White paper

Protecting your company against cybersecurity threats

Cyber threats have become a security focus for all companies. Phishing schemes, business email compromise, ransomware, attacks on mobile devices, and insider threats all pose increasingly serious challenges. Information security risk mitigation strategies can help address many of the dangers, but often, the first and best defense is the "human firewall" — employees who are trained to recognize and report cyber threats and possible incidents.

The financial losses from cyberattacks are staggering, with the cost of a data breach averaging $4 million,[1] but the overall cost and financial damage can be much higher. Cybersecurity attacks can damage a company's reputation, decrease its stock price and status, and result in lost customers, lower share value, and declining financial strength.

Additionally, in the aftermath of a cyberattack, companies may need to pay for expenses such as forensic investigations, legal expertise, replacement of lost or stolen physical equipment, application security upgrades, customer notification, call center assistance, customer credit monitoring, and possible regulatory fines. Added costs can also be incurred for the loss of intellectual property and damage done to the IT infrastructure hosted by a third-party organization.

The rise in cybersecurity incidents is likely to continue and can affect any company, regardless of industry. Many cybercriminals are linked to rogue nations and organized crime syndicates. Once data, funds, intellectual property, and business intelligence are stolen, criminals move assets quickly and capture or recovery becomes less likely. Experts estimate the annual cost of data breaches will reach $2.1 trillion globally by 2019.[2]

TYPES OF CYBERATTACKS PREVALENT TODAY

The majority of data breaches succeed because they rely on company employees taking some action — for example, responding to a malicious email or text message. These messages ask recipients to open an attachment or click on a link, possibly giving cybercriminals entry into company networks and access to sensitive data.

(continued)

SHOULD YOU CONSIDER CYBER INSURANCE?

To help manage the costs and activities associated with data breach recovery, many companies are turning to cyber insurance. Executives and boards view cyber insurance as one of the necessary risk management tools to help round out a sound risk mitigation strategy and approach.

Cyber insurance coverage is still relatively new and there is limited case law experience to indicate if it is effective. Its popularity is growing, however, and the global cyber insurance market is expected to reach $14 billion by 2022.

Cyber insurance policies generally cover damages and claims related to:

- The theft, loss, or unauthorized disclosure of company data
- Malware, ransomware, and denial-of-service (DOS) attacks resulting in the theft, corruption, deletion, or alteration of company data
- The unauthorized selling or sharing of company or customer data
- Product liability claims from customers on hacked equipment

Most insurers require companies to have certain information technology security measures in place to qualify for coverage. They generally ask for the completion of a detailed cyber insurance application that covers the company's loss prevention policies and measures such as encryption, firewalls, data back-up plans, mobile device management, and employee data-handling protocols.

Companies are wise to "read the fine print" on cyber insurance policies. They don't cover everything, such as damage to reputation and brand, loss of customer confidence, the potential loss of business partners, or the full impact of the loss of intellectual property. Many policies have "carve-outs" that exclude paying out for a data breach, depending on whether the company had taken sufficient steps to protect itself from cyberattacks.

MUFG Union Bank, N.A.
A member of MUFG, a global financial group

MUFG

Companies are at risk from a wide range of cyber threats:

- **Phishing schemes** – Cybercriminals broadly disseminate phony emails or text messages, hoping to lure unsuspecting recipients to click on a link or take other actions that could put their credentials and company information at risk. Phishing emails often are worded to cause alarm and provoke quick action. They may contain attachments, photos, .pdf files or Microsoft documents that can trigger malware or ransomware, or infiltrate a company's network when opened. Many phishing emails are spam-styled messages with no specific target.
- **Spear-phishing** – These phishing attacks are targeted to specific individuals whose job functions can provide access to company funds or sensitive data. The cybercriminal impersonates a legitimate business or individual and sends an email request to trick the employee into providing user names, passwords, account numbers, credit card details, and other sensitive company data. Often, the sender's email address appears correct, but it is slightly different from the address of a legitimate business partner and under the control of the cybercriminal. A form of spear-phishing is "whaling," where executives from a company are actively targeted.
- **Business email compromise (BEC) scams** – These targeted attacks often begin with the cybercriminal sending a spoofed (fake) email message to pose as a senior company executive, directing an employee to send an Automated Clearing House (ACH) payment or wire transfer of company funds to a bank account or vendor. The account may appear legitimate, but it actually is controlled by the cybercriminal. As soon as the funds arrive, they are quickly transferred out and the money may be lost.
- **Distributed denial-of-service (DDoS) attacks** – These attacks originate from many compromised computers distributed across the internet, involving hundreds or thousands of systems. They simultaneously attack a target, overwhelming systems with fake data traffic and effectively shutting down access to company websites. DDoS attacks may be used as a decoy to draw the attention of cybersecurity defenders away from other criminal actions intended to steal company data or funds.
- **Mobile device threats** – Many companies have adopted "bring your own device" or BYOD policies, but the widespread use of smartphones, tablets, and smart watches in the workplace pose an additional layer of vulnerability. Simply clicking on links in text messages or downloading a vulnerable mobile application can put mobile phones and all their data (email, contacts, passwords, and activity history) at risk.

