CFO

UnitedLex

Changing the CFO Mindset on Cybersecurity

What CFOs don't know can hurt their bottom line

Despite increasing cybersecurity involvement, too many CFOs still lack the cyber-savvy necessary to get ahead of threats. Here's why.

Cybersecurity, poorly managed, is a material financial risk, affecting a company's ability to succeed or survive. A data breach can negatively impact corporate results, corporate reputation, customer relationships, and the growth trajectory of even the most successful company.

The cyber-risk landscape is ever expanding, with a growing volume and variety of attacks coming from outside the enterprise, as well as increasing sophistication of malicious employees on the inside. Unfortunately, all businesses connected to the digital world are under threat, whether they have discovered it or not.

The CFO's Role

To gain a much deeper understanding of CFOs' thinking about cybersecurity, and the roles they play in managing it, CFO Research recently surveyed 128 senior finance executives. The survey findings show that most CFOs understand that they need to play an active role in cybersecurity management, but many lack a complete understanding of the threats they face and the tools they might use to manage those threats.

The CFO's role is to protect the bottom line and ensure the viability of the enterprise. The survey found that, because of the risk to corporate performance that data breaches represent, CFOs and senior finance executives are taking an increasingly active role in managing cybersecurity. Four in ten (42%) finance chiefs surveyed say they are the owner or a co-owner of cybersecurity at their companies. A recent Grant Thornton study echoes this data point, finding that 38% of CFOs are responsible for their firms' cybersecurity.

And two-thirds (66%) of our survey respondents say they are comfortable understanding/discussing information security (e.g., risks, technology) and translating this information for their Board.

This level of CFO involvement in cybersecurity management validates a recent survey by the Ponemon Institute, which found that 79% of C-level U.S. and U.K. executives say executive-level involvement is necessary to achieve effective incident response in the event of a data breach.

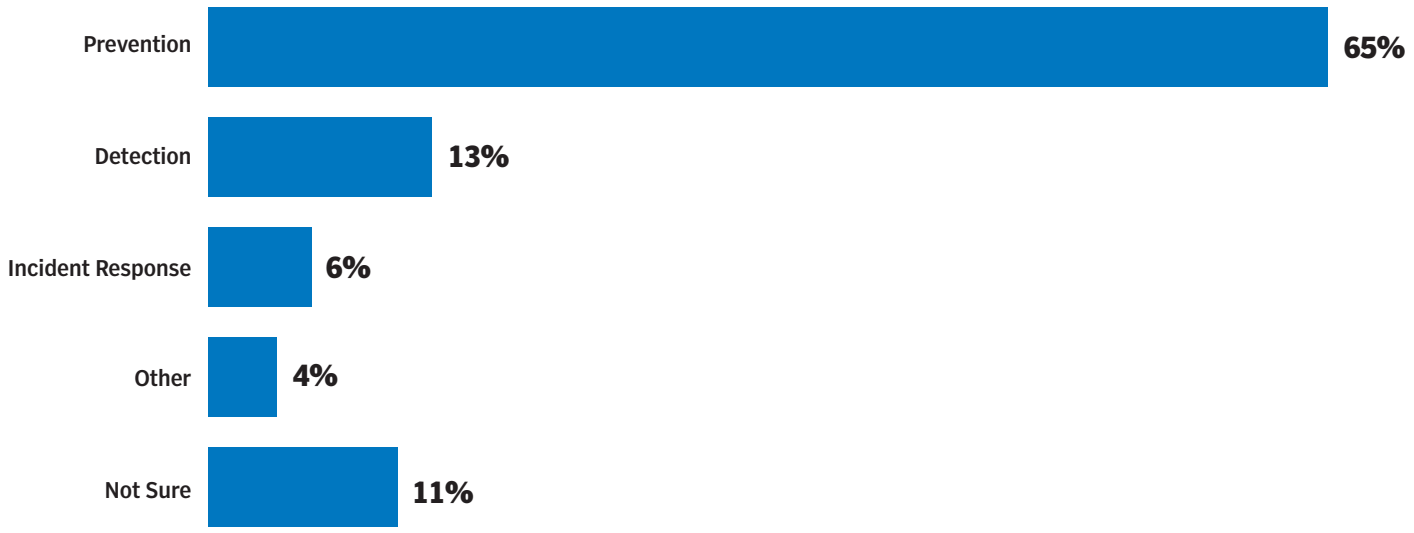
The CFO has a seat at the cybersecurity table, but do these cyber-savvy finance stakeholders have the insight needed to significantly and positively impact their organization's cyber-risk program?

