


CYBER SECURITY

A CFO's Guide to Cyber Security in the Coming Year

LEVERAGE TECHNOLOGY AND
YOUR FINANCIAL INSTITUTION
TO BUILD BETTER DEFENSES

A CFO's Guide to Cyber Security in the Coming Year

This publication has been prepared for informational purposes only, and is not intended to provide, and should not be relied on for, general, tax, legal or accounting advice. Please consult with your own tax, legal and accounting advisors before engaging in any transaction. Huntington makes no representation or warranty, express or implied, with respect to the content, and accepts no liability arising from any use or reliance on this publication.

Member FDIC.  and Huntington® are federally registered service marks of Huntington Bancshares Incorporated. Huntington. Welcome.™ is a service mark of Huntington Bancshares Incorporated. © 2017 Huntington Bancshares Incorporated.

INTRODUCTION

A CFO's Guide to Cyber Security in the Coming Year

Mobile and cloud-based technologies are making it easier for finance teams

and other corporate users to perform everyday tasks such as checking on transactions and logging into financial systems from wherever they may be.

As risk management leaders, CFOs need to ensure that valuable corporate data and systems are protected, while striking the right balance between risk and resilience.

Managing risk and bolstering security have become more complicated as cyber attacks continue to grow in sophistication and frequency. Securing IT systems is more important than ever, as all business functions — including the human resources, supply chain, and research functions that are vital to many operations — are exposed to cyber attacks.

According to the *2016 RIMS Cyber Survey*, companies responded to cyber threats using not just technology, but also education, preparation, and risk transfer. Indeed, the top priorities cited by respondents were active monitoring and analysis of information security (75 percent), followed by scanning tools

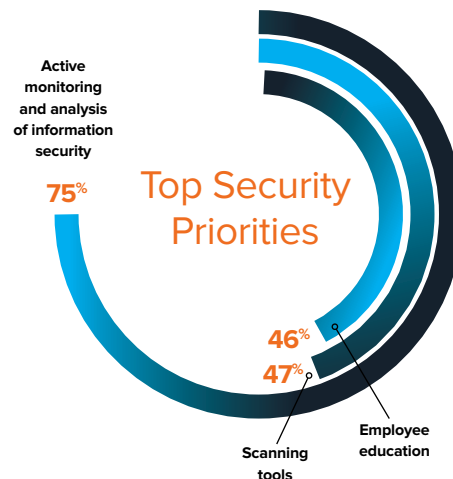


(47 percent) and employee education (46 percent).

This eBook explores some of the ways that financial and other data can be compromised and how CFOs can mitigate those risks.

Topics include:

- ▶ **An overview of some of the major trends in cyber security,** including sophisticated schemes such as “CEO email” scams.
- ▶ **Assessing cyber security risks in your organization, including** internal security practices as well as data shared with external sources such as banks, vendors, and administrators of retirement and health care plans.
- ▶ **Developing a plan to recognize fraud, particularly banking** transactions, and working with your banking partner to ensure secure electronic payments.
- ▶ **A look to future tools and techniques for combatting cyber fraud.**



Source: 2016 RIMS Cyber Survey



Be Aware of Major Cyber Security Threats

According to IBM's *2016 Cyber Security Intelligence Index*, unauthorized access was the most frequently occurring cyber security incident, with 45 percent of respondents experiencing this type of attack in 2015.

Malicious code was the second most common cyber attack, with 29 percent of respondents reporting this type of breach. This type of intrusion includes phishing campaigns in which an outsider mimics a company e-mail address or uses social engineering

to assume the identity of the CEO, a company attorney, or trusted vendor.

According to Wombat Security's *2016 State of the Phish* report, 85 percent of all organizations reported being the victim of a phishing attack in 2015. The level of sophistication is also on the rise. Two-thirds of the organizations surveyed experienced attacks that were targeted and personalized, up from 22 percent the previous year.

A related cyber threat is business e-mail compromise, a sophisticated scam targeting businesses that regularly perform wire transfer payments with

According to IBM's *2016 Cyber Security Intelligence Index*, unauthorized access was the most frequent cyber security breach, followed by malicious code.



foreign suppliers and/or businesses. The perpetrators initiate fraudulent emails that appear to be from executives and employees in which they request wire transfers.

