The human side of cybersecurity:

An employer's guide to managing cyber risk

Introduction

Today cybersecurity has become part of everyone's job, regardless of technical expertise. So we want to help you make sense of it wherever you sit in your organization — especially if that's not Information Technology.

Cybersecurity is a topic of increasing importance for organizations in all sectors. Different industries face different levels of risk and have different risk management capabilities, but all have a common goal: to protect the data and assets of their employees as well as those they serve.

Today cyberattacks continue to reach unprecedented levels with ever-changing targets and tactics. A new survey of cybersecurity experts reveals: "More than 90 percent of respondents [cybersecurity experts] believe that cyber risk is systemic, i.e., capable of impacting many companies at the same time."[1] Cybersecurity is a topic that warrants leadership, innovation and action.

This paper is intended to provide a practical and not too technical overview of:

1. The cybersecurity landscape
2. Cyberattack methods
3. Considerations for employers

The cybersecurity landscape

Cyberspace is everywhere. Cybersecurity isn't.

Organizations of all sizes and types, across all sectors, in all geographic regions rely on systems that are data-driven and internet-based. As the Department of Homeland Security states: "Our daily life, economic vitality, and national security depend on a stable, safe and resilient cyberspace."[2]

As much as the ability to function in cyberspace is a necessity, so too is cybersecurity. Cyber is consistently one of the top three risks businesses face, with the average cost of a breach at approximately $4.3 million.[3] Cyberattacks have become commonplace. The Guardian referred to 2016 as "the year of the hack"[4] but the topic has proven evergreen. In February 2017, news broke that a vast content delivery network (unintentionally) leaked user data and passwords for 5.5 million websites, including some of the most popular websites U.S. consumers visit every day.[5] A hacker known by the alias Rasputin has breached prominent American universities, and threatens to target additional universities, plus federal, state and local government agencies.[6] In May 2017, the global ransomware attack called "WannaCry" became the biggest cyberattack ever—and in the process, proved even the most advanced and well-funded hospitals are at risk.[7]

[1] Is Cyber Risk Systemic?, AIG, May 2017.

[2] Department of Homeland Security, https://www.dhs.gov/topic/cybersecurity, accessed 2/17.

[3] IBM (2016) Cost of a Data Breach Study, retrieved from www-03.ibm.com/security/data-breach, accessed 2/17.

[4] "How 2016 became the year of the hack and what it means for the future," The Guardian, https://www.theguardian.com/technology/2016/dec/21/how-2016-became-the-year-of-the-hack-and-what-it-means-for-the-future.

[5] "CloudFlare Leaked Sensitive Data Across the Internet for Months," Fortune.com, 2/24/17.

[6] "Hacker Breached Dozens of Universities and Government Agencies, Report Says," Fortune, 2/15/17.

[7] "Why Hospitals are So Vulnerable to Ransomware Attacks", CNN, 5/16/17.. http://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/.

Everyone has a role to play

Cybersecurity is no longer exclusively the responsibility of information systems and technology experts. Rather, leaders from various departments must all help their organizations manage cyber risk within their own span of control. Today's leaders set the stage for creating a working knowledge of cybersecurity among employees, which in turn helps their organizations prevent cyberattacks whenever possible, spot them when they do occur, and respond swiftly as needed.

Within each area of an organization (regardless of discipline), cybersecurity should be part of day-to-day working life. Professionals representing departments from Legal to Finance to Communications and beyond bring unique perspectives and skillsets.

For example, as part of their overall day-to-day responsibilities, human resources professionals may be considered the first line of defense against cybercrime. They serve as stewards of employees' personal data from the start of the candidate application process, to hiring and onboarding, and throughout the employee lifecycle. They also help employees learn (and either reinforce or change) what is considered acceptable or unacceptable within the company culture.

Human resources professionals can play a critical role in helping to raise awareness of cyberattack methods. They are well-suited to partner with information systems professionals and others to create a culture of cyber awareness and resilience.

Cyberattack methods

Cyber criminals prey not only on systems and infrastructure, but also on people—or rather, people's emotions.

Criminals often use a technique called **"social engineering."** Social engineering is the art of clever manipulation of natural human tendencies for the purposes of defrauding a victim or target; in cybercrime, this typically means gaining access to secured areas, confidential information, IT systems, data or other assets that may be protected by a firewall or other means. Instead of using technology to hack in, criminal social engineers use people as their means of attack. They make emotional appeals to individuals' hopes and fears, and take advantage of social norms regarding authority, reciprocity, politeness and guilt. By using people's emotions against them, cybercriminals can successfully obtain user login credentials that open the door to whatever assets they want to destroy or steal.

Other attack methods include:

- **Denial of service attacks**—these attacks have the power to shut down or severely limit access to utilities, transportation and/or government services—with potential to cause greater harm than just denying access to a website.
- **Cyber extortion**—this is a method by which criminals threaten to expose data or deny access to data unless the victim (individual or organization) meets certain demands, usually for money; often this is done through software called "ransomware." The May 2017 "WannaCry" attack in the U.K. and Europe is a perfect example.
- **Phishing**—this is a technique in which criminals attempt to defraud people by creating phony websites, links or emails, often designed to look like they come from well-recognized brands or from familiar or respected people (e.g., they may impersonate the head of Human Resources and request copies of W2s or personal data). By the time an individual notices something doesn't look right, it's too late—either a virus has been downloaded or they've provided personal information or passwords.