Disconnect: Awareness

More than one-third (37%) of the senior finance executives surveyed say they have not had a data breach in the last 12 months. A 2014 Grant Thornton survey of finance executives found that an amazing 74% of respondents said their company has not experienced a data breach.

These data points appear to represent an overly optimistic sense of security among both surveys' respondents. The 2013 Data Breach Investigations Report (DBIR) noted that more than six in ten (62%) security incidents took "months" to discover, and 4% of security incidents took a year or more to discover. The fact that the CFO is not aware of a data breach does not mean it hasn't happened. In fact, CFOs might consider the very real possibility that ALL companies have suffered a data breach in the last 12 months—i.e, at the very least a network intrusion. In many cases, networks are compromised and the attackers simply lay in wait for years.

FIGURE 1 Where is most of your cybersecurity budget spent?



(Percentage of respondents)

Disconnect: Focus

Most survey respondents are comfortable with their organization's cybersecurity posture, with two-thirds (67%) reporting that they are comfortable that their organization's cybersecurity budget is being spent effectively. But there's a problem.

While 65% of respondents say that their cybersecurity budget is spent on prevention (see Figure 1), a full 61% say unknown threats are their greatest concern. These two data points reflect a clear disconnect. That's because unknown threats are not addressed by traditional prevention tools.

In general, preventative technologies rely on signature-based detection, leveraging the fact that the attack methods and malware have been used before and have been identified by the cybersecurity community. Unfortunately, attackers monitor this information as well, so once their code and methodology has been discovered, it is altered.

Enterprises that focus primarily on prevention (rather than detection or response) increase the risk of missing unknown threats, such as attacks using weak or stolen login credentials and advanced attacks that do not involve malware. To illustrate how common those "hard-to-see" threats are, almost 80% of network intrusions involve weak or stolen login credentials. For these reasons, focusing on prevention is not the most effective way to spend your time or money.

Disconnect: Response Planning

Experts also cite the critical importance of having an incident response plan with clearly defined roles and processes. Such a plan should involve more than just the basics of detection, containment, investigation, remediation and recovery. It should also include steps aimed at minimizing legal liability, reputational impact, and employee morale.

Unfortunately, the Grant Thornton study showed that a small percentage are focused on incident readiness, with only 4% reporting that they have created an incident response plan.

Despite the lack of uptake, a defensible and well-defined incident response process is the single most important component of an information security program. As we noted at the beginning, no matter how good your preventative technologies are, a sophisticated (or lucky) attacker is going to get in sooner or later.