How Secure Are Your Systems?

As cyber attacks become more sophisticated, it is imperative for CFOs to take the reins of managing the company's cyber defense. While finance chiefs must work with IT and business unit leaders to plan for the inevitable cyber attacks, they are increasingly the ones taking the heat for data breaches and other cracks in cyber security. Finance chiefs are being questioned not only at the board level but also by the Securities and Exchange Commission and other government entities on how they are managing their cyber security risk.

While many organizations have dedicated professionals that are focused on preventing an attack from the outside, internal weaknesses are also a threat to data security. The Association of Corporate Counsel's recent *The State of Cybersecurity Report* cited survey findings that 24 percent of in-house lawyers blamed employee error for a breach at their company. Employee mistakes rank higher than phishing attacks (12 percent), third-party access (12 percent), and lost devices (9 percent).



“It is not just a strong perimeter defense that matters,” said Dan Bissmeyer, Chief Security Officer at Huntington National Bank. “You can’t have a hard shell and a soft interior.” He cited the need for physical security, properly vetting of employees and contractors, and carefully managed access to the information specific to roles in the organization.

Your Financial Institution Can Help You Mitigate Risk

One of the most effective ways a CFO can minimize a data breach is to have a strong relationship with their financial services provider. Steps such as requiring dual approval on

certain monetary transactions and administrative changes can go a long way to protecting the interests of the company and the bank.

“Your bank should be as interested in helping your company make money and protecting that money as anyone else in your organization,” said Charles Peirano, SVP and Enterprise Fraud Program Director at Huntington National Bank. “Together you and your financial services provider can discuss options to help you meet these goals.”

C-level executives should be having regular conversations with their financial institution about how to avoid all types of risk that can



interrupt business, said Don Boian, Chief Information Security Officer at Huntington National Bank.

“Cybersecurity should be viewed in conjunction with an overall business continuity strategy, and your financial institution should be helping your business operate and be successful,” Boian said.

CFOs should also review the processes for accepting bitcoin and other blockchain-based digital currencies with their financial institutions. “While digital currencies offer the promise of greater security and efficiencies, they are outside of the traditional banking arrangements,” said Carol Fox, VP, Strategic Initiatives for RIMS, a risk management trade organization.

Testing, Testing, Testing

While it is imperative to put a plan in place to prevent data breaches, it is no longer sufficient just to communicate that plan to internal staff and trusted vendors, experts noted. Companies also need test their cyber defenses regularly. “There has to be periodic testing and ongoing education of employees and outside vendors with access,” Peirano said. “Data security — like all security — is only as good as the weakest link.”

It is also important to hold insurance providers, payroll processors, and

benefits administrators and others to the same standards as internal users. “Third-party providers who have access to any sensitive data regarding customers and/or employees should go through the same rigorous vetting process that is used to ensure internal data,” Bissmeyer noted. “They should be held to the same auditing processes.”

Bissmeyer also encouraged CFOs to pay close attention to restricting access, both internally and externally, to the data that is necessary to perform the task. “For example, if there is no need



for someone in a certain position to have access to social security numbers to perform their job, then no one in that role should have access.”

Peirano said it is important to create a culture where employees feel free to challenge the need for information. “No one wants to question the CEO if they get an email that appears to be from the CEO that says funds need to be moved immediately, but everyone has to have a critical eye these days and should feel free to take that extra step to verify.”

Staying Alert to New Threats

There is a daily and constant barrage of new threats to data security, which is why it is critical to continue to educate everyone in the organization about best practices.

Endpoint protection — guarding PCs and laptops against malware — continues to be a challenge as new threats are continuously emerging. An overwhelming majority (86 percent) of respondents to a survey by Cyberedge Group (published in the

“No one wants to question the CEO but everyone has to have a critical eye these days and should feel free to take the extra step to verify.”

— CHARLES PEIRANO,
HUNTINGTON
NATIONAL BANK



2016 Cyber Defense Report) said their organizations are not satisfied with their current endpoint protection software. That number is up significantly from the previous year's survey, when 67 percent reported dissatisfaction with their endpoint protection. Social media accounts, smartphones, and tablets were also areas that respondents noted were emerging concerns for the coming year.

