

BANK OF AMERICA 

Cyber Security Journal

The latest ideas on digital security to help you safeguard what's most important to you

INSIGHTS ON THE NEXUS BETWEEN PEOPLE, TECHNOLOGY AND BUSINESS

HOW TO EDUCATE (OR BECOME) A CYBER-AWARE EMPLOYEE
Ways to make sure everyone at your company understands how important they are to security.

INSIDER THREATS: HOW DO YOU MANAGE THE RISK?
Ideas on how to navigate a growing cyber threat within your defense systems and everyday operations.

Contents

Cyber Security Journal • Issue 4

Letter

3 From Craig Froelich, *Chief Information Security Officer*

Features



4

How to educate (or become) a cyber-aware employee

Cyber security depends on alert, responsive employees. But to tap into this critical human resource, companies need to create adaptable education practices and make awareness a part of everyday workflows, conversation and culture.



10

Insider threats: How do you manage the risk?

Actions by employees and third parties, whether intentional or unintentional, can be as damaging as the most severe breach by a cyber criminal. Your company's security depends on a clear understanding and management of insider risks.

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to, warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor. © 2022 Bank of America Corporation. All rights reserved. 4359629

We're Dedicated to Protecting You Year-Round.



Craig Froelich

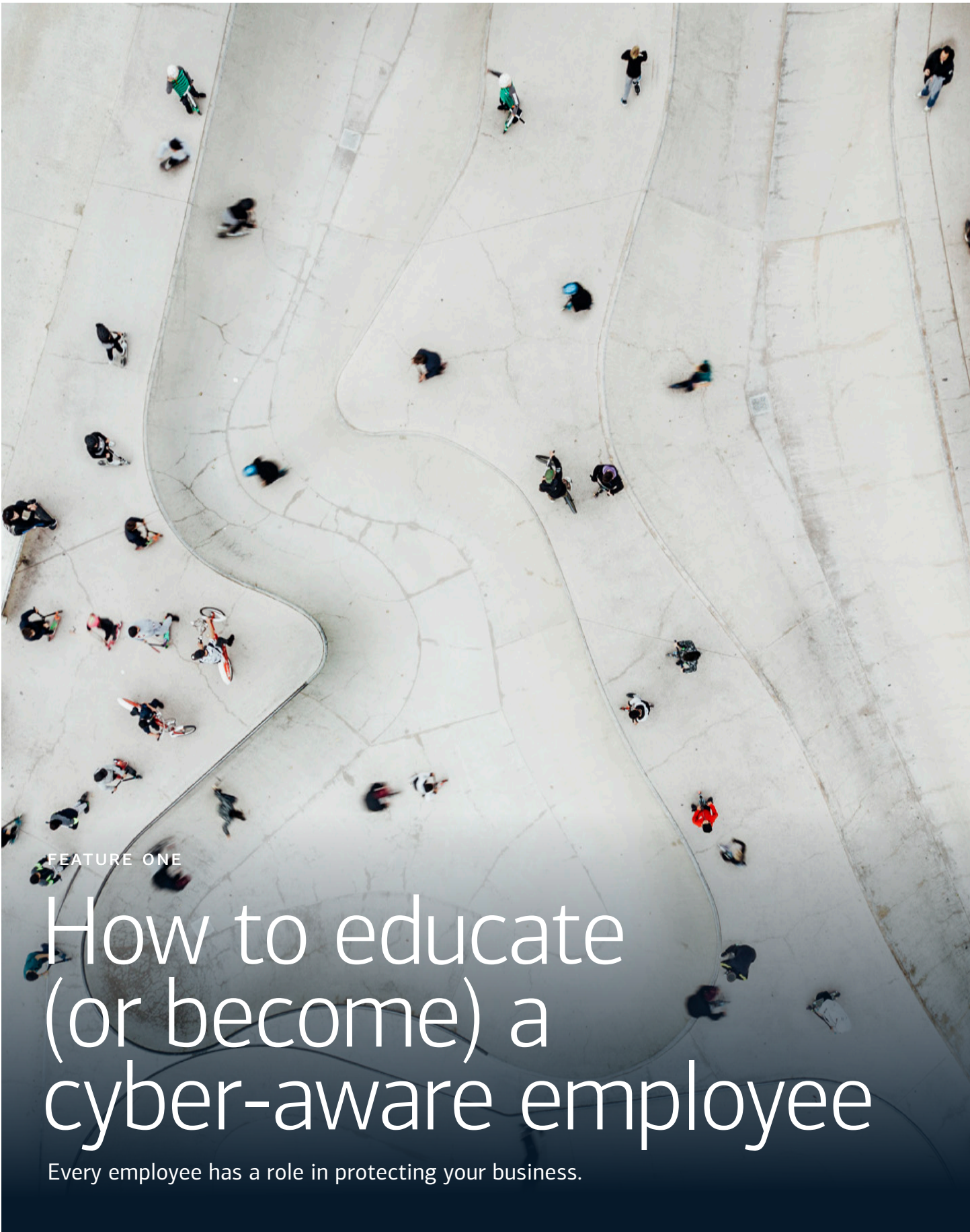
Protecting client information is our top priority. Proactive communication and access to a variety of educational tools is one of the ways we build on that protection. In 2020, we launched our *Cyber Security Journal* as a resource to help clients stay updated on the latest developments in cyber security and learn tips to remain cyber safe.

