# KEEPER OF THE VAULT:

# A BUSINESS OWNER'S GUIDE TO CYBERSECURITY

†This is not a CPA firm.
*Assurance, attest, and audit services provided by Carr, Riggs & Ingram, L.L.C.

"Carr, Riggs & Ingram" and "CRI" are the brand names under which Carr, Riggs & Ingram, L.L.C.* ("CRI CPA*"), CRI Advisors, LLC† ("CRI Advisors†" or "Advisors†"), and Capin Crouse, LLC* ("Capin Crouse CPA*"), and CRI Capin Crouse Advisors, LLC† ("Capin Crouse Advisors†") provide professional services. CRI CPA*, Capin Crouse CPA*, CRI Advisors†, Capin Crouse Advisors†, Carr, Riggs & Ingram Capital, LLC and their respective subsidiaries operate as an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations and professional standards. CRI CPA* and Capin Crouse CPA* are licensed independent certified public accounting ("CPA") firms that separately provide attest services, as well as additional ancillary services, to their clients. CRI CPA* and Capin Crouse CPA* are independently-owned CPA firms that provide attestation services separate from one another. CRI Advisors† and Capin Crouse Advisors† provide tax and business consulting services to its clients. CRI Advisors† and its subsidiaries, including Capin Crouse Advisors†, are not licensed CPA firms and will not provide any attest services. The entities falling under the Carr, Riggs & Ingram or CRI brand are independently owned and are not responsible or liable for the services and/or products provided, or engaged to be provided, by any other entity under the Carr, Riggs & Ingram or CRI brand. Our use of the terms "CRI," "we," "our," "us," and terms of similar import, denote the alternative practice structure conducted by CRI CPA*, Capin Crouse CPA*, Capin Crouse Advisors†, and CRI Advisors†, as appropriate.

CRI CARR RIGGS & INGRAM®

criadv.com

Cybersecurity can feel like a game of chance — one where cyber thieves are holding all the cards. After all, when whales like Amazon Web Services, SolarWinds, Colonial Pipeline, and Microsoft turn up losing hands in the cybersecurity strategy game, what chance do lightweights have?

One thing is for sure — cyberattacks are coming fast and furious. Since 2000, the FBI has received more than 9 million complaints of malicious activity. To give some perspective, during its infancy, the FBI's Internet Crime Complaint Center (IC3) received approximately 2,000 complaints per month. In the past five years, the average has been 2,000 complaints per day.

Cyberattacks are here to stay — both because the financial result is lucrative for criminals, and because the bad guys can easily hide from law enforcement. But that doesn't mean you should fold and walk away from the table.

In this guide, we will help you shift the odds in your favor. We will help you understand your organization's true cybersecurity risks (including what is truly at stake), how to design reasonable controls that strike an appropriate balance between security and convenience, and — just as important — how to equip your people with the skills they need to prevent, detect, and respond to cyber breaches.

## COMPLAINTS TO FBI INTERNET CRIME COMPLAINT CENTER

- **Total complaints in 2024: 859,532**
- **Total victim losses in 2024: $16.6 billion**
- **Total victim losses in 2023: $12.5 billion**
- **Year-over-year loss increase: 33%**
- **Costliest schemes: Investment schemes, $6.57 billion**
- **Crime type with most complaints: phishing/spoofing, 193,407 complaints**

**2024 Internet Crime Report**, FBI Internet Crime Complaint Center

# TABLE OF CONTENTS

# 4 STEPS TO ASSESS YOUR CYBERSECURITY RISK

Do you know where an attacker could break through your company's cyber defenses? Chances are, there are more points of vulnerability than you realize, and the stakes are high to protect what's important.

Customers, employees, regulators, boards of directors, and many other stakeholders hold businesses accountable for securing sensitive data. Customers in certain highly regulated industries have their own downstream cybersecurity expectations to comply with, making cybersecurity risk assessments an increasingly common part of standard operating procedures.

One reason for this heightened level of expectation is that every organization is a potential target — no matter the industry or size. In many cases, a small company can be a target simply because it leads to a bigger target.

An example of that scenario is the (appropriately named) mega retailer Target. This infamous watershed cyberattack was made possible by malware planted by a phishing email on the system of a heating and air conditioning vendor. Stealing the vendor's credentials allowed the attackers to access a Target-hosted webpage dedicated to vendors. All they needed to do then was wait and watch to find a way into Target's network. The attack was executed with a frighteningly low level of complexity.

## 4-STEP CYBERSECURITY RISK ASSESSMENT

When you don't understand your true cybersecurity risks, you can't effectively control and mitigate those risks. So how do you know what your true risks are?

### 1. Identify what is at stake.

Assessing cybersecurity risk starts with a clear understanding of what assets are at risk.

Business owners need to know what digital assets they have in play and how to protect them. In today's world, more and more companies maintain information in digital form. The effects on businesses and their clients can be catastrophic if assets are lost, stolen, tampered with, or subject to unauthorized access.

What information and systems run the business day-to-day? What data do you have that an attacker might find valuable? If you own a retail operation, then you most likely have a point-of-sale (POS) terminal to accept credit card payments. Right there are two IT assets: the POS terminal and the data that it collects. Also, consider how secure the servers hosting the critical accounting and finance applications are. Patents and other intellectual property have also become hot targets for attacks. If something happens to these assets, the impact could go beyond the immediate financial hit to include a damaged reputation or a weaker competitive position.

**Other examples of high-value digital assets include:**

- Customer lists
- ACH/wire transactions
- Payroll information
- Proprietary manufacturing processes
- Product launch plans
- Login information
- Employees' health information

Once you've identified digital assets, you can prioritize them. Consider their value to your business, as well as their value to criminals, disgruntled employees, or competitors. Think about the potential impact if those assets were compromised. Where could an attack result in lost revenue or business interruptions, or cause legal issues? In many cases, the reputational damage has the biggest impact on the business — even more than the direct financial impact of the loss or manipulation of the asset itself.

## 2. Understand how data flows.

Identify every place where digital assets are in use, at rest, or in transit. These touchpoints may include local workstations, portable devices, local networks, data centers, or email servers.

Understanding how data moves through your IT system is much easier when you start with a strong understanding of the digital assets included in that system.

**For example, in the retail example above:**

- Credit card numbers and other financial and personal information are *collected* at the POS terminal.
- Some of that information is *transferred* to a third-party payer (the credit card company).
- Another subset of information is *captured* by your accounting system.

Each of these access points — where data enters and exits the IT system — opens up a chance for data theft, loss, or manipulation. Knowing where data is stored, how it is accessed, and who is using it can highlight possible weak points and help prevent a costly breach.

Another important byproduct of this step is the opportunity for good vendor management. Make sure you understand the risks of using third parties. Businesses that outsource asset management cannot offload the responsibility to sustain cybersecurity. Armed with a clear view of how data flows to vendors and other third parties, you can investigate how they are managing and protecting that data. Also consider requesting a service organization control (SOC) report, which assesses the controls that service providers (e.g., data centers, software-as-a-service companies) have in place to maintain the integrity of their processes, systems, and data.

## 3. Evaluate current security measures.

Evaluate the policies and controls that protect what's at risk. One common misconception among smaller companies is that they can't afford the level of protection they need. But many of the most effective controls are common-sense practices that involve some additional effort, but little additional cost.

One of the most effective controls is to carefully manage who can access certain critical IT systems. When was the last time you reviewed who has administrator rights to your server? Another low-cost control involves password requirements. Are you requiring longer, more complex passwords for your important IT systems?

It's true that vulnerability scans, penetration testing, and other security tools can help identify gaps in the security perimeter. But in many cases, you can build a higher fence by implementing some cybersecurity best practices. You or your fellow employees might actually be the most significant vulnerability, due to the prevalence of phishing scams. Armed with a little knowledge, you can take action to shore up those defenses through communication and training.

## 4. Prioritize investments to remediate gaps.

The goal of a risk assessment is to identify and prioritize risks so you can make the most of your budget while meeting the needs of the business. Based on an understanding of what is at risk and the current state of security, you and your fellow leaders can make informed decisions about investments in training, technical controls, and cybersecurity awareness programs. Focus on testing the most important processes most frequently, and maintain a regular schedule for those less-critical company processes. In doing so, your organization can maintain high-level security without unnecessary effort.

## NOW REPEAT

Remember, a risk assessment is not a one-and-done project. It should be a continuous and dynamic process. Once the highest-priority risks are addressed, go back and address the next-highest priorities, and so on. Periodically, you should also circle back to monitor and review how controls are working. And of course, as new vulnerabilities are discovered, assess the impact of these new risks on the company.

# HOW TO CALCULATE INHERENT AND RESIDUAL RISK

The consequences of a cybersecurity breach can be dire for any business, no matter your company's size or the industry in which it operates.

The most important factor in assessing risk is the value of what you're trying to protect — both to your organization and to potential attackers. Even if you think you have a good handle on your company's valuable assets and the potential holes in your defenses, without a documented cybersecurity risk assessment, you're probably missing something.

