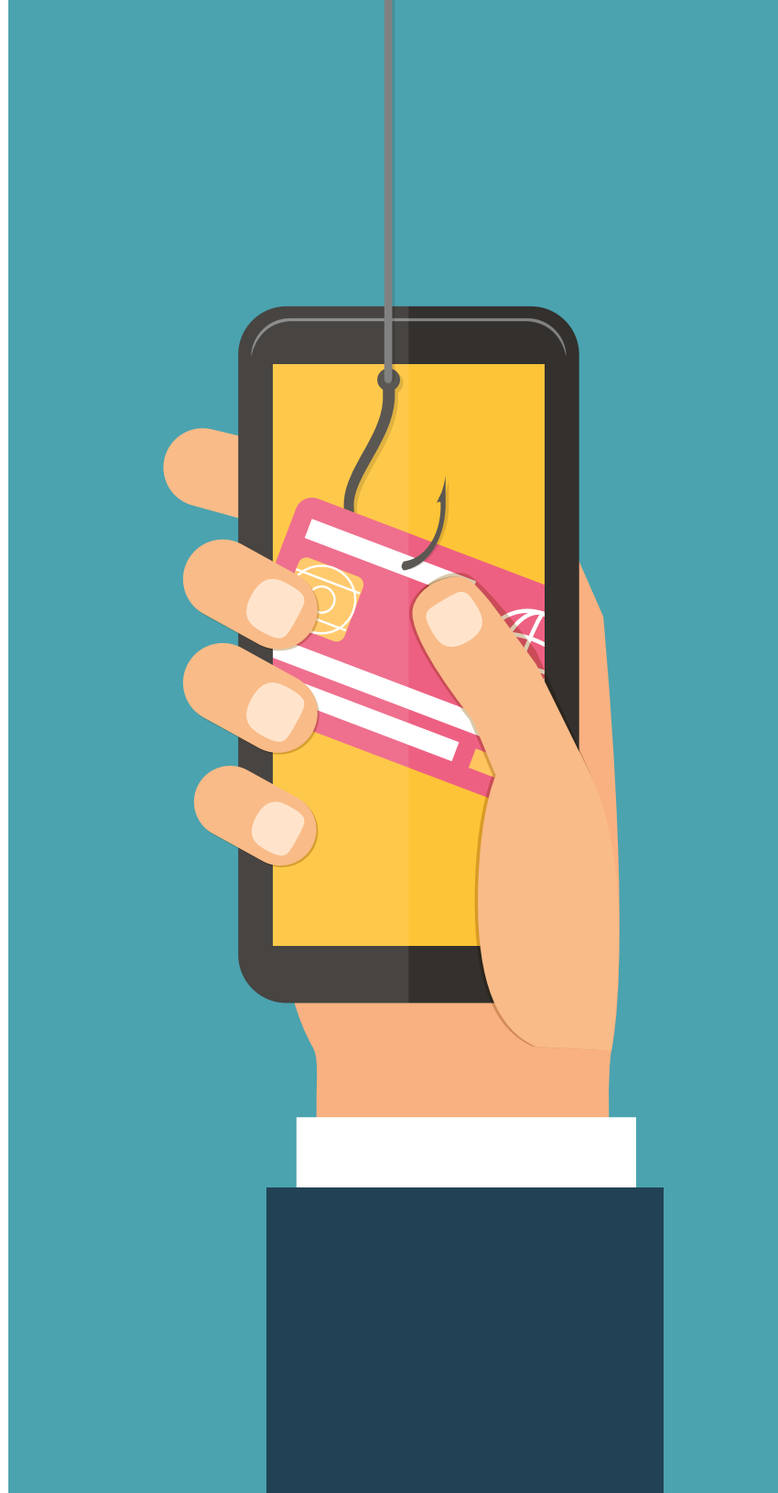
[4] *http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/*

[5] *http://www.verizonenterprise.com/DBIR/2015/*

[6] *https://www.pcisecuritystandards.org/*

[7] *http://www.sans.org/reading-room/whitepapers/analyst/vulnerabilities-survey-continuous-monitoring-36377*

[8] *http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/*



Information Security Trends

One of the biggest challenges that organizations face today is making sense of all the data generated by the myriad security systems on their networks. Antivirus tools, firewalls, intrusion-detection systems, intrusion-prevention systems, unified threat management appliances, and other technologies can be extremely noisy and flood security administrators with a mind-numbing volume of data. Add the chatter from mobile devices, virtualized systems, and cloud-connected assets, and the data can become quite overwhelming for organizations.

Consider the fact that enterprises on average receive some 17,000 malware alerts on a weekly basis, a vast majority of which turn out to be false. Chasing down such alerts costs organizations an average of $1.27 million in wasted effort.[9] In fact, just 19% percent of the alerts generated by security systems are usually reliable. Because of the sheer volume of data, administrators end up looking at just 4 percent of the alerts they receive, creating an enormous exposure for organizations.