We continue to build on the information shared last year with our first *Cyber Security Journal* of 2021. Within this Journal, you'll gain an understanding of insider threats, and how best to mitigate them, as well as explore the importance of cyber education programs. Bringing these two topics together, and explaining that a culture of cyber security is the key to risk mitigation across your organization, mirrors the bank's approach to security. From our systems to our operational processes and throughout everyday business interactions, information security and data protection is at the core of all that we do.

As always, we are committed to partnering with you on your information security and dedicated to sharing our knowledge and expertise to help protect you, your business and the broader community.



Chief Information Security Officer, Bank of America



FEATURE ONE

How to educate (or become) a cyber-aware employee

Every employee has a role in protecting your business.



How to educate (or become) a cyber-aware employee

Cyber Security Journal
Issue 4



Cyber education needs to reflect a company's unique risk profile — and its culture.



Cyber crimes often depend on the manipulation of people as well as technology. While defense strategies often focus on tools, many cyber experts believe employees are potentially the most valuable security asset — provided they realize how important they actually are. Companies that take cyber education seriously can gain an important advantage in an era of ever-evolving threats.

What's more, that education should exempt no one: Ideally, each employee will participate in and promote companywide awareness. These days, it's not enough to simply provide annual risk-based cyber education and training exercises. In most companies, cyber

awareness should be a common cultural value and a benchmark of every employee's performance.

Like any discipline, cyber security includes fundamental principles and information that apply to almost any business. But every awareness program needs to be tailored to the company's distinct market

position, individual threat landscape, business risks, customer requirements and culture. There is no "one size fits all" approach that anticipates every possible threat a company may face: In one study, 69% of surveyed small businesses reported that cyber incidents were becoming "more targeted" each year.¹

There is robust debate about what types of training and threat simulations are most effective. Since security is partly a function of what does not happen, in terms of breaches, infections, data loss and other incidents, it can be problematic to evaluate the effectiveness of any particular training regimen. Furthermore, it is a challenge to choose which tools and simulations will best serve a company, as more products and training packages become available.

“Employees are potentially a company's most valuable security asset — provided they realize how important they actually are.”