Different industries have different frameworks for assessing risk. Banks can turn to the **Cyber Risk Institute's Risk Profile**. Healthcare providers and their business associates can conduct a HIPAA security risk assessment using the U.S. Department of Health and Human Services' downloadable **Security Risk Assessment Tool**. Organizations in non-regulated industries may turn to resources like the Center for Internet Security's **Critical Security Controls framework**.

**But at its core, cybersecurity risk boils down to a basic formula:**

(Likelihood of Occurrence
× Impact of a Potential Breach)
÷ Strength of Mitigating Controls

= Residual Risk

This seemingly simple formula requires quite a bit of nuanced understanding — of your business's valuable assets and where they reside, of the weak points in your defenses, and of the best ways to lower your risk level.

Before examining the components of this formula, a note about inherent risk and residual risk:

**Inherent risk** (represented by the numerator of the formula) is the "raw" level of risk that exists before applying any mitigating controls.

**Residual risk** is what you get by dividing your inherent risk score by the strength of your mitigating controls. Keep in mind that you don't have to mitigate everything down to the ground. While you want your residual risk as low as possible, it will never get to zero. After all, there's always a possibility of something completely unforeseen happening (hello, global pandemic!).

But if the likelihood of a breach is low, then inherent risk is probably also low. So rather than applying more mitigating controls that will have rapidly diminishing returns, shift your attention to more likely threats.

## LIKELIHOOD OF OCCURRENCE

Determining the likelihood of a threat boils down to two questions: *What assets and critical functions are we protecting? Are people motivated to steal or disrupt them?*

For a manufacturer, proprietary manufacturing processes and product launch plans might be attractive to competitors and even nation-state attackers. Companies that hold vast amounts of personally identifiable information (PII) — data that could be used to identify a specific individual — typically have a high likelihood of a breach by financially motivated attackers. Medical records, which contain all the personal details needed to pull off high-scale identity theft (e.g., date of birth, Social Security number, address, mother's maiden name), are a treasure trove for malicious actors. Bank account, credit card, and debit card numbers, and even cryptocurrency account credentials, are also valuable commodities on the dark web.

## IMPACT OF A POTENTIAL BREACH

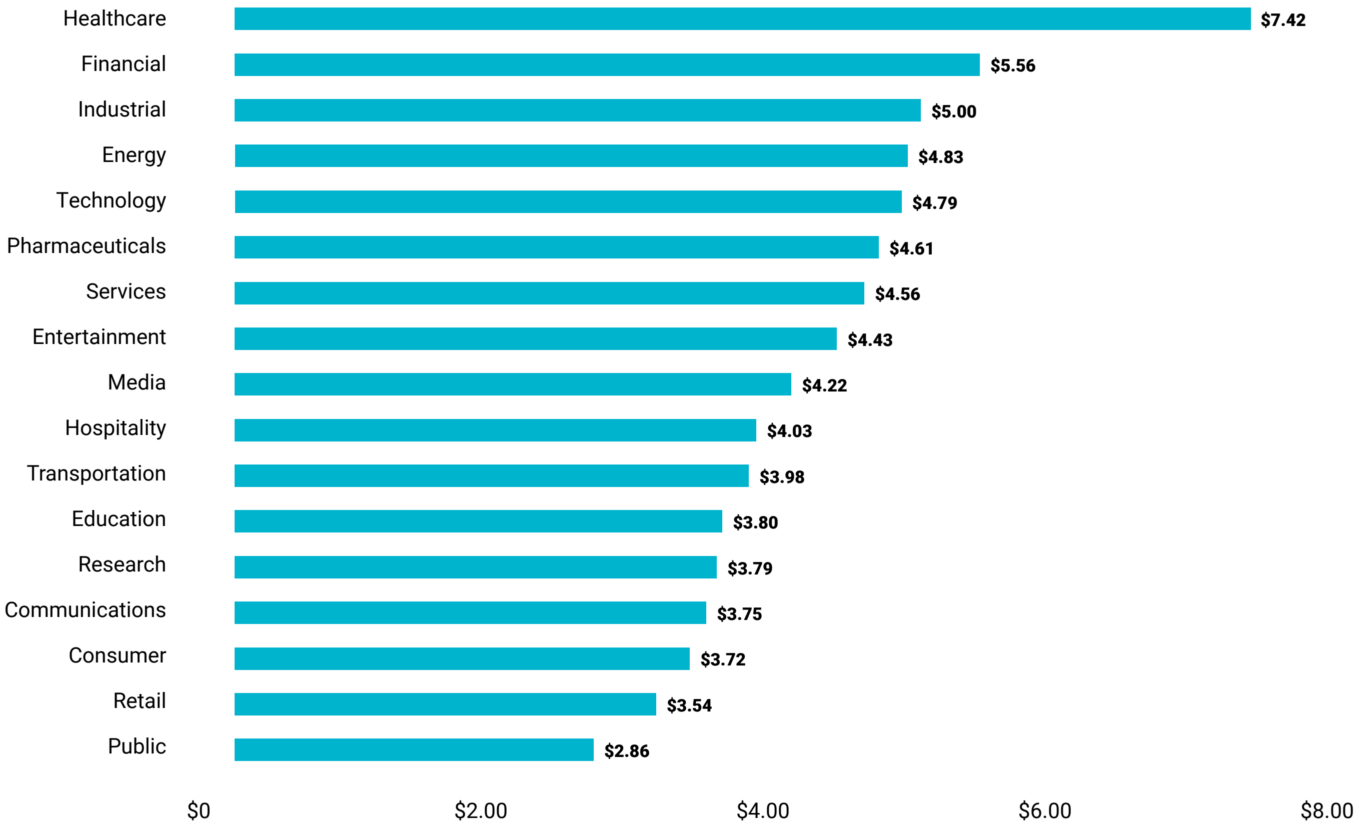
The second component of inherent risk is the potential impact of a successful breach. While there are nonfinancial factors to consider (e.g., reputation), ultimately, they all come back to the company's bottom line.

The cost of a data breach is closely tied to the type of data that is compromised. In IBM Security's **Cost of a Data Breach Report 2025**, 53% of breached organizations said that customer PII was compromised, far more than any other type of data, averaging a cost of $160 per record. Breaches of employee PII and intellectual property happened less frequently, at 37% and 33% of breaches, respectively; however, the cost per record was more expensive, at $168 per employee PII record and $178 per record of intellectual property.

The cost of a data breach varies widely by industry, and healthcare organizations consistently incur the highest cost per data breach. In the 2025 IBM study, healthcare organizations reported an average $7.42 million cost per data breach — 67% higher than the global average of $4.44 million across all industries. The financial industry ranked second at $5.56 million.

## GLOBAL AVERAGE COST OF A DATA BREACH BY INDUSTRY

Measured in US$ millions **(IBM *Cost of a Data Breach Report 2025*, Pg. 12, Fig. 3)**



What do these industries have in common? Regulatory scrutiny. Organizations that must comply with various regulatory requirements often have higher average data breach costs due to fines, penalties, and the costs associated with the required constituent notifications.

Cost of compliance isn't the sole factor that makes breaches in regulated industries so expensive (although those fines can certainly pack a punch). At the end of the day, lost business is just as damaging as regulatory fines. In the IBM Cost of a Data Breach Report 2025, lost business costs (see sidebar) accounted for just over 30% of the average total cost of a data breach, at $1.38 million.

**In the IBM *Cost of a Data Breach Report 2025*, lost business costs include the following:**

- Customers who defected because of the breach
- Increased cost of acquiring new customers due to diminished goodwill
- Revenue losses from system downtime

However, the most significant component contributing to the cost of a breach related to detection and escalation — which includes such things as costs required to investigate and confirm the existence of a breach, to prepare memos or briefings to leadership, and to engage external legal counsel or crisis management teams. In a breach costing $4.4 million, the costs to identify and escalate a breach were $1.47 million. While this amount has declined since the previous year, it continues to highlight the importance of investing in controls to not only prevent attacks but also detect potential issues. Breaches are a matter of when, not if, so organizations that can more efficiently detect, investigate, and escalate a breach can implement containment and remediation activities faster, reducing the overall cost of the breach.

## MITIGATING CONTROLS

One way to assess the state of your company's mitigating controls is to ask the following questions:

***How quickly can we catch a breach?***

On average, companies in the IBM Cost of a Data Breach Report 2025 required 241 days to identify and contain a breach — down from the 2021 peak of 287 days. As mentioned above, detection is a key component to reducing breach costs, and the nine-year low of 241 days shows that organizations are investing in the tools, technologies, and resources to detect issues more effectively.

The breach life cycle varies widely depending on industry. In healthcare, the life cycle averaged 279 days — which was about 5 weeks longer than the global average. Adoption of security automation and artificial intelligence (AI) continues to speed up the average time to identify and respond to a breach. IBM found that adoption of these detection controls reduced the average life cycle of a breach by 80 days and the total cost by $1.9 million compared to organizations that did not utilize automation or AI.

