FORTRA™

10 Cybersecurity Mistakes to Avoid

Cyberthreats are all around and increasing every day. But there's no need to let fear overwhelm you. Staying ahead of the would-be attackers doesn't have to be a constant game of whack-a-mole or something that keeps you up at night. You can protect your company's assets and enjoy some peace of mind.

Being aware of the problems, or potential problems, is step one. You're reading this, so you've got that covered. Vigilance is required, but you can take simple steps everyday to cover the basics, which you may already be doing. Standard corporate cyber hygiene – maintaining accurate hardware and software inventory, running updated endpoint protection, using firewalls, employing intrusion prevention and detection, conducting regular patching and maintenance – lays the foundation.Depending on your industry and the type of data you handle, there may be specific security measures you need to implement. But is there anything you shouldn't be doing?

In fact, there are plenty cybersecurity mistakes companies often make. Hopefully, you won't recognize your company here. If you do, it's time to take action. More on that later. For now, here are 10 cybersecurity mistakes to avoid.

STEP 1

Lack of Executive Support

At this point, most executives realize the importance of data security. No one wants to be the next CEO who has to explain why it took so long to identify a breach or address a known weakness. But top leadership may not understand what, or how much investment, is required to stay ahead of the bad guys. It's up to the chief security officer or chief information security officer to make the case for modern, flexible data security and infrastructure protection.

Lack of executive support challenges many IT teams when they try to gain budget approval for proactive and ongoing security initiatives. Unfortunately, these same budgets are often approved after a breach has occurred. One way around the budget impasse is to include the cost of a breach in the budget package. Contrasting the cost of prevention with the devastating consequences of a very real threat can help loosen the purse strings and deliver the executive support crucial to an effective security program.

For example, the worldwide average cost of a data breach is $4.4 million ($9.4 million in the US), a record high, according to Ponemon's Cost of a Data Breach 2022 report. But companies that had implemented one of 20 security measures, such as red team testing or the formation of an incident response team, saved an average of $209 thousand per incident.

For example, the cost of a data breach is $164 per record, according to Ponemon's Cost of a Data Breach 2022 report. Extrapolate that dollar figure by the number of records often lost during a breach and it's easy to see how quickly the cost adds up.

STEP 2

Infrequent Testing

Gone are the days of once-a-year testing to check off that box on the IT to-do list. Testing at intervals required for compliance may not be enough either. The dynamic nature of most corporate environments calls for much more frequent testing. Not keeping up with best practices for your organization may put you in jeopardy of a breach.

Just as early detection is important to the health of our bodies, it is as important to the well-being of an organization's network security. Similar to developing healthy habits such as exercise, sound nutrition, and regular check-ups, managing a corporate information network requires the same diligence. To improve security, it is imperative that regular assessments be conducted throughout the year to address any new vulnerabilities