How to educate (or become) a cyber-aware employee

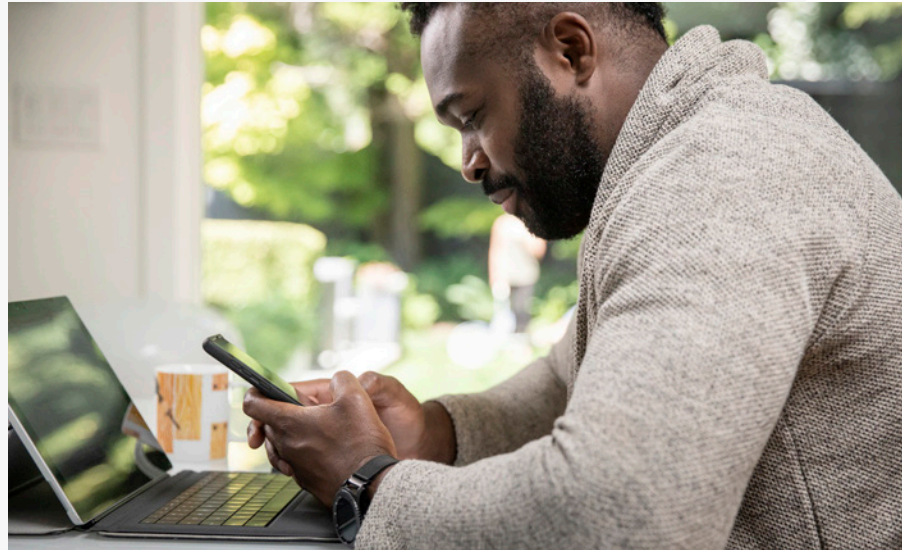
Cyber Security Journal
Issue 4

Fortunately, even businesses with limited budgets can improve their cyber education with open-source tools and an approach that prioritizes awareness. The most secure companies will benefit from employees who treat cyber security as a primary function and willingly play a defender's role.

New threats in the new normal

It's important to recognize that cyber threats arise from new malware and criminal tactics and new work processes. If malware and social engineering are the criminals' tools, the new work processes present opportunities to use the tools.

The coronavirus pandemic, for example, created a host of new security challenges almost instantaneously. In 2020, millions of workers were sent home to work, often using unsecured personal devices and computers in a rapidly deployed



Increasingly, cyber crime is targeting remotely supervised workers.

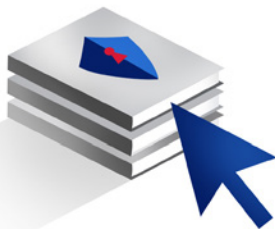
Cyber education tools and methods

Simulations: Mock security incidents that help workers learn to identify and report social-engineering threats.

Gamification: The use of game mechanics to drive engagement in business scenarios and change behaviors.

Tabletop exercises: A scenario-based simulation of the various stages of a cyber attack, typically played in teams.

Hackathons: An internal event in which developers and others work together to solve a security threat or coding error.



remote-work initiative. Cyber criminals wasted no time in launching sophisticated coronavirus phishing campaigns targeting remotely supervised workers. A recent survey found that more than half (53%) of businesses reported a spike in phishing attempts during the pandemic, and 30% said that social-engineering campaigns like phishing are becoming more sophisticated and successful.²

Also on the rise are business email compromise (BEC), vishing (voice phishing) and smishing (text phishing), in which a cyber criminal impersonates a trusted friend or co-worker in a bid to steal data and money. These social-engineering scams can be particularly risky for mobile phone users, since consumer mobile devices typically lack anti-phishing or anti-malware safeguards that are used on corporate devices. What's more, mobile equipment often connects via cellular or home Wi-Fi without the protective cloak of corporate virtual private networks (VPNs).

There also is a growing need for education to cover risks associated with third and fourth parties. Third-party risks are associated with a company's vendors and suppliers, while fourth-party risks occur when third parties outsource tasks to their suppliers. As these connections multiply and involve more elements of company networks, employees need tools for assessing the potential risks and identifying weaknesses in the security and prevention policies of partners and vendors.

With so many changes afoot simultaneously, cyber security awareness has become an indispensable job skill for practically all employees. But the onus is not on individuals alone: Companies must prize alertness and



How to educate (or become) a cyber-aware employee

Cyber Security Journal
Issue 4

find ways to keep security in the general conversation at all times. Cyber education programs need to reflect the current threat landscape and include cyber hygiene as a core value.

A culture of cyber security is critical to education

Cyber education will be most effective when it is built on a culture of security in which cyber security is embedded in the company DNA. In a security-focused culture, every employee knows what role they play, takes ownership of their security responsibilities, and is held accountable for their actions.

A culture of security should build knowledge and trust — and not create fear by intimidating employees who make a mistake. In fact, there is a growing consensus that motivation through fear is not effective.³

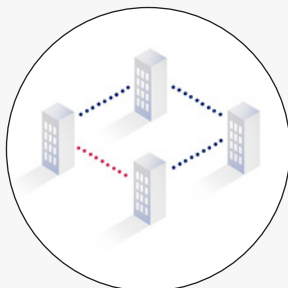
The “why” behind cyber security education must be made real — and relevant — to all employees. It’s particularly important to communicate the potential real-world impact of breaches on business performance

Cyber education for an expanding threat landscape

Security depends on all employees maintaining awareness of the risks a company faces. While every company’s security profile is unique, here are general categories education may address:



BEC, phishing, smishing and social-engineering scams, in which criminals manipulate and deceive employees.