***Are we doing all we can to protect our valuable data? And if so, is that enough?***

Maybe you have invested all the resources that you can in automated controls, but the risk still isn't mitigated to an acceptable level. Could you institute a process whereby manual inspections supplement automated controls? In cases where the residual risk remains too high, companies increasingly transfer this risk using cyber insurance. (Just remember that cyber insurance is not a panacea for cyber risk.)

## WHAT'S YOUR RISK FACTOR?

On a personal level, you might not think about risk in a particularly formulaic way. Instead, you probably have a gut-level understanding of how risky different scenarios are. But when it comes to your business, you can't afford to rely on a gut check.

# KEEP PASSWORDS SECURE

Passwords are often the first line of defense against cyber threats, yet they remain one of the weakest security links for many organizations. Cybercriminals continuously refine their password-cracking techniques, exploiting weak or reused credentials to compromise sensitive data — putting businesses at risk of financial and reputational damage.

In industries like finance and healthcare, where regulatory compliance is critical, the consequences of these attacks can be severe, with a single compromised password potentially resulting in fraudulent transactions, regulatory penalties, or the exposure of sensitive patient records. Protecting both financial and operational integrity requires a clear understanding of how passwords are cracked and the implementation of robust defenses to reduce exposure to cyberattacks.

## COMMON PASSWORD ATTACKS AND HOW TO DEFEND AGAINST THEM

Recognizing the tactics cybercriminals take to steal passwords is the first step in protecting your business from attacks. The following are three of the most prevalent password-cracking methods, along with proactive measures companies can take to mitigate these risks.

**Brute force attacks:** Brute force attacks involve cybercriminals systematically guessing passwords by testing different character combinations until they find the correct one. These attacks have become more efficient with increasing computing power. Hackers use software to automate brute force attempts, testing millions of password variations in minutes. Predictable passwords — such as sequential numbers or common phrases — are particularly easy to crack.

Protecting against brute force attacks requires multiple security layers. Using long, randomly generated passwords — at least 12 characters — makes brute force attempts far more difficult. Enforcing account lockout policies, which temporarily disable accounts after multiple failed login attempts, further reduces the risk of sustained attacks. Multi-factor authentication adds an extra barrier, keeping accounts secure even if a password is compromised.

**Dictionary attacks:** Dictionary attacks allow cybercriminals to break into accounts using precompiled lists of commonly used passwords and phrases. Unlike brute force attacks, which test every possible character combination, dictionary attacks exploit predictable human behavior. Many users prioritize convenience, opting for passwords that make these attacks highly effective.

Mitigating dictionary attacks requires a proactive approach, such as using passphrases — longer combinations of random words, numbers, and special characters — that add complexity while remaining easy to remember. Businesses can reduce risk further with password filtering tools that block weak or breached passwords.

**Rainbow table attacks:** Rainbow table attacks exploit weaknesses in password storage by using massive databases to decipher encrypted credentials quickly. While most companies store passwords in a hashed format rather than plaintext, weak hashing algorithms and inadequate security measures can still leave them vulnerable. Attackers compare stored hashes against rainbow tables — vast collections of precomputed hash values — until they find a match, drastically reducing the time needed to crack passwords.

Defending against rainbow table attacks requires "salting" passwords, which adds random data before hashing to prevent direct comparisons within precomputed tables.

## PARTNERING FOR STRONGER CYBERSECURITY

Weak password habits leave companies vulnerable, making strong password protection a critical part of any defense strategy. With cyber threats constantly evolving, waiting to act isn't an option. Work with your cybersecurity advisors to identify vulnerabilities and implement strategic defenses that keep your business secure.

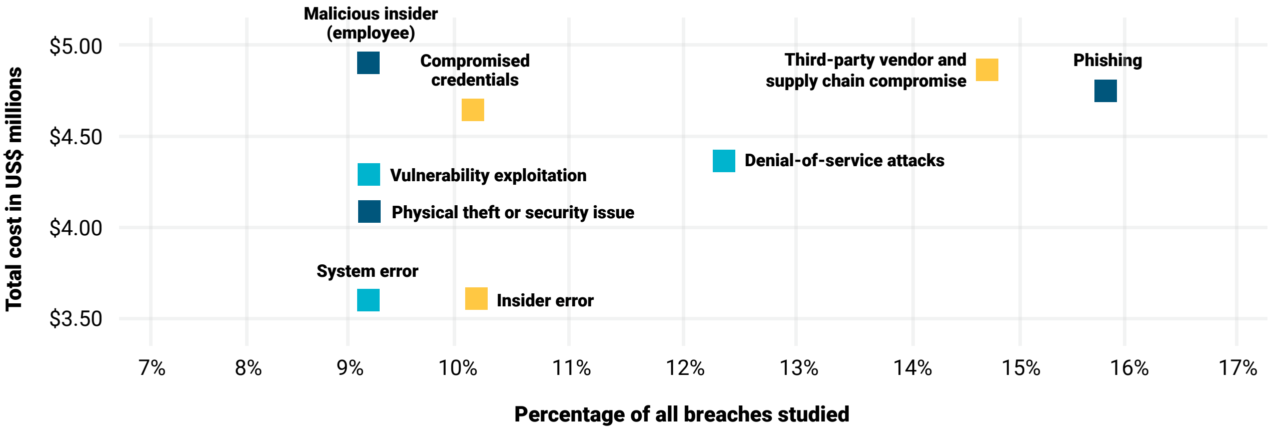
# SOCIAL ENGINEERING ATTACKS: CONSIDERATIONS FOR SMBs

When most people think of someone hacking their business, they picture sophisticated cybercriminals infiltrating the network, breaking password protocols, and penetrating the firewall. Although that can happen, social engineering continues to drive cyberattacks, from high-profile data breaches at the largest corporations to ransomware and other attacks that many small and middle-market businesses (SMBs) fall victim to each year.

This kind of cyberattack doesn't take a lot of money or sophisticated equipment to carry out, but the result can be quite costly for businesses. In 2025, some of the most expensive data breaches were attacks that were initiated through phishing. According to the IBM Cost of Data Breach Report 2025, phishing was the most common initial attack vector, at 16% of the breaches studied, resulting in an average breach of $4.8 million. For many attacks, phishing and other forms of social engineering are the start. When end users fall for social engineering attacks, they often divulge login credentials allowing bad actors to gain access to systems to steal sensitive information or deploy other attacks, such as ransomware.

## GLOBAL AVERAGE COST AND FREQUENCY OF MALICIOUS DATA BREACHES BY ROOT CAUSE VECTOR

**(IBM Cost of Data Breach Report 2025, Figure 9)**



**Cybercrime isn't going away — and the tactics used continue to evolve — but you can mitigate the risks of social engineering with effective training, testing, and tools.**

## COMMON SOCIAL ENGINEERING ATTACK VECTORS

Hackers can access a company's sensitive information through a variety of social engineering techniques: faking the identity of an authorized user, guessing login credentials by mining social media profiles, or even boldly walking into the office and sitting down at an unsecured workstation. The three most common methods of trying a social engineering attack on an SMB are:

1. **Email —** Many businesses work hard to train staff to watch for potentially fraudulent emails, but it's still an extremely successful attack vector — partly because it's so easy to make an email appear to be coming from someone other than the true sender.
2. **Telephone —** Phone calls are another common tactic. The calPhone calls are another common tactic. The caller pretends to have a legitimate request for access to systems or information, and if the recipient complies, cybercriminals can gain the data they seek.
3. **Physical access —** Hackers might pretend to belong somewhere, such as a bank, an office, or a restricted-access area like a server room. If it works, they can get into the network using their own equipment or through an unattended workstation (even easier, since it's probably already logged in). Once in, they're free to steal, delete, or corrupt data as they like, or to install viruses and malware that infect the system.

These tactics are tried and true; however, bad actors continue to evolve their techniques. Just as organizations have adopted AI and automation to enhance their defenses, the hackers have adopted AI to enhance their social engineering strategies.

Take Arup, a British design and engineering firm, as an example. An employee in Arup's finance division joined a virtual meeting with other staff members, including the chief financial officer, who ultimately authorized transactions totaling over $25 million. The catch: Everyone in that virtual meeting — except the finance worker — was a deepfake. The bad actors started their attack with a phishing email, inviting the employee to this virtual meeting, and then utilized AI to dupe the individual into sending fraudulent transactions.

This story reminds us we have to remain on our toes. We are in an age when many things may not be as they appear and traditional verification techniques may not work as they once did.

## WHY DOES SOCIAL ENGINEERING WORK?

Psychology is key to a successful social engineering attack. People don't want to get in trouble, and they are curious by nature. And in certain industries — such as nonprofit, healthcare, and financial services — organizational culture encourages employees to be helpful. By exploiting these basic human traits, hackers can bypass even the most sophisticated and carefully planned security systems.

For example, a bad actor posing as an IT auditor with an urgent request to test the safety of employee passwords is often successful; nobody wants to be the person who quibbles about protocol, holding up important work that makes the whole company safer. Similarly, an email attachment claiming to offer tantalizing information — the salaries of everyone at the company, perhaps — is nearly irresistible. If the document carries malicious content like a virus or ransomware, just one click can put the entire network at risk.