(continued)

TIPS TO COMBAT CYBERSECURITY THREATS

Cyberattacks succeed when employees are not fully aware and watchful. Recently, cybercriminals have been aggressively adopting tactics that rely on employee actions rather than trying to exploit or attack corporate software systems.

By building awareness of the threats and conducting ongoing training, employees can change their behavior and become more vigilant. Some best practices that enable employees to strengthen cybersecurity are:

1. Use strong passwords or passphrases with two-factor authentication whenever possible.
2. Keep passwords private, use a password manager to remember them, and do not reuse passwords on more than one site.
3. Slow down when responding to emails. Look for red flags that may indicate phishing.
4. Don't click on links or download attachments unless you know the email is from a legitimate source.
5. Avoid using free public Wi-Fi with workplace devices. Always connect through your company's virtual private network.
6. Never transmit confidential company information using a personal email account.
7. Never provide sensitive or personal information to anyone by email or phone unless you can verify their identity.
8. Never download sensitive company information onto a physical storage device such as a thumb drive.
9. Don't overshare on social media — cybercriminals use social media to track travel plans of employees and executives.
10. Treat laptops, tablets, and phones like money; always keep them with you and secure access to them with passcodes.
11. Keep desktops and computer screens clear of sensitive information in the office and lock the computer screen when stepping away from the desk.
12. When traveling or working outside the office, follow appropriate security measures, such as keeping PC and personal devices locked and stored in safe places, and use passwords for access to devices.

WHAT YOUR COMPANY CAN DO TO MITIGATE CYBER RISK

The first step in addressing cybersecurity threats is to develop a risk mitigation strategy. It should begin with a review of IT assets to gauge their vulnerability to attacks, complete with risk assessments to ascertain vulnerabilities and strengthen safeguards. It's important to account for sources of potential risks, including those posed by third-party vendors and business partners. Cross-functional teams comprising IT, security, and finance professionals can help develop this risk strategy.

Another important part of a risk mitigation strategy is to develop a cyberattack response plan with representatives from IT, operations, legal, compliance, security, marketing, communications, and public relations. The response plan should detail how the company would respond in the case of a data breach and whether public messages would be needed. The response plan should be shared with senior executives and the board.

One of the most important elements of an effective plan is for businesses to focus on education and training to raise their employees' awareness of cyber threats and what to do in the case of encountering a potentially threatening source. An adequate budget to support ongoing education and training is essential to remaining vigilant, because threats are ongoing and constantly changing.

Finally, a company should have a strong cadre of cybersecurity practitioners as part of its enterprise-level security program. Systems, applications, and networks need to be regularly patched, updated, and backed up. And access to devices, data, and applications by employees and third-party vendors ought to be only on a "need-to-use" basis and actively managed.

MAKE CYBERSECURITY EVERYONE'S CONCERN

Employees play a critical role as part of a company's first line of defense against cybersecurity threats. Although they are most often responsible for inadvertently allowing a threat into company systems, through ignorance or negligence, employees also can form a "human firewall" to prevent attacks from succeeding.

A key element of a cyber risk mitigation strategy is to educate employees on an ongoing basis about the latest risks and threats. By raising awareness of the prevalence and techniques of cyberattacks and the severity of their consequences to the company, employees can assume an important role in risk mitigation and remain vigilant to protect company assets. Employees also need to know what to do in the event of a potential cyber breach. Employees should know how to report any suspicious item they have received, especially if the item has been clicked or opened. Reporting is the follow-on step in risk mitigation as it allows cybersecurity professionals to "close the door" that may have been opened to cybercriminals. The combination of awareness and reporting results in the resiliency necessary to tighten the security perimeter.

Businesses can follow the FBI's reporting of new and emerging cyber risks and obtain industry alerts to stay abreast of the latest cyber threats. The FBI's web page on cybercrime can be found at https://www.fbi.gov/investigate/cyber. Businesses can also follow the threats reported and analyzed by the United States Computer Emergency Readiness Team (US-CERT) at https://www.us-cert.gov/.

With improved employee awareness of the risks and a sound risk mitigation strategy in place, companies can improve their chances of protecting data, money, intellectual property, and other assets from cyber threats.

[1]"Forbes Insights: Enterprises Re-Engineer Security in the Age of Digital Transformation," a survey of CIOs and CISOs, 2017. Available for download at: https://www.forbes.com/forbesinsights/bmc_security/index.html

[2]"Cyber Crime Costs Projected to Reach $2 Trillion by 2019," by Steve Morgan, Forbes, Jan. 17, 2016. Available at: http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#16be59a43bb0

[3]"Hacker Lexicon: What Are DOS and DDOS Attacks?" by Kim Zetter, Wired.com Security blog, Jan. 16, 2016. Available at: https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/

[4]"Cyber Insurance Market to Top $14 Billion by 2022: Report," blog post by Mike Lennon, Security Week blog, Dec. 9, 2016. Available at: http://www.securityweek.com/cyber-insurance-market-top-14-billion-2022-report

8914122-M (04/18)