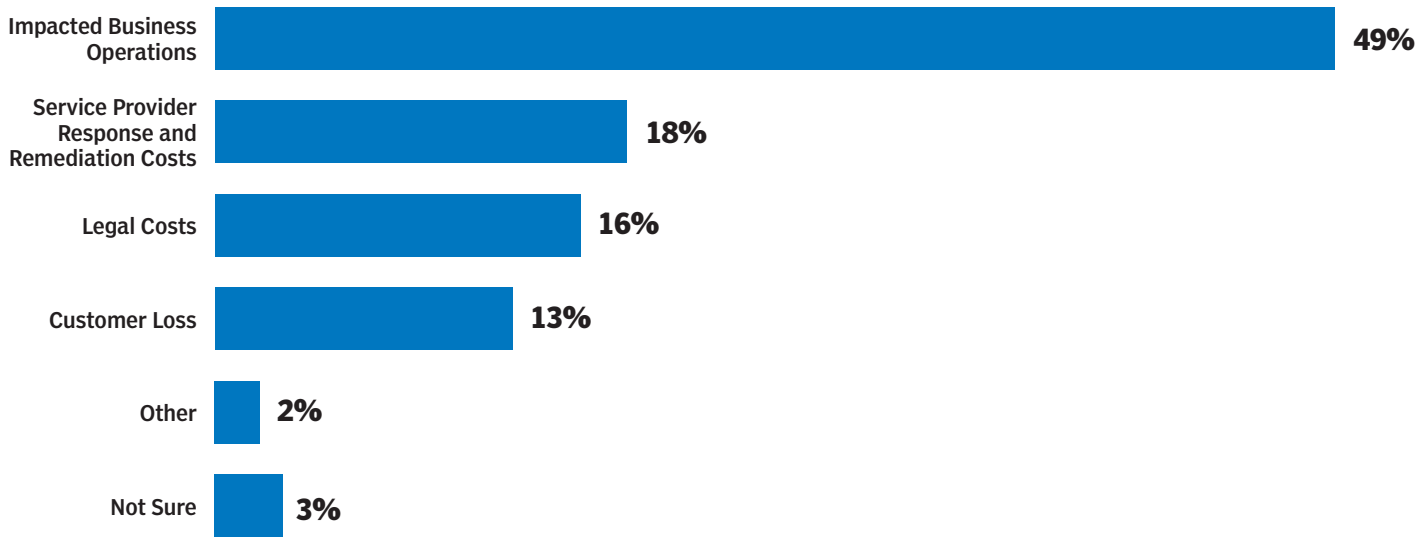
Still, only 53% of senior finance executives we surveyed say their company has a formal incident response process. And only 23% of finance chiefs have a formal role in incident response. With so much at stake, the CFO should play a formal role in the process.

Disconnect: Damage Assessment

Figure 2 shows where finance executives expect the largest financial impact to come from in the event of a data breach. Nearly half (49%) of respondents say the largest financial loss would be from impacted business operations. This includes the downtime of critical systems and other operational interruptions resulting from breach investigation and remediation processes.

Survey respondents seemed to downplay the financial impact of customer loss (13%), but again these executives seem to be underrepresenting a significant risk. Consumers' concerns about the security of their personal data following a breach have severely and lastingly damaged many businesses. While impact from disrupted business operations are easier to quantify in the short term, the "long tail" of disrupted customer relationships can last far into the future. In the Ponemon 2015 Cost of Data Breach Study, "lost business" defined as abnormal turnover of customers, increased customer acquisition activities, reputation losses, and diminished goodwill, represents the greatest financial impact. Furthermore that cost is increasing year over year.

FIGURE 2 Where would you expect the largest financial impact to come from in the event of a cybersecurity breach of your organization?



(Percentage of respondents)

With all the determined efforts that companies make to acquire and retain customers, it makes sense for the CFO to ensure that the company has a holistic response plan that extends beyond information security activities to mitigate the risk of lost business in the event of a data breach.

Making the Connection

There is no silver bullet to prevent a cyber attack. The most your firm can do is be a fast-moving target that stands ready to respond.

As a CFO, what you can do is understand the stakes of this conflict, take an active role in its management, and if needed seek counsel to augment your advanced threat detection and security analytics tools with equally advanced human analysis and judgment.

More and more companies, particularly midsize firms with high threat profiles, are turning to specialized Managed Security Services Providers (MSSPs) that employ a more holistic, context-driven methodology to deliver security monitoring. The best of these providers layer human intelligence and human analysis on top of their monitoring in a practical and scalable way. They are able to bring all your executive stakeholders to the table to design and implement a forward-leaning incident response plan and security awareness program.

It's the best a CFO can do. Good luck.