## PREVENTION STARTS WITH TRAINING AND TESTING

Individual behavior is what lets hackers in or keeps them out, so when it comes to thwarting social engineering attacks, training and testing are the two most effective prevention strategies.

Social engineering **training** should focus on educating frontline workers on:

- How to recognize when something is out of the ordinary
- How (and when) to report it
- How to respond

Every business should have a written policy detailing protocols for verifying the identity of callers, email senders, and in-person visitors. For example, if an email contains any red flags at all, recipients should know to contact the IT department using a familiar number or help desk email address — not via a number or link included in the email — to verify that it's legit (and do this before clicking on links, downloading attachments, or responding to the email).

And don't only focus on email. Organizations should have protocols for verifying and responding to requests via any medium. Phone-based scams continue to increase. Remember the attack on MGM Resorts back in 2023? That attack started with a phone call. Members of the hacking group Scattered Spider contacted the company's help desk, impersonating an employee of MGM Resorts. Through the conversation, they were able to get the help desk personnel to provide access to the impersonated employee's valid login credentials. From there, the hackers were able to further their attack.

It's also critical that the training includes simulations and practice sessions. After all, it's one thing to understand the policy in theory, and quite another to react appropriately when it's happening. The goal is to impart a healthy skepticism in all members of the organization, so that they become comfortable and confident following established procedures in real-world scenarios.

Frequent social engineering **testing** is another imperative. This allows the company to identify vulnerabilities, whether that's a particular attack vector (e.g., email requests or a sensitive location that needs more security) or specific individuals who need more training. Those who fail a test need to know that they failed and receive retraining and coaching, until it becomes automatic to follow established procedures before taking any action that could open the door for hackers.

In addition to training and testing, businesses can adopt **technology** to help stop social engineering attacks. Companies that run their own mail server should implement some type of third-party protection tool that can scan incoming mail for viruses and malware. Some businesses go so far as to forbid attachments completely unless they go through a secure method of transfer, such as a file share platform that ensures the validity of each attachment. And for physical threats, camera systems can send an alert to those responsible for information security when someone enters an area with servers or other sensitive equipment.

## THE FIRST AND LAST LINE OF CYBERSECURITY DEFENSE

Tools like these can reduce risk, but don't make the mistake of thinking they'll provide adequate protection or make up for human error. Cybersecurity experts like to say that in social engineering, your people are your first and last line of defense. Training and testing (and retraining, if necessary) really are the keys to preventing a successful social engineering attack.

# CYBERSECURITY TRAINING: WHO, WHAT, WHEN, WHERE, AND WHY

## WHO

- Include all stakeholders, and keep in mind leadership involvement is key. Every member of your leadership team should attend the training, sit in the front row, and actively participate.
- Select the trainers carefully. A member of your IT team is not necessarily the best choice to lead cybersecurity training. IT personnel are often too busy working on the daily issues that crop up to focus on current threats and developments. They also might use "tech speak" that won't be easily understood by the audience. Choose someone who understands the cyber risks and issues and has strong teaching and presenting skills.

## WHAT

- Keep the training simple and direct. Use clear language.
- Ensure attendees understand the important role they all play in protecting your organization. Stress that just one click can infect your whole system, and illustrate the point with real-life examples of breaches caused by an unsuspecting employee.
- Expect limited cyber vocabulary. Be sure to explain terms such as phishing, vulnerabilities, malware, and ransomware.
- Make sure attendees understand:
    - The importance of using strong passwords, not sharing them, and using different passwords for different accounts
    - Why they shouldn't use email to exchange confidential or secure information

    - The dangers of visiting unsafe websites
    - The risks of using public Wi-Fi networks

- Discuss new threats, how they could affect your organization, and what to watch for.
- Provide real-world examples of cyberattacks and breaches.
- Consider conducting a phishing test beforehand, sharing the results during the training, and retesting a few weeks later

### WHEN

- New threats emerge continually, so it's important to hold training often, perhaps quarterly. Consider augmenting this by sharing quick tips monthly.
- Document attendance to make sure all employees receive training. Have an option for those who have to miss the session, such as a repeat date or recording.
- Make sure new employees receive cybersecurity training as part of the onboarding process, perhaps through a face-to-face meeting with your information security officer.

### WHERE

- In-person training tends to be more effective at limiting phishing risks.
- A webinar can be a good option if attendees are in multiple locations or timing is a challenge.

### WHY

- We're all overloaded with too many emails, texts, and more. This can make it hard to spot warning signs or suspicious activity.
- Even with the best controls in place, humans are susceptible to phishing, social engineering, and other threats.
- New threats emerge constantly. Ongoing cybersecurity training is vital to keeping all your network users apprised of current threats.

# HOW TO REINFORCE A CYBERSECURITY EMPLOYEE CULTURE

As phishing and other social engineering scams become more commonplace and sophisticated, the human factor is often the weakest brick in the walls of a company's information security. Yet many companies' security strategies focus more on network firewalls and other technical controls than on awareness and education.

A layered strategy that includes firewalls, antivirus software, and encryption is all for naught if an employee clicks on a phishing link that gives a hacker the keys to the vault: unrestricted access to the corporate network.

The good news is that cybersecurity is more accessible than you think. The most important step you can take to strengthen your cybersecurity posture is to equip your people with the skills they need to prevent, detect, and respond to cyber breaches.

## STRENGTHEN THE HUMAN FIREWALL

Arming your employees to protect your information systems doesn't have to be overwhelming, but it does require a focused effort. So what can business owners and executives do to instill a culture where everyone acts as a responsible steward of personal private data?

**Establish an appropriate tone at the top.** YYou set the tone for the rest of the organization. Make it clear that being a good steward of personal data is just as important as being a good steward of someone's money or other valuables.

**Name a cybersecurity champion.** This should be someone who can dedicate a significant portion of his or her time to making sure the organization is prepared to prevent, detect, and respond to cyberattacks.

**Make training mandatory.** Requiring cybersecurity training for all employees sends the message that this is important to the organization. And that means dedicating the necessary resources to make it effective. Schedule these training sessions during business hours. By paying your employees for their time, you are showing that you consider data security worthy of that capital investment. Also understand that all eyes are on you as a leader. When the rest of the organization sees you participating, they are more likely to embrace the lessons.

**Encourage healthy skepticism.** YYour training should drive home the importance of usng good judgment before taking any action online. Anyone who receives an urgent email directing them to review an attached payroll plan, for example, should think about whether it makes sense in the context of what they've been discussing with that sender. Does the message sound like something the person would have sent? If there are any doubts, then employees need to know to pick up the phone or walk down the hall and talk to that person before clicking or downloading anything.

**Prepare participants to respond quickly.** The initial incident response is critical when it comes to mitigating the effects of a breach. Those early steps can dictate how far the breach goes, how much of the network it affects, and how big the reputational damage will be. You want your training participants to be able to anticipate the types of attacks that are likely for your industry and be prepared to take immediate action. A cybersecurity risk assessment can help you determine the types of attacks for which your business is at highest risk. At a minimum, your employees should learn to recognize phishing emails that could launch ransomware and other forms of malware, as well as other forms of social engineering.

**Use real-world scenarios.** Realistic scenarios are the best way to keep your users engaged. Most important, give participants a chance to practice what to do if they suspect a breach. For example, how many of your employees know how to go about disconnecting from the network?

**Clearly outline breach reporting responsibilities.** Make sure employees understand how to report a breach. In addition to reporting the breach internally, your organization might be subject to specific breach notification laws. In that case, you will need a well-defined notification process.

**Test your participants.** Testing is an essential part of any type of education. Incorporate testing throughout training sessions to assess progress and keep learners engaged. These can be informal and inserted into the conversation. For example: “You receive an email from the CEO ordering you to make a wire transfer by the end of the day. What do you do?” In addition, competency-based testing after each training session allows you to assess the learners’ levels of retention and understand just how effective the training has been.

**Evaluate your training.** Evaluate and update your cybersecurity training program often. Just like your participants need testing, your training needs testing. Are the examples and models in your training program informative, and do they provide enough realistic experience for users? Are you using actual hardware and software that is likely to be affected by cyberattacks?

### GIVE YOUR EMPLOYEES SOME BACKUP WITH LAYERED SECURITY

Cybersecurity training is crucial, and it can go a long way toward protecting your business. But we’re all human, and we all make mistakes. Most likely, sooner or later, an employee will unintentionally open you up to a vulnerability.

What happens then? The outcome depends on what else is protecting you. Linus Pauling, the Nobel Prize-winning scientist, once observed that the best way to have a good idea is to have a lot of ideas. Likewise, the best way to have good security is to have a lot of security.

That doesn’t mean haphazardly throwing together every idea you can think of; it means having layers of security. Any single safeguard can fail, but the more safeguards you have, the more likely it is that at least one will succeed.