Third- and fourth-party risks. Issues related to vendors a company has direct and secondhand contact with, through network access, or software services or data sharing.



Security of mobile and personal devices employees may use for work purposes.



Remote work protocols that cover home offices and business travel.



Insider threats. Intentional or unintentional security breaches caused by employees or contractors.



How to educate (or become) a cyber-aware employee

Cyber Security Journal
Issue 4



Cyber education must have a leadership strategy and company-wide engagement.

Best practices for creating a culture of security awareness

- Establish formal cyber education programs.
- Make security training engaging and relatable.
- Provide clear and intuitive security procedures.
- Provide frequent, mandatory education on current cyber threats.
- Lead by example, from the top down.
- Refer all employees to publicly available cyber security resources, such as National Cybersecurity Alliance.
- Continually update software and systems.
- Explain the importance of strong passwords.
- Promote secure cyber habits.



and data security. Doing so will drive home the consequences of disregarding security processes and help ensure the success of data-protection programs.

Employee engagement is also essential. Rather than issuing a list of do's and don'ts, businesses should establish relevant, engaging learning programs that help build a sense of shared responsibility, accountability and engagement. As part of security

education, businesses should provide security knowledge employees can use in their personal lives to help build secure habits that last.

The most critical success factor, however, is proactive, pervasive support of education by senior leadership. Cyber training will not be widely adopted and effective without active promotion and participation from the C-suite.

A balanced awareness curriculum

A balanced education curriculum should encourage employees to participate in learning by combining realistic (and relatable) simulated cyber threats with positive, supportive feedback when a threat has been correctly identified. For instance, phishing simulations should help those who click a malicious email link to learn from their mistake without creating friction or resentment.

It's also important that cyber education aligns with your business culture and current approaches to education in general. It should reflect a company's risk profile and address topics that are familiar risks for employees and the business.

Given the accelerated evolution of threats and technologies, a company may need to step up its awareness program and implement continual and

consistent education. A single, annual training seminar may no longer be sufficient for employees to remain alert and informed for the rest of the year. Security educators need to promote awareness at all times.

For many companies, phishing simulations are the most critical — and urgent — learning exercises. The rapid evolution of phishing techniques has made it necessary for training to reflect current, real threats to the business.

“Rather than create a list of do's and don'ts, cyber education should encourage employee engagement.”



How to educate (or become) a cyber-aware employee

Cyber Security Journal
Issue 4



Simulations can improve preparedness and increase overall cyber awareness.

Although they're not new, phishing simulations can still be effective and are comparatively easy to carry out. They involve sending mock phishing emails to employees, with tabulations of who opens the email and who clicks the would-be malicious links or files.

Those who open and click the simulated phishing message should receive feedback and guidance on identifying future phishing attempts. Employees who report the email as a phishing attempt should be recognized and rewarded.

Some security educators are incorporating game mechanics and competitions to boost engagement and participation in training. For example, an "escape room" challenge can put employees in the shoes of a would-be social engineer as they try to steal information in a fabricated environment.

Exercises with a similar learning process are ones that play out the what-ifs in a security breach. What-if scenarios can be powerful because instead of laying down rules, participants act out multiple scenarios that show what a social-engineering attack or data compromise looks like and how to respond.

In designing education exercises, consider including team-based activities that test skills and create a sense of amicable competition. And remember that publicly recognizing success is key to making employees feel valued and motivated. ■


Key takeaways:

- Security education should reflect the organizational culture, risk appetite and risk awareness of the individual business.
- Companies must build awareness programs that are embedded in a culture in which responsibility for security is shared by everyone.
- Security education should cover risks that are real and relatable to employees.
- Employees should be trained on third- and fourth-party risks.
- Companies should ensure that employees of third- or fourth-party partners are educated on security policies and prevention.

¹ Ponemon Institute: "2019 Global State of Cybersecurity in Small and Medium-Sized Businesses," October 2019.

² Cybersecurity Insiders and Great Horn, Phishing Attack Landscape report, 2020.

³ Wall Street Journal, "Why Companies Should Stop Scaring Employees About Cybersecurity," December 7, 2020.