Cybercriminals specialize in these methods much like law-abiding workers specialize in their careers. Cybercrime is a business. When career cybercriminals organize, they set up "business" units just as commercial enterprises do—departments that bring together individuals who specialize in the same tactics; some perform the social engineering, others build the malicious software ("malware"), others spend their days hacking. The organizations that would be their targets need to be just as organized across all disciplines, from IT to HR. Today's leaders must have an organized plan for dealing with the criminal organizations that wish to profit from attacking them.

Considerations for employers: Start with people

Employers may consider enhancing their cybersecurity by organizing solutions around three areas: people, processes and protections.

People

Paradoxically, the best ways to combat a high-tech cyber threat is to start low-tech: with people. The premise of social engineering as a cyberattack method is to use unsuspecting people as a weapon against their organizations.

The antidote to social engineering is a culture of cyber awareness. Train and empower individuals to have a healthy skepticism about requests that seem "phishy" (as in phishing attacks), such as:

- An unknown caller asking for contact information of another employee
- An unexpected email urging the recipient to click a link
- A stranger trying to connect via social media
- Any requests to log in or supply user IDs or passwords

The most effective cybercriminals are chameleons—their emails may look like they come from legitimate sources or they may even seem to have social connections in common with their "targets." But they know their identities won't hold up to closer scrutiny, which is why they create false urgency to respond immediately.

Encourage employees to pause in these cases, even when their emotions or their helpful attitude might lead them to do otherwise. Make it clear: If an employee has any inkling a request seems suspicious, it's okay to slow down and verify the source. In many cases, this can be done quickly through a simple check of an online search engine. A two-minute delay could either prevent a cyberattack or at least bring peace of mind that the request is indeed legitimate.

After educating the broad employee base, the next step is to identify who has access to sensitive data; why (i.e., whether they require sensitive information to do their job); how they're trained to protect it; and where responsibility and accountability fall—looking at roles up, down and across organizational charts. Training will vary by job, but remember: Cybersecurity is everyone's job.

Processes

There's no singular "right" way to manage cyber risks, but there are some best practices generally agreed upon by cybersecurity experts. Following these practices, organizations should ensure that there are solid policies and procedures in place to govern the collection, storage and transfer of sensitive employee and organizational data. To the extent that this data is maintained and/or accessed by any third-party providers, provider processes must be considered as well as the organization's own processes.

Consider a seven-step process, some of which may be done in partnership with in-house Information Technology teams and/or by hiring experienced cybersecurity consultants[8]:

Establish standards — Use best practices such as strong passwords, regular virus scans, software updates, data back-ups and other processes.

Develop a plan — Create a cross-functional team of senior management to plan for cybersecurity events and consider hypothetical attacks.

Map out a risk profile — Study cyber patterns and attack modes to develop a tailored approach to protecting company assets.

Assess and measure — Estimate the scope of potential attacks, using rough figures to avoid "analysis paralysis."

Mitigate risk — Invest in risk mitigation measures to protect company assets at greatest risk.

Think about cyber insurance — Consider obtaining cyber insurance to provide contingent capital and specialized assistance in the event of an attack.

Get started — A rough plan is okay—becoming resilient to cyber risk starts with a single step.

[8] AIG, https://www.aig.com/knowledge-and-insights/building-a-Cyber-resilient-business?cmpid=KNC-Google-aig-FTZ-G-INN-Cyber-B, accessed 7/19/17.

Protections

Finally, organizations should protect their data assets with the same rigor with which they protect all other organizational assets—if not more so. A cyber breach would put other assets (personnel, monetary assets and property) at risk. As such, organizations should ensure that the systems and technology used to manage cybersecurity risk meet their needs today, with flexibility to adapt to the changing cybersecurity landscape of tomorrow. Cybersecurity consultants can help provide assessments of current systems and direction if additional systems should be considered.

Insurance coverage provides another form of protection, as well as peace of mind in the event of a breach. Although it's not a stand-alone solution to the complex challenges of cybersecurity, cyber insurance may be an important element of a multifaceted cyber resilience strategy.

Learn more

We're committed to supporting your needs as a professional, as well as the needs of your organization and your employees. We'll do that by providing valuable insights into organizational trends and hot topics. And we want to hear from you. What keeps you up at night and how can we help? Please contact us!

- To learn how we can help you address the topics that matter most to your organization, starting with your retirement plan needs, contact your AIG Retirement Services representative or visit aig.com/RetirementServices.
- To learn more about cybersecurity best practices and solutions available, visit aig.com/cyberedge.

About us

AIG Retirement Services is part of AIG, a Fortune Global 500 Company. You can be confident knowing you are partnering with the strength and experience of an organization entrusted with more than $230 billion in retirement assets for approximately 3 million participants.* For nearly 100 years, AIG companies have been helping protect clients and their families from the unexpected and helping them safeguard their futures. Additionally, our service includes contributing more than 62,000 hours of volunteering annually in the communities we serve.

*Source: Figures include AIG's Life & Retirement defined contribution, annuity and mutual fund business. AIG Retirement Services represents AIG member companies including The Variable Annuity Life Insurance Company (VALIC) and its subsidiaries, VALIC Financial Advisors, Inc. (VFA) and VALIC Retirement Services Company (VRSCO). As of 12/31/18.

Real strategies Let us put real retirement solutions to work for your organization and your employees
CALL 1-888-478-7020 **CLICK** aig.com/RetirementServices

VC 28435 (05/2019) J262303 ER