### CREATE A CULTURE OF VIGILANCE

Business leaders must not only take seriously their responsibility to protect the data entrusted to them, but they should strive to instill that sense of personal responsibility throughout the entire organization. Making the necessary investments of time and money to create a culture of cybersecurity vigilance can avert a far more costly data breach.

## DEVELOP A STRATEGY TO MANAGE YOUR IT ASSETS

Creating an inventory of all your organization’s information technology and systems and a plan to manage them is vital. After all, you can’t protect all your systems if you don’t know exactly what needs to be protected.

### SETTING YOUR STRATEGY

Like learning chess, IT asset management can seem like a mountainous task, but strategic planning will make the task manageable and save you headaches and sleepless nights. The first step in playing chess is to understand each piece, and managing your IT assets is no different. You need to understand what “pieces” are to be managed within your organization by including them in the inventory.

**So, what exactly are IT assets?**

- Your **physical hardware** inventory should include hardware such as servers, workstations, laptops, mobile devices, firewalls, intrusion detection switches, routers, switches, printers, copiers, fax machines, and Internet of Things devices (e.g., Apple TVs, Amazon Echo, and other smart devices). Include critical details about each asset, such as location and warranty information.

- Your **software and application** inventory should similarly identify all software installed on systems and applications that employees access, including those with web-based logins. This inventory should include details such as the version in use, system administrator, web address, license period, and number of licenses.
- Your **data inventory** should identify and classify the types of data stored. For example, public information that is available on your website is different from proprietary details about your organization or sensitive information about your constituents. Before you can secure this data, you must inventory it to know what it is, where it is stored, and how it is accessed. With the continued scrutiny surrounding data protection, including regulations like the General Data Protection Regulation and the Colorado Data Privacy Act, this data inventory can be particularly useful for seeing where potential data trails might be within your systems.

# APPLICATION AND SOFTWARE INVENTORY: HOW DOES IT WORK?

It's imperative to have a handle on all the software and applications your employees access. Here are three steps to help you create and manage an effective application and software inventory system to maintain a secure environment.

## Step 1: Determine What Is in Use

What systems are employees logging into daily? This should include not only software and applications installed locally on workstations and servers but also any web-based applications employees can access. Determining what is being used and what exists in your environment is one of the most difficult steps in the inventory process. To do this:

- **Poll the departments within your organization.** Ask them what they are using, what they use it for, and who should have access to it.
- **Review web activity reports or employees' browsing histories.** This will help you determine which sites your employees are actually accessing. Compare this information to your poll results. You may be surprised at how many more systems you find!
- **Determine the applications installed on servers and workstations.** There are automated tools that can report on all software installed on systems at a point in time. If you don't have one of these solutions, you can manually review devices to see what is installed.

## Step 2: Document, Document, Document

Everything you uncover above should be documented within your inventory system, which can be as simple as a spreadsheet or database. This inventory should include details that would be helpful to your organization, such as the application or system name, vendor information, license period, system administrator or owner, type of data stored, website address, and application controls configured. These details are critical for ongoing management.

If any concerning software, applications, or exceptions are noted during the evaluation process, be sure to document them. Exceptions could include software you didn't know staff members were using or an application that is outdated or obsolete but still used for a specific reason, such as a vendor requirement. Any exceptions should be approved by the appropriate level of management.

### Step 3: Ongoing Management

Once you've addressed the big but vital task of creating your application and software inventory, it's time to address processes and controls to help with ongoing management. This is generally much easier than creating the inventory, especially if you have automated tools.

Ongoing management typically involves the following steps:

- **Restrict administrative access rights on local systems.** By limiting local administrative access, you reduce the risk that end users could install applications on their workstations or laptops.
- **Configure web filters.** A web filter can be configured to restrict unauthorized sites by blocking specific websites or site categories (e.g., gaming, social networking) or to allow only authorized websites.
- **Review web filter activity reports.** As noted before, this can alert you to sites that employees are accessing, ensuring that you are aware of all the applications they may be using.
- **Review for extraneous or obsolete software and applications.** Note that without an automated inventorying tool, this task becomes much more cumbersome and is often less efficient and effective.
- **Revisit exceptions.** Exceptions should be reapproved at least annually.

By identifying and properly managing the software and applications in use, you can implement layered controls and processes to better secure your environment.

# THIS IS NOT A TEST: INCIDENT RESPONSE AND RECOVERY

In the game of cybersecurity, betting the farm on an ironclad perimeter defense is a losing strategy.

Many "first identifiers" of cybersecurity incidents are unsure of what to do when they see a suspicious message or alert. Unfortunately, in those first critical moments, the incident can grow from a minor inconvenience into a major catastrophe.

Appropriate incident response and recovery procedures are essential components of a comprehensive information security program. They can also mitigate the effects of an attack and reduce the likelihood of future breaches.

An incident response and recovery plan should spell out how the organization will:

### 1. Contain the threat.

In the event of a suspected breach, the first objective is to limit the impact. Each person who might discover a cybersecurity incident must know the important steps that will keep that attack from propagating throughout the network. Just as vital, those actions must preserve any forensic evidence. For example, if an employee encounters an infected machine, then in most cases, the device should be disconnected from the internet and the network without powering it down (and employees must know how to disconnect). The employee should then immediately call IT support or the company's designated security officer.

### 2. Respond.

The proper incident response depends on the type of attack vector and the risk rating of the digital assets at stake. In our previous example of an infected machine, disconnecting the device is an appropriate response because the files it contains could be high-value digital assets. Additionally, this response is appropriate because the attack occurred on a single machine. By contrast, a network-level attack — such as a distributed denial of service attack, which makes a network unavailable to its users — requires more response planning. Such planning includes implementing monitoring tools and conducting scenario-based testing to equip security personnel to make response decisions quickly.

At a minimum, anyone who could detect a cybersecurity attack must know how to complete an incident report. Employees should also know their responsibility to notify management, the board, customers, and regulators.

### 3. Recover.

Business must continue after a cybersecurity attack. A recovery plan focuses on returning to normal operations as quickly as possible and reducing the likelihood of another such event. Store a copy of the incident response and recovery plan in a location outside the local network to ensure that you can access it — and keep it secure from cyberattackers.

Recovery plans should include ongoing monitoring procedures to verify that the issue is fully resolved, and they should integrate any lessons that may help prevent similar circumstances in the future.

Additionally, a recovery plan should include a post-breach analysis and meeting. The analysis should address additional mitigation strategies required to stop or prevent an attack. The purpose of the meeting, which should be conducted within 24 to 48 hours of the attack, is to debrief the security team and company stakeholders while conducting a risk assessment to gauge the likelihood of a future attack.

Of course, it is not enough to simply have a recovery plan in place. Organizations should also conduct scenario-based testing to help ensure that their planned strategies will work against an attack.

## STORE SENSITIVE DATA SECURELY IN THE CLOUD

Advances in technology have allowed small businesses to become more efficient — and more profitable — by keeping data in the cloud. Whether you're running resource-intensive applications or simply storing files for internal use, cloud-based systems can make accessing and backing up critical business information easier and more secure.
That said, it's a mistake to assume cloud storage automatically ensures robust security for highly sensitive data.

Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform — known as the Big 3 — dominate the cloud services landscape for small businesses, but they're far from the only games in town. In many cases, businesses are using multiple types of cloud storage services.

Cloud storage offers ample benefits that are appealing to small businesses. It saves money by eliminating the expense of running and monitoring in-house servers. It's infinitely scalable — your business will never outgrow the cloud's capacity — and can boost resilience too, keeping your data out of harm's way when fires, floods, or criminal acts damage offices and equipment. Plus, with your data stored in the cloud instead of a local computer, teams can collaborate easily and work from anywhere they have internet access.

Another important benefit is the potential to achieve significant security upgrades over local storage, with secure data centers and advanced features to help you keep bad actors away from sensitive data.

However, simply putting data in the cloud isn't a guarantee of safety; security in the cloud hinges on implementing and adhering to the latest strategies for cloud-enabled systems and environments.

AWS features server-side encryption with customer-provided keys (SSE-C). It means that the provider doesn't store or have access to the encryption keys, which helps keep unauthorized users from accessing stored data. But SSE-C and similar security features are still vulnerable to cybercriminals, and hackers have learned how to use these legitimate encryption mechanisms to execute cloud-native ransomware attacks.

An approach to security called Zero Trust offers businesses a powerful way to reduce risk by eliminating the old "trust but verify" mindset. Instead, every user, device, and application must continuously prove it has the right to access specific resources, which helps block attackers even if they manage to steal a password or breach the network perimeter. By enforcing least-privilege access, segmenting systems, and monitoring activity in real time, Zero Trust limits the damage a single compromise can cause while improving visibility and control across cloud environments.

## CLOUD SECURITY STRATEGIES

Cloud service providers have varying cloud architectures and different security features — everything from single sign-on and multi-factor authentication to AI-driven pattern analysis and advanced threat detection technologies. Learning how to lock down these environments is a significant undertaking, since each service will require a unique approach and set of security methods.