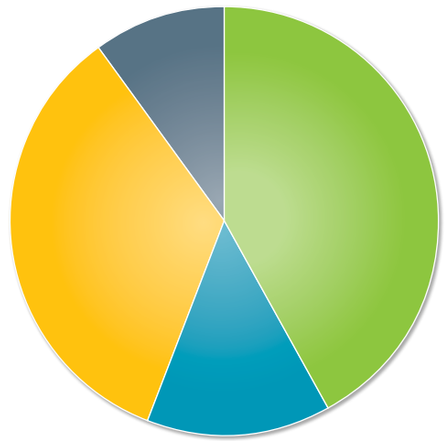
A case in point is Target's massive data breach of 2013. One of the problems Target faced was its inability to separate the wheat from the chaff in its security alerts. After the breach, executives admitted that they might have been able to reduce the impact of the intrusion had they paid closer attention to alerts generated by security monitoring tools.[10]

As a security administrator or a business owner, you need to get a handle on the data to get the visibility needed to ensure real security. Information is at the center of the intelligence-driven security model, and it is only by collecting, aggregating, and analyzing data from all the sources you have on your network that it becomes possible to enable a true situational awareness capability. The goal in using information in this manner is not just to deflect attacks at the network perimeter, but to quickly detect and mitigate the ones that do manage to break through.

Implementing such a capability requires organizations to be able to tap into, collect, correlate, and contextualize data from multiple internal and external sources using SIEM tools.

Forty-two percent of the respondents in the UBM survey have implemented SIEM and 14% plan to do so in the next 12 months. Another 34% expressed interest in implementing the technology but have no immediate plans for doing so. A mere 10% said their organizations are not interested in information and event management tools.

The numbers suggest that SIEM is a top-of-mind issue for many enterprise organizations. The mind-numbing frequency with which businesses are getting breached these days



- Yes, we currently use SIEM tools to correlate and analyze security data ... **42%**
- No, but we plan to implement SIEM in the next 12 months **14%**
- We are interested, but have no current plans **34%**
- No, and we are not interested **10%**

↑ Figure 5. Has your organization implemented, or does it plan to implement Security Information and Event Management (SIEM) tools to correlate and analyze data from multiple security products?

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

appears to have heightened awareness of the need to enable greater situational awareness to security information and events.

Among those using SIEM tools, 45% believe the technology has helped them detect malicious activity they might have missed otherwise. A recent Ponemon Institute study found that businesses using SIEM tools were generally better at detecting and containing intrusions and spent about $1.9 million less on data breach-related costs compared with companies that had no SIEM tools. Those numbers are consistent with the findings of HPE's State of Security Operations report on the capabilities and maturity levels of cybersecurity organizations in 2015.[11] None of the companies surveyed said they were achieving a minimum security monitoring capability without a SIEM.

Perhaps as a result of such tools, 38% of the UBM survey respondents said they were able to detect an intrusion as soon as it happens, while 40% said they would be able to catch it in a few days. Average dwell times for intrusions ranged from a few weeks to a few months for 18% of the respondents.

A vast majority of the respondents in the UBM survey appear to have a generally favorable view of SIEM tools. In fact, only 4% of those surveyed said SIEM products did not meet their requirements. Many feel SIEM is useful, but also pointed to specific reasons for not having implemented the capability yet.

45%

believe SIEM tools have helped them detect malicious activity they might have missed otherwise.

For instance, 30% said that SIEM tools are useful but too costly, while another 21% said SIEM is useful but complex to implement.

Despite such concerns, many enterprises appear to be moving ahead with plans to bolster their SIEM capabilities with behavioral analysis and continuous monitoring tools. In the survey, 45% said they already use tools to monitor DNS and NetFlow, while 17% plan to do so in the next 12 months. Another 26% expressed interest in using such tools but said they don't have the budget to invest in them immediately.

Such tools help companies monitor network traffic on a continuous basis and detect departures from normal behavior that are often the indicators of a compromise. When used in conjunction with SIEM tools, behavioral analytics and continuous monitoring products can go a long way toward enabling a real-time situational awareness capability across the enterprise. ■

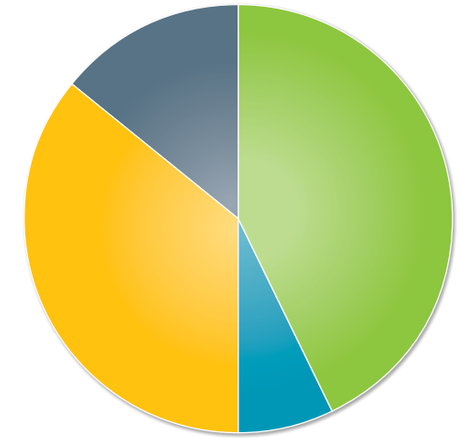
[9] *http://www.ponemon.org/*

[10] *http://www.reuters.com/article/2014/03/13/us-target-breach-idUSBREA2C14F20140313#ytMAvA2F1ErPqvyG.97*