FEATURE TWO

Insider threats: How do you manage the risk?

It's not just about technology. The response to this cyber challenge is specific to how each business operates.



Insider threats: How do you manage the risk?

Cyber Security Journal
Issue 4



Imagine the potential consequences in the following scenarios: Cyber criminals hijack customer accounts after they compromise a social media platform manager's credentials through social engineering. Employees of a software provider misconfigure security rules and inadvertently expose customer records to the public. A disgruntled employee of a manufacturer sabotages a source code and steals intellectual property after being passed over for a promotion.

These examples, which are all based on actual incidents, illustrate the severity of major security breaches caused by insiders. Unlike external hackers and cyber criminals who must gain access to a company's systems, insiders already have access and can either cause harm themselves or be manipulated by outsiders to do so.

Insider threats may seem like an exclusively technological challenge, but make no mistake: They also involve normal business processes that can involve employees at all levels of the company. Protection depends on a clear understanding of how the company operates and which processes might increase risk.

There are three main categories of insider cyber security risks. **Non-malicious, unintentional threats** come from employees who violate access rules, either through inattention or negligence. That could be someone who is unknowingly exploited through social engineering or phishing, or an employee who accidentally emails sensitive data to the wrong person. It's the most common category of insider threat and, while inadvertent, can end up costing more per incident if it opens the door to credential theft.¹

Non-malicious and intentional threats involve people who deliberately violate a security policy but do so without intent to cause the company harm. This can be a person who sends company data to a personal email account in order to work on it

“Many organizations view cyber security as a function of technology and data and overlook the importance of insider threat awareness.”



Employees and third parties can make a company more — or less — cyber secure.

Insider threat prevention as a process

Companies with limited security budgets can mitigate insider threats through measures that depend more on people and processes:

Training: Provide employees with resources that define the insider threat particular to the company and promote cyber security hygiene.

Incident response plans: Build a set of processes for responding to insider breaches and update it regularly.

Leadership: Designate employee or departmental leads on insider threats.

Analyze loss: If an insider incident occurs, assess the damage and re-evaluate the cost of increasing cyber security spending.

Prioritize data: Determine what company data is mission critical and protocols for access.





Insider threats: How do you manage the risk?

Cyber Security Journal
Issue 4



Insider threats may involve deliberate or inadvertent actions by employees.

some way — usually out of anger or other heightened emotion — and there is the criminal opportunist who tries to steal from the company for personal gain. These criminal actors might be placed by advanced external parties (e.g., nation-states) in order to infiltrate the organization for other criminal purposes. Actors with malicious intent tend to make up the smallest percentage of insider threat cases, but the damage they cause can be very costly.²

at home, or one who takes shortcuts such as sharing login credentials with a co-worker.

Malicious insiders can be divided into two types: There is the intentionally malicious person trying to hurt the organization in


Trends that elevate insider threat

The frequency and the cost of internal threats have been rising considerably. The number of insider incidents increased by 47% between 2018 and 2020, and

Four Key Elements to Insider Threat Defense

Protecting an organization from internal risk requires a strategy that combines technology, process and people, including:


1



Access Management

- Access management tools
- Segregation of duties (SoD)
- Least-privilege access
- Zero-trust principles
- Physical access to facilities


2



Monitoring and Analysis Tools

- Data loss prevention (DLP)
- User- and entity-behavior analytics (UEBA)

3



Company Policies

- Clearly communicated
- Consistently applied
- Regularly reviewed
- Informed by IT and HR

4



Education and Training

- Documented policies and procedures
- Cyber security employee awareness training
- Company culture



Insider threats: How do you manage the risk?

Cyber Security Journal
Issue 4



Threat defense requires a careful assessment of who has access to what, and when.

“ Access is the most important factor to consider with regard to insider threats because access is what makes an insider an insider.”

the overall cost of these threats rose from \$8.76 million to \$11.45 million in the same time span.³

The rise in remote and distributed work is also increasing the use of cloud capabilities — whether approved video conferencing tools, unapproved communication channels, or even data storage — thereby further expanding threat vectors. Other technology-based risks arise from remote workers' home networks being more vulnerable than in-office networks or being configured insecurely.