Make sure your IT teams recognize the responsibility to secure cloud data and have the resources to delve into appropriate security tactics for each cloud provider your business uses. But some best practices, like strong encryption, are more universal. These platform-independent strategies can help you manage cloud-based cyber risks.

**Identity and access management (IAM):** Closely manage digital identities using your provider's IAM features to fine-tune and monitor user access to organizational resources.

**Data classification:** Sort data into categories based on level of sensitivity. This can help make your IAM efforts more effective.

**Configuration and APIs:** Keep hackers at bay by confirming proper configuration of your cloud services and verifying that all application programming interfaces (APIs) are secure.

**Life cycle policies:** Establish clear protocols to securely govern the full life cycle of all data your business collects and creates, including inception, retention, use, and disposal.

**Monitoring and auditing:** Continuously monitor and log data access and use, auditing access logs frequently so you can detect and quickly respond to any suspicious activities.

**Automation:** Automate regular data backups and recovery processes for extra confidence that your business has continuous data protection.

**Regulatory compliance:** Maintain awareness of the latest best practices and security compliance requirements to help you understand and manage emerging threats.

**Threat assessments:** Detect new risks and unaddressed vulnerabilities with regular cloud threat reports.

**Training and awareness:** Provide regular training and review sessions to ensure team-wide understanding and compliance with your organization's data security and life cycle policies.

**Cloud-native defense tools:** AWS GuardDuty, Azure Security Center, and Google Security Command Center are offerings from cloud providers that can enhance the ability to monitor security events.

# MAINTAIN SECURITY IN A REMOTE WORK ENVIRONMENT

Giving your user base the ability to work remotely creates additional challenges as your network becomes decentralized. With strategic planning, however, you can create a remote working environment that supports your organization while maintaining the security of your systems and data. Here are six steps to follow.

### 1. Identify the need and extent of access.

You cannot manage what you cannot measure, so start by defining the who, what, and how of your remote working environment.

- Who needs to be working remotely? Is it the entire user base or a select group?
- What are they accessing? Are they accessing internal network resources, cloud-based applications, or internal and client data?
- How are they accessing it? Are they accessing internal resources via virtual private network (VPN) or cloud-based solutions? Are workers using personal devices, or are all devices owned by the organization? Are they using laptops, workstations, mobile devices, or a combination of these?

The answers to these questions determine what controls you implement and how you manage them. For example, if only a handful of users require access, manual controls and acceptable use policies may be sufficient. If more individuals require remote access, additional management and centralization of controls may be warranted.

### 2. Define acceptable use policies for the identified resources.

Policies and procedures related to how remote workers access your data must be defined. If personal devices can access your business resources, then some procedures addressing that risk should also be incorporated into policies. It's imperative to define these areas:

- Who owns the devices, the data accessed and created, and the installed applications?
- What responsibilities do remote workers have? Consider password, anti-malware, patching, encryption, and physical security requirements.
- What restrictions are in place for data storage and device synchronization? Many devices back up automatically. If an employee uses a personal computer for work purposes, business data may inadvertently be included in personal backups.
- What are the procedures if a device is lost or stolen? Can the data be wiped remotely? Do employees know who to notify and the timeframe for notification?
- What are the procedures to ensure data is removed properly from a device if an employee leaves or if a device is sold, sent for repair by a third party, transferred to another individual, or discarded?

## 3. Configure controls to support your policies.

Many remote workers use remote access and cloud-based applications. Using your inventory of applications, first ensure that each system is properly secured. Enable strong password parameters and conservative lockout settings, and configure multi-factor authentication for all remote access and high-risk, externally accessible applications. This is a non-negotiable control!

Don't forget about controls that are specific to various types of applications. For example, enterprise versions of virtual meeting applications often have enhanced controls over the free versions, including end-to-end encryption, unique meeting IDs, and other controls to prevent unauthorized users from joining the conference. Similarly, data storage applications often have capabilities to prevent your data from being accessed or stored in locations you don't manage and control. For example, in Microsoft 365, you can restrict sharing with external parties that are not within your organization, and you can enable configurations to reduce the risk that confidential information is emailed without being properly secured.

Next, set retention periods to limit the impact if data or systems are compromised. With the nature of remote work, large amounts of data are often stored in the cloud for ease of access. However, is all this data truly needed? Consider this question when evaluating the potential impact if any of these systems are compromised. Establish a retention period for data and a process for deleting or removing it when it is no longer needed.

Finally, secure any devices that will access the resources. Remote workers and the devices they use become an extension of your network. Even if the devices are employee-owned, you now are responsible for securing them to protect the data and systems they access.

**Centralize and enforce these controls:**

- Install anti-malware protection on all devices and ensure the definition files are updated regularly.
- Apply patches and updates to operating systems and applications.
- Enforce password-protected screen savers and inactivity timeouts to protect users when they walk away from the device.
- Configure encryption to protect any data stored locally on the device.
- Enable the ability to remotely wipe a lost or stolen device.

If existing management systems cannot support remote devices, you may need a more robust mobile device management solution. These solutions often provide enhanced controls for data storage and syncing.

## 4. Consider evolving risks associated with technology in home office environments.

Home office environments introduce unmanaged technology. Home office networks typically don't just have a laptop connected, and network resources are shared with other family computers, printers, scanners, and Internet of Things (IoT) devices (e.g., smart TVs, thermostats, refrigerators, and alarms). If not properly secured or segmented, these other home office devices could affect the laptop or computer that employees use to access your business resources.

In addition, many of these smart devices listen for commands (e.g., "Hey Alexa!"). To do this, these devices are "always on," which means they are always listening and sending the data to various data centers for processing. Therefore, if an employee regularly has sensitive, work-related conversations with a smart listening device nearby, it's likely that these conversations are being recorded and stored.

It's imperative that your employees understand these risks and acknowledge relevant procedures within acceptable policies. Consider the following as recommended practices for home offices:

- Create a guest network to segment work-related traffic from guest and family member activity, if possible. Connecting all non-business systems to this guest network and properly segmenting them from your business resources is one of the most critical controls.
- Configure a complex password with strong encryption on the wireless network. If feasible, enable multi-factor authentication on the management console.

- Establish procedures for ensuring updates to all home office devices that connect to the same network used for accessing work resources. This includes other computers and laptops, smartphones, tablets, smartwatches, wireless routers, printers, scanners, smart TVs, and other IoT devices.
- Consider the ability to run vulnerability scans on home office networks. If your organization has a tool to test vulnerabilities, evaluate the feasibility of extending this use to home office networks. Depending on the number of remote workers, this may not be feasible.
- Install anti-malware protection on relevant systems on the home office network, and configure the software for full system scanning. This could include workstations, laptops, and smartphones.

## 5. Train your user base.

Once employees are remote, the way you manage controls changes, and the layers you have at your physical office may no longer apply. Ultimately, the key to creating a secure remote work environment lies in empowering end users to make smart choices, and true security exists only when users have both the tools and the knowledge they need. Make your employees aware of the risks associated with remote work. Talk to them about current threats, the risks of using public Wi-Fi, and the heightened threat of malware when using computers for both business and personal use.

## 6. Prepare for the incident.

Many organizations have incident response plans for identifying, containing, and mitigating incidents in their physical office environments. When you implement remote working environments, these remote home offices become an extension of your network. Do your incident response plans extend to incidents occurring in these remote offices? And do your remote workers know how to identify, contain, and escalate an issue in their remote environments so that it doesn't impact your data or other users?

Establishing — and clearly communicating — incident response procedures before employees begin working from home is imperative. For example, in the event of malware infection, workers should also know how to disconnect completely from the internet. Similarly, does the end user even know what is potentially suspicious activity in the first place — unexpected restarts of their computer, unexpected promptings for their user ID and password, or numerous popups? And if they do suspect suspicious activity, who do they call?

Policies and procedures should also cover incidents related to physical security. What if the physical security of their device is compromised — what should they do, and who should they notify?

**In addition to providing written guidelines, leaders should:**

- Test remote workers to verify that they know what to do following any type of security incident.
- Provide ongoing training and testing to make sure knowledge of policies and procedures is complete and current.
- Define the steps for supervisors and managers to follow if they receive an incident report. This could include an in-person meeting at the office, depending on the severity of the incident.

# CYBERSECURITY TIPS FOR WORKING FROM HOME

- Select a work site that offers adequate privacy (i.e., not the local Starbucks).
- Don't let others (including curious kiddos) use your work laptop.
- Keep it locked with your password when you are not using it.
- Update your wireless access point to the latest firmware version.
- Consider keeping access to your work laptop separate from all other devices, such as lights and thermostats.
- Increase the complexity of your Wi-Fi Protected Access (WPA) password settings. Use a random password with at least 12 characters, including letters, numbers, and special characters. Steer clear of kids' names, last names, addresses, and pet names.
- Only connect to the office using a VPN.
- Make sure your antivirus is up to date and all your operating system updates are installed.
- Make sure you complete the updates as they come out.
- Limit email to work only.
- Don't install software you haven't been authorized to install by your IT department.
- If you suspect you have an issue, disconnect your laptop and contact your IT department. Do not reconnect it to the internet or VPN until you receive the "all clear" from your IT folks.