[11] *ftp://ftp.hp.com/pub/msc/7D1B944C-F0CF-4C94-A9AD-614E8156C7F6.pdf*

Network Security Trends

Perimeter technologies like antivirus software, network firewalls, intrusion-detection systems, and intrusion-prevention products have long been the linchpin of enterprise security strategies. Organizations have firmly believed that the best strategy for preventing data breaches is to stop the attackers at the entrance to the castle. Consequently, they have spent the bulk of their security dollars on perimeter technologies.



More..... 43%
Less..... 7%
About the same..... 36%
Don't know..... 14%

Figure 6. Over the next 12 months, do you expect your organization to spend more or less money on perimeter security products and services?

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

Despite growing questions about the effectiveness of a perimeter-centric security strategy, enterprises are still heavily reliant on such tools. In fact, an overwhelming 79% of the UBM survey respondents said they would either increase perimeter security spending or maintain their current level of spending on the tools. Just 7% said they would reduce spend on these products, while another 14% said they did not know what their organizations would do.

The responses highlight a continuing dissonance between what organizations are doing and what many security experts believe they should be doing in regard to network security. Other surveys have shown the same gap.

An InformationWeek/Dark Reading survey-based report released in August 2015 had 60% of the respondents saying they considered firewalls as their most important defense. Other security products like those for web application protection and data leak protection and vulnerability assessment ranked much lower, even though security analysts have been stressing the importance of such tools to overall enterprise security for quite some time.[12]

Nevertheless, a majority of the respondents in the UBM survey said they are spending between 20% and 30% of their overall IT security budgets on perimeter security tools. About 14% are spending between 30% and 50% of their security dollars on perimeter defenses.

A startling 49% of the survey respondents said they are spending more on perimeter security than they were three years ago, and 43% say they will increase spending on this category even more over the next 12 months.

On a related—and pertinent—note, a full 33% of respondents said they didn't know how much their organizations are spending on perimeter tools, pointing to a distressing lack of awareness on a critical topic.

Clearly, the concerns expressed by some security analysts about the ineffectiveness of perimeter tools are not shared by a majority of survey respondents. However, many appear reconciled to the fact that perimeter tools alone are no longer enough to mitigate security threats.

When asked to assess the effectiveness of their perimeter security products, a substantial 35% of

the UBM survey respondents described the tools as being very effective in stopping a majority of attacks. However, 61% said such tools were not enough on their own to mitigate all threats, while 3% said the products allowed more attacks to pass through the perimeter than they blocked.

Firewalls and antivirus tools continue to be the mainstays of enterprise perimeter security strategies. An overwhelming 89% of organizations surveyed said they have implemented either a firewall or next-generation firewall technology, while 84% said the same of antivirus/anti-malware and anti-spyware products.

The portion of respondents adopting intrusion-detection and -prevention tools appears to be somewhat lower in comparison, with 57% saying they have deployed an IDS capability and 51% saying they have implemented IPS.

At least some of the continued spending on perimeter tools appears driven by the emergence of relatively new tools and techniques for blocking network threats. One example is application sandboxing.

Sandboxing is a technique that is used to isolate applications from untested or unverifiable code. Sandboxes provide a safe environment for executing untrusted code and programs from nonvetted third parties. The idea is that if the code is malicious, it will execute only within the confines of the secure sandbox and not within the application environment.

The concept of application sandboxing itself is not entirely new, but it is only relatively recently that organizations have begun implementing the capability as part of a multilayered perimeter defense strategy.

The results of our survey reflect what appears to be some nascent interest in the technology, with 29% saying they have implemented a sandboxing capability as part of their perimeter defense. ■

[12] *http://reports.informationweek.com/abstract/21/12550/Security/How-Enterprises-Are-Attacking-the-IT-Security-Challenge.html?cid=smartbox_techweb_analytics_7.300005674*

Data Security Trends

There's growing acknowledgment among security researchers and practitioners that it is next to impossible for enterprises to block all attacks that are directed at them. Given the highly persistent and targeted nature of most modern cyberattacks, many believe a data breach is almost inevitable for most organizations. The reasoning goes that no matter how well protected you are, a determined enemy will always find a way to slip past your perimeter simply because modern networks are so large, complex, and interconnected that

it's almost impossible to consistently keep every single entry point secure all the time.