Attending hacker conventions is another way to keep abreast of the latest cyber security threats. "It is beneficial to have someone in the organization who is keeping current with all of the ways that bad actors can potentially compromise your systems and testing your defenses against the latest methods of attack," Cox said.

While it is important to stay informed of the latest malware and other phishing schemes that attempt to penetrate systems from the outside, many future threats will be carried out by insiders. "The use of insiders to penetrate an organization's valuable data is becoming increasingly common," Bissmeyer said, emphasizing the need for proper vetting and monitoring of employees and vendors as well as tight access control.

In addition, as companies mount strong cyber defenses, experts noted that there is an uptick in non-cyber crimes. "With ACH systems becoming more secure, more criminals are resorting to

the old-fashioned route, such as check fraud, to gain access to a company's account," Peirano said.



CONCLUSION

Finance Must Lead Cyber Security Efforts

Every person in the organization has a role to play in mitigating the risk of a cyber attack. CFOs are tasked with securing highly sensitive financial, employee, and customer data. Cyber security is a big responsibility that is always evolving as new threats are launched on a daily basis.

While acting as data defenders, finance chiefs also have to be concerned with providing access and visibility to the data and analytics that have become so vital to the success of any business. Information has to remain accessible without becoming vulnerable to internal or external misuse.

What can CFOs do to protect their company's valuable data without risking a cyber attack? Some key takeaways from this eBook include:

- ▶ **Be aware of the many ways that your company's systems and data** can be compromised and be prepared to defend against the continuously evolving methods of attack.
- ▶ **Establish a security plan, communicate the strategy to employees** and vendors, and test your cyber defenses periodically to mitigate risk.
- ▶ **Work with your financial institution to help safeguard your** company's financial and other data. This can help to thwart fraud attempts such as CEO phishing scams.
- ▶ **Foster an environment where everyone takes responsibility for** cyber security and feels at ease questioning the need to access data or the veracity of an email.

The need for strong cyber security initiatives will only grow in the future. According to the *2016 Cyberthreat Defense Report*, 62 percent of respondents expect to fall victim to an attack, and 85 percent will spend 5 percent or more of their IT budget on cyber security. The job of the CFO is to invest wisely to minimize the impact of a data breach.



SPONSOR'S PERSPECTIVE

Team Up With Huntington to Fight Cyber Crime

There's perhaps no greater threat to the well-being of your business today than cyber crime.

In an increasingly digital world, online fraud and cyber attacks are ever-present and growing. Today's perpetrators are breaching even the most secure business environments with evermore diversity and sophistication. Lapses in communication and failure to employ appropriate coverages and safeguards can result in irreversible damage and financial loss.

At Huntington, we serve as a key strategic resource to business leaders and their teams. Through a comprehensive approach to business risk and financial management, our banking and insurance professionals help countless businesses secure information, protect against loss and preserve their financial strength.

It all comes down to developing a deep understanding of your business backed by experience serving hundreds, if not thousands, of peers across your industry. The result is differentiated intelligence in the delivery of valuable insights and a dynamic array of solutions that help your business perform.

At Huntington, we look out for every client. Let us put our award-winning team to work for you.

Rick Remiker

SENIOR EXECUTIVE VICE PRESIDENT AND DIRECTOR, COMMERCIAL BANKING

The Huntington National Bank



HUNTINGTON RECENTLY RECEIVED 11 AWARDS OF EXCELLENCE IN MIDDLE MARKET BANKING IN 17 AREAS, SOME OF WHICH INCLUDE NATIONAL AWARDS IN OVERALL SATISFACTION, PROACTIVELY PROVIDING ADVICE, INDUSTRY EXPERTISE, LIKELIHOOD TO RECOMMEND, FUNCTIONALITY AND RANGE OF ONLINE SERVICES, DIGITAL FUNCTIONALITY, EASE OF PRODUCT IMPLEMENTATION AND CUSTOMER SERVICE.

Member FDIC.  and Huntington® are federally registered service marks of Huntington Bancshares Incorporated. Huntington Welcome.™ is a service mark of Huntington Bancshares Incorporated. © 2017 Huntington Bancshares Incorporated.