# SAFEGUARD YOUR BUSINESS FROM THIRD-PARTY CYBERSECURITY RISKS

Businesses of all shapes and sizes increasingly rely on third-party vendors for a wide range of services. From payroll processing and cloud-based accounting systems to IT support and customer service platforms, these strategic partnerships can streamline operations, reduce costs, and allow internal teams to focus on core business functions. But with that convenience comes increased exposure. Third-party relationships can introduce serious cybersecurity risks that may compromise sensitive client data, disrupt operations, and leave businesses vulnerable to regulatory and reputational fallout.

As cybersecurity threats tied to third-party service providers grow more complex and far-reaching, federal and state regulatory bodies have responded with heightened scrutiny, proposing new rules and updates to improve oversight, accountability, and data protection across the vendor landscape.

## UNDERSTANDING THIRD-PARTY CYBERSECURITY RISKS

Third-party vendors often have broad — and, at times, unrestricted — access to sensitive information, including client financial records and proprietary data. With that level of access comes a critical responsibility to uphold strong cybersecurity standards and safeguard the trust placed in them. Vendors lacking adequate cybersecurity measures can become vulnerable entry points for cybercriminals. A single breach can expose your business to regulatory penalties, legal liabilities, and lasting reputational harm.

## EVALUATING AI RISK WITHIN THIRD-PARTY RELATIONSHIPS

The use of AI by third-party service providers is another emerging risk area. Businesses should evaluate whether their vendors are leveraging AI to deliver services — and whether that use puts company data at risk of exposure or misuse.

Some providers may incorporate client data into proprietary large language models or rely on third-party tools like ChatGPT, increasing the risk of data loss, unauthorized access, or policy violations. While AI can offer valuable efficiencies, its use within your vendor network should be carefully assessed as part of your broader supply chain risk strategy.

## EFFECTIVE PRACTICES FOR MANAGING THIRD-PARTY CYBERSECURITY RISKS

While the risks are real, there are practical steps you can take to protect your business and hold vendors to a higher security standard. Taking a proactive and intentional approach to managing third-party relationships can reduce exposure, maintain compliance, and reinforce trust with your clients.

**Consider implementing the following practices to help you manage third-party cybersecurity risks effectively:**

1. Conduct Thorough Due Diligence: Before engaging with a vendor, assess their cybersecurity policies, protocols, and compliance with relevant regulations.

2. Implement Continuous Monitoring: Regularly monitor and audit vendor activities to promptly detect and address potential vulnerabilities. Continuous oversight helps ensure that vendors maintain the security standards required to protect your firm’s data.

3. Establish Clear Contractual Agreements: Define security expectations, responsibilities, and incident response procedures within vendor contracts. Confirm that vendors are obligated to notify your firm promptly in the event of a cybersecurity incident.

4. Limit Data Access: Grant vendors access to only the data necessary for them to perform their functions. Implement strict access controls and regularly review permissions to minimize exposure.

5. Utilize System and Organization Controls (SOC) Reports: Request SOC reports from vendors to gain insights into their control environments and identify potential risks within the supply chain. SOC 2 reports, in particular, assess controls related to security, availability, confidentiality, processing integrity, and privacy.

6. Provide Regular Security Training: Educate your employees about the risks associated with third-party vendors and the importance of adhering to security protocols when interacting with them.

## THE GROWING RISK OF SUPPLY CHAIN ATTACKS

Another growing concern is the rise in supply chain attacks, which are cyberattacks that target a business indirectly by infiltrating less secure elements within its network of vendors, suppliers, or service providers. Instead of attacking a company head-on, cybercriminals exploit vulnerabilities in third-party systems to gain access to the primary organization's data and infrastructure. These attacks are particularly dangerous because they often go unnoticed until significant damage has already been done. In many cases, the impact isn't limited to a single organization — it can cascade across the supply chain, affecting multiple businesses at once, making it crucial to assess the security of every third-party relationship you maintain.

As organizations outsource more, the complexity of their environments expands. The IBM Cost of a Data Breach Report 2025 found that approximately 15% of the breaches studied originated from a supply chain or third-party vendor compromise. In addition to being the second most frequent type of attack, it was also the second costliest, at $4.91 million per breach.

It's no wonder supply chain risk continues to garner attention. Notable supply chain attacks over the last several years included the December 2020 SolarWinds attack, the May 2023 zero-day vulnerability that was identified in Progress Software's MOVEit platform, and the December 2024 cyberattack through a software vendor that targeted the Office of Foreign Assets Control department of the U.S. Treasury.

Organizations rely on third parties to provide security and redundancy capabilities that the organizations cannot implement themselves. Large service providers often have the resources and ability to scale their operations so they — in theory — can provide better controls than we could implement in our own organizations. For example, a vendor providing you an application may host that application in a hardened data center with the most robust, up-to-date security measures — controls that you may not be able to apply in your onsite server room. However, you then rely on that vendor to do what they advertise: to keep your system secured, updated, and backed up regularly. Failure of this service provider impacts you — a perfect example of supply chain risk.

Another particularly disturbing statistic is the increased time it often takes to identify and contain breaches that originate via the supply chain. The IBM Cost of a Data Breach Report 2025 found that supply chain breaches took the longest to identify and contain, at a whopping 267 days. And that extended timeline increases the cost and impact to the affected organizations.

## ASSESSING SUPPLY CHAIN RISK

The growing prevalence of supply chain attacks — and the fact that they are so difficult to detect — means that every business must take this risk seriously. The more third parties have access to your data and systems, the greater the risks to the confidentiality and integrity of that valuable data and the availability of your systems.

**The Cybersecurity and Infrastructure Security Agency warns that organizations are especially vulnerable to software supply chain attacks for two reasons:**

- Many third-party software products require elevated system privileges that give them broad access to nearly every system in the network, and many customers accept these defaults without question.
- Third-party software often requires regular connectivity between the vendor's network

and the customer's network, for the legitimate purposes of providing updates and patches. This open door could enable the insertion of malicious software (as in the SolarWinds example) or even the prevention of an update, which makes customers vulnerable to further attacks.

When a threat actor compromises a software vendor, they bypass the customer's perimeter security (e.g., border routers, firewalls), and they can continue their criminal pursuits within your network for as long as they have access to the compromised vendor.

## SUPPLY CHAIN RISK VS. VENDOR RISK

Supply chain risk management differs from vendor risk management. Vendor risk management focuses mainly on whether the vendor is financially stable and doing what they are supposed to be doing, but supply chain risk management addresses the potential impact to your internal assets as a result of the security practices of those third parties.

**Some key questions to ask as part of supply chain risk management include:**

- Does the vendor have direct control over your internal assets?
- What is your level of risk if the vendor is breached?
- What controls are in place to mitigate these risks?
- How does the vendor stay current on emerging vulnerabilities?

## TIGHTEN YOUR SUPPLY CHAIN

The increasingly complex network of software and hardware vendors on which most businesses rely means supply chain attacks are likely to continue. Rather than trying to put the genie back in the bottle, companies need to heighten their awareness of the risks involved.

The good news is that with rigorous vendor risk management practices, awareness of evolving regulations, and a strong cybersecurity culture, you can mitigate these risks and maintain the trust of your clients.

# CYBERSECURITY TRENDS TO WATCH

# RANSOMWARE

High-profile ransomware attacks plague large and small businesses alike and continue to demonstrate how vulnerable our supply chains and infrastructure are to cyberattacks. A **June 2021 open letter** from a White House cybersecurity advisor reminded business leaders that no company is safe from being targeted by ransomware. Some of the takeaways from this letter ring true today, including a reminder that "companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively."

## WHAT IS RANSOMWARE?

Ransomware is a form of malware that infects a computer and encrypts files on the computer and network. Once these files are encrypted, the only way to open them again is with a key that only the bad guys possess. The perpetrators will sell you the key to decrypt the files. However, keep in mind that cybercriminals are behind these schemes, so even paying for the key may not guarantee the unlocking or retrieval of your files. And in some cases, the bad guys "double encrypt" the files, which means even if you pay the ransom and receive one encryption key, the files could still be encrypted.

Just as with other attack mechanisms, ransomware tactics have evolved. Not only do we see the encryption of data, but for many victims, the data is stolen before it is encrypted. The bad actors can then extort the victim not once, but twice. Not only will the bad actor demand money to decrypt the data, but the hacker will also demand payment to not release the information on the dark web. And sometimes, the attackers take this a step further and will contact your partners, your board, your customers, and other constituents to demand additional smaller payments in order to not expose the information.

And finally, some bad actors go the "encryptionless" ransomware route: Once the malware captures the data, the attackers don't bother encrypting it but simply demand a ransom in order to not expose the data on the dark web. This can be just as lucrative as an encryption ransom. This technique is becoming so popular that Sophos found in their **2025 State of Ransomware** report that only 50% of ransomware attacks in 2025 involved data encryption — down from 70% in the previous year.