Consequently, there's a greater focus on technologies like encryption, database monitoring, and data leak prevention systems for protecting sensitive data. Rather than relying solely on tools for preventing access to sensitive data, the effort is to mitigate damage if attackers do manage to find a way to access the data.

In many cases, data protection efforts are being driven by regulatory requirements. For instance, 129 respondents in the UBM survey pointed to regulatory compliance as the primary driver of their data protection efforts. But that's not the only reason.

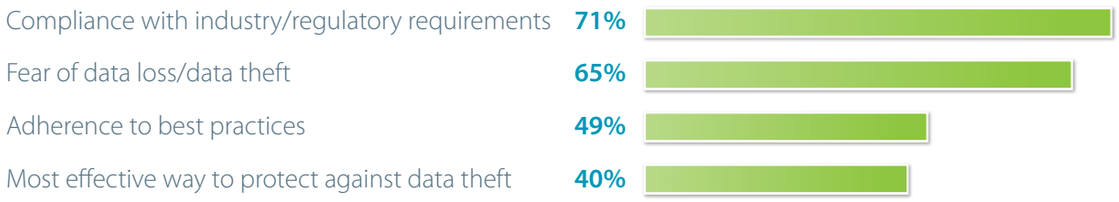


Figure 7. What has been the biggest driver(s) of data-level security efforts at your organization?

Note: Multiple responses allowed

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

For 65% of the respondents, it was fear of data theft and data loss. Another 49% said their data control efforts were spurred by a desire to adhere to best practices, while 40% said it was the most effective way to protect against data theft.

Data protection tools come in various forms and capabilities. Encryption continues to be the most common and widely recommended approach for protecting data. Numerous data protection regulations and industry standards like PCI DSS even require organizations to encrypt data while both at rest and in motion. The rules typically provide a safe harbor for organizations that implement data encryption.

Despite this, many organizations continue to drag their feet on encryption, often with disastrous consequences. For instance, over 80 million Social Security numbers were exposed when attackers managed to gain access to a database belonging to health insurer Anthem Inc. that stored the data in unencrypted form[13]. The company is not the only one guilty of such an omission.

Not very surprisingly, encryption was the most favored data protection control employed by respondents in the UBM survey. A total of 60% of the organizations represented use encryption to protect data in transit from point to point, while 54% said they use encryption to protect data at rest. Both numbers are somewhat higher than expected given the number of recent data breach incidents that have involved unencrypted data.

Even so, it means more than four in 10 organizations have sensitive data stored in an unprotected manner in their databases and are transmitting the data in an unprotected fashion. The exposure that organizations face from this continued failure to encrypt data cannot be overstated. Many consumer class-action lawsuits filed against organizations that have suffered data breaches have invoked a lack of encryption as a sign that the organization had not adhered to recommended security best practices.

Encryption is just one of the options available for protecting data. Other approaches include database activity monitoring tools, data leak/loss prevention systems, and tokenization. Each of these technologies works in different ways to protect data from inadvertent or malicious exposure.

60%

of the organizations surveyed use encryption to protect data in transit.

For example, database monitoring tools keep an eye on all activity at the database level and issue alerts on unexpected changes, additions, deletions, or access. The tools have been around for well over a decade and are often considered a critical component of a company's compliance profile.

Data loss prevention products work by monitoring network traffic for data elements, like Social Security and credit card numbers, and alerting administrators when prohibited data attempts to egress a network. DLP tools are often used to monitor for insider abuse but can play a vital role in monitoring for data exfiltration by cyberattackers.

Tokenization is an approach in which a credit card number, SSN, or any important bit of data is replaced with a token comprising a randomly generated number or alphanumeric characters. The token acts as a surrogate for the actual number during all transactions, thereby protecting the number or data element from risk.

Our survey showed organizations using all of these technologies to varying degrees. For

instance, 49% of the organizations surveyed use database monitoring tools to protect data, making it the second most widely used product in this category after encryption. Slightly less than half (46%) of the respondents are using DLP products to protect against malicious and inadvertent data leaks, while 31% said they use tokenization.

With enterprises increasingly using cloud services to host their applications and data, cloud encryption gateways have emerged as another key component in enterprise data protection strategies. About 29% in the UBM survey said they rely on cloud encryption gateways to protect their data in the cloud.

43%

Respondents who plan to increase spending on data protection tools

The numbers present a somewhat mixed picture on enterprise adoption of data protection technologies. On one hand, companies appear to be using a fairly wide spectrum of products to protect sensitive data from compromise. On the other hand, only a relatively small proportion are making the effort to do so.

One glimmer of hope comes from the spending plans that companies have for data protection tools. The proportion of respondents who plan to increase spending on data protection tools (43%) is greater than those who said spending will remain the same over the next 12 months (33%). Only 6% expect spending for the category to fall in the next year. ■

[13] *http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560*