Working remotely increases risk in more basic ways as well. With less physical oversight and observation (such as from security cameras or office mates), employees have more opportunity to cause intentional harm by capturing sensitive information with a smartphone camera, for example, or covertly installing invasive software.

The best defense unites IT and all enterprise partners

A strong insider threat defense will likely develop a combination of software tools, processes and information from across the enterprise that covers physical security, human resources, and collaboration across investigative teams. Technology that

detects and deters threats is becoming more sophisticated, but it still depends on good data and collaboration to be efficient.

Access management is the critical piece of the defense, since access is what makes an insider an insider — they have approved and sometimes privileged access and a better understanding of where and what a company's valuable assets are.

To protect those assets, companies should ensure that they have not only implemented solid access management tools but have also set up strong policies and controls. These can include segregation of duties (SoD), which keeps users from assuming excessive privileges that allow them to circumvent normal controls; least-privilege access policies, which give the minimum privileges necessary to perform a function; and in some



Insider threats: How do you manage the risk?

Cyber Security Journal
Issue 4



Insider Data Points

Assessing the cost of
internal threats:

\$11.45 million

Documented cost of insider threats in 2020

62%

of incidents involve non-malicious,
unintentional insiders

\$871,686

Average 2020 cost per incident from
insider-related credential theft

23%

of incidents involve criminal
and malicious insiders

77

Average number of days to contain
an insider threat incident

66%

of organizations had more than 30
insider threat incidents per year

All statistics from Ponemon Institute, 2020 Cost
of Insider Threats Global Report, January 2020.

cases zero-trust principles, where no one is given access without strict identity verification, explicit authorization and continuous monitoring and validation.

Access management can also encompass physical access to facilities, where employees are given access to only the floors and areas required for their work functions.

Even with this infrastructure in place, insiders with authorized access can still pose a security risk, so the next line of defense may implement solutions for monitoring, logging and analyzing who has access to what and when. Data loss prevention (DLP) software can help identify, monitor and protect company data to avoid both unintentional leaks and intentional misuse of data by insiders. User- and entity-behavior analytics (UEBA) can help identify anomalous activity that may indicate a potential insider threat.

But even the most advanced tools require clear and consistent processes and policies in place — and regular review of them — to be effective. IT can work with enterprise partners to set up processes to ensure that if emotional triggers are identified, for example, they can implement proactive controls as a preventive measure before an impassioned employee can take rash action. Employees whose employment has terminated should have access restricted or removed immediately, with controls implemented based on time of notification rather than waiting until the person has left the premises.

“As technology improves and we’re better able to prevent and protect, threat actors will increasingly target human weakness to gain access to your company or your data.”



Management must extend to terminated vendor contracts and ex-employees.



Insider threats: How do you manage the risk?

Cyber Security Journal
Issue 4



While every employee is potentially part of the problem — they are also a part of the solution.

Education mitigates the unintentional insider risks

Of course, tools and rules are only useful if employees are using them appropriately and consistently. Well defined, documented policies and procedures — and resources such as handbooks and intranets to disseminate them — can help employees understand how anyone can become a threat vector, often without any malice intended.

Technology-based threat detection will continue to improve (through developments in machine learning and advanced analytics, for example), but criminal actors will always be able to count on human fallibility for opportunities to breach defenses. Cyber security awareness and education will remain essential to recognition and prevention of all types of insider threats.

“Companies need to identify their most valuable assets — be it intellectual property, client lists, brand, or reputation — in order to determine the greatest risk of insider threat.”

As with all aspects of cyber security, insider threat defense becomes more effective the more it meshes with company culture. In addition to improving communication and training, companywide awareness can help managers discern when stressors or emotional triggers may be affecting an employee or ensure that best practices are being applied consistently. Organizations that increase awareness and employee buy-in are deploying one of the most effective threat deterrents available. ■

Organizations that increase awareness and employee buy-in are deploying one of the most effective threat deterrents available. ■

¹ Ponemon Institute, 2020 Cost of Insider Threats Global Report, January 2020.

^{2,3} Ibid.

Key takeaways:

- Insider threats are technological and people-based challenges. It requires an enterprise effort to create a solid defense.
- Unintentional security incidents may do less damage, but they're much more common and might set off a more serious breach.
- Employee awareness and training are essential to mitigating non-malicious insider threats and increasing awareness of malicious activity.