The FBI discourages ransomware targets from paying ransoms — and in the vast majority of cases, paying up doesn't pay off. While many information security professionals indicate they do not believe their organization would pay the ransom if it was hit by a ransomware attack, people continue to pay. Sophos found that 49% of those organizations attacked paid the ransom to get the data back. And in cases where safety and public interest is at play, ransomware victims often feel that paying is the only option. Colonial Pipeline's CEO **reported** that he felt compelled to pay a $4.4 million ransom because getting the pipeline flowing again "was the right thing to do for the country."

## RANSOMWARE IN THE CLOUD

As ransomware attacks become more and more common, it's important to understand what you can do to keep your data secure in the cloud — including what you're responsible for versus security measures that your cloud provider will take on your behalf.

Personal cloud storage services like iCloud, Dropbox, and Google Drive enable object versioning by default, making it easy to recover files that are lost or damaged. That's not necessarily the case with the Big 3 cloud providers that so many small businesses rely on. In fact, AWS, Azure Storage, and Google Cloud Storage do not enable file recovery services by default. If ransomware locks you out of one of these providers' systems, you'll have no way to access the information stored there unless other backups exist.

Be sure you understand the features and controls your cloud data storage provider offers, and learn how to achieve the level of data security you need. Backups, object versioning, and object locking are all features that can help you ensure data integrity and availability.

They come at a cost, though, so you'll need to conduct cost-benefit analysis and decide which features are a wise investment for your business. You'll also want to plan how you'll create backups external to the cloud, with rules specifying which files, how often, and how to safely store these backups.

## WHAT YOU SHOULD DO TO PROTECT AGAINST RANSOMWARE

How do you avoid becoming a victim of a ransomware attack? And if successfully attacked, how can you recover?

- **Educate team members.** In order to protect against an attack, team members need to know how to identify a potential threat and how to prevent it. Ransomware is often spread by malicious links found inside emails. Therefore, educating your team regarding the different scenarios used to distribute those links is the first line of defense. Emphasize not opening attachments or following links from unknown or unverified sources — as well as those that they did not specifically ask to be sent.
- **Install security patches promptly, and keep antivirus software updated.** Many times, the malware containing the ransomware can be thwarted by having the latest security patches and antivirus software updates. Rather than delay or ignore the prompts to make these updates, install them immediately.
- **Have clear policies in place to protect your data from ransomware.** Clear direction regarding email attachments and file downloads (and the users' responsibilities) is essential in combating ransomware.
- **Back up data regularly and keep backups segregated.** Nothing will keep you 100% safe, so you need a plan that will help you roll with the punches if the worst-case scenario occurs. Have a backup solution that will allow recovery back to files from a date prior to the ransomware attack. The appropriate interval is a company-by-company decision, and understanding your data is essential. For example, consider how often critical data is created, and how hard it would be to re-create the data that might be lost in an attack.

# BUSINESS EMAIL COMPROMISE

Every year, businesses lose vast sums to fraudsters who compromise legitimate business email accounts to conduct unauthorized transfers of funds. These scams are known as business email compromise (BEC). The FBI received more than 21,000 complaints about BECs in 2024, and these scams cost businesses an eye-popping $2.77 billion.

One form of BEC is known as executive impersonation fraud, which entails a skilled criminal (or group of criminals) crafting an email that appears to be from one of the key executives within the company or a vendor. The domain of the email address may be identical to the company's domain except for one or two letters (e.g., joe@victimco.com vs. joe@vicitmco.com), or the email address might even be "spoofed" so that it appears legitimate.

The criminals do their homework to make their scheme convincing. They typically scour the company's website and social media accounts to carefully investigate the executive they are impersonating. Additionally, they research their intended target, who will ideally be someone with the authority to initiate or approve wire transfers.

To defend against BEC, it is critical that employees recognize the following warning signs:

- The email appears to be from a senior executive or vendor but comes from an address that differs from the official, company-issued domain.
- The sender conveys urgency or secrecy by asking to communicate only through email (perhaps due to supposed regulatory restrictions).
- Payments are directed to foreign bank accounts, especially where the company has never done business.
- Requests may occur when the key executive or vendor is traveling or unavailable.

## CREATE A ROBUST DEFENSE

BEC relies on employees' willingness to bypass normal financial controls. Companies can dramatically reduce their risks with the following basic precautions.

- **Create a culture of skepticism.** Employees should know that questioning authority — especially in regard to initiating financial transactions — is not only allowed, but strongly encouraged.
- **Build employee awareness of the latest email scams.** In addition to companywide cybersecurity education, all employees who have authority to request, approve, or execute wire transfers should receive regular (ideally, quarterly) training on common social engineering attacks.
- **Implement and enforce a social media policy.** Employees should be careful about what they share on social networking sites, especially details about key executives' travel itineraries.
- **Strengthen controls around wire transfers.** First, restrict authority for initiating or approving financial transactions to a few individuals. Then, design and implement procedures to verify the origin of all wire transfer requests. Many companies require verbal confirmation from someone calling from a company-issued phone number, followed by secondary verification from another individual via another phone call using an authorization code.
- **Document all of these steps. I**n the event that these controls fail and a security breach occurs, your documentation will be invaluable for showing regulators and prosecutors that your company implemented reasonable and appropriate safeguards to mitigate data loss.

# WHALING

In a whaling attack, the goal is bigger than stealing a victim's identity. These cybercriminals are harpooning for control of the executive's personal computer to learn passwords and gain access to critical digital assets and confidential information.

Often the whaling email is related to "official" business, such as a subpoena supposedly being issued against the executive or a complaint filed with the Better Business Bureau. The email often uses icons and language that seem official, and it usually conveys a sense of urgency (e.g., a threat for non-responsiveness). In reality, the attached "subpoena" document or the necessary software download will launch malware (usually a Trojan/keylogger) — or the email includes a hyperlink directing the victim to an infected website.

The email or webpage seems authentic because the cybercriminals take the time to capture not only an email address but also some other key and specific information — often a correct job title, direct phone number, names of other key executives, and sometimes even circumstances particular to that entity. In some cases, the criminals find this information publicly available on an entity's website. In other cases, they buy it on the black market.

The message here is clear: The buck stops with you. As a highly visible leader, you could be the unwitting participant in an attack, and since you set the tone for the rest of the organization, make sure you model the behavior you expect.

# HOW DO YOU KNOW YOUR CYBERSECURITY DEFENSE SYSTEM IS WORKING?

For a homeowner, the knowledge that a trained eye has evaluated the home security system — and attested that it is in good working order — can go a long way toward a good night's sleep.

The same goes for business owners and executives in charge of keeping the company's data and digital assets safe. Many business owners and executives believe that they can manage these risks with technology such as firewalls and antivirus software. But an alarm system that has not been activated is useless, and likewise, defensive technology will not overcome bad controls and human error.

Your stakeholders — boards of directors, customers, employees, investors, business partners, and regulatory bodies — expect you to have processes and controls in place to prevent, detect, and mitigate the effects of cybersecurity events. Increasingly, these stakeholders expect independent third-party reports that attest to the effectiveness of the organization's cybersecurity risk management program.

The American Institute of CPAs (AICPA) has created a robust, industry-agnostic framework intended to provide the market with a standardized approach to evaluating and reporting on a company's cybersecurity risk management program. This consistent reporting approach could potentially streamline compliance requirements that might otherwise distract company resources away from cybersecurity risk management.

## CPAS OFFER A TRAINED EYE TO VERIFY CYBERSECURITY READINESS

Accounting firms draw on a unique combination of skills and characteristics that can prove invaluable when evaluating cybersecurity defense systems:

1. **Integrity.** The CPA profession was built on core values of independence, objectivity, and professional skepticism. As a result, an audit by an independent CPA has become the gold standard when it comes to assessing internal controls over financials. That same auditor's mindset and discipline are invaluable when assessing the strength and security of a cybersecurity risk management program.

2. **Risk management specialists.** CPAs can provide cybersecurity examinations that fulfill the risk management needs of a broad range of stakeholders. Auditors are highly skilled at assessing an organization's risks and internal control effectiveness.

3. **Broad perspective.** In addition to CPAs, many midsized and larger accounting firms today have IT specialists who can help strengthen the entity's cybersecurity defenses. Some of the designations that business owners and executives should look for include Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Information Technology Professional (CITP).

When it comes to cyber threats, no organization is too small or insignificant to be a target. Those organizations that have engaged CPAs and skilled IT professionals to examine their cybersecurity defense systems can sleep soundly with confidence in the effectiveness of those programs.

# SLEEP SOUNDLY WITH CONFIDENCE IN YOUR CYBER DEFENSES

Cybercrime isn't going away, but you can mitigate the risks with effective training, testing, and tools. CRI is ready to put your cybersecurity system to the test. With expertise in data security, privacy regulations, and security best practices, CRI's cybersecurity professionals can provide unbiased recommendations for risk mitigation strategies designed to protect your company.

CONTACT US TO SCHEDULE A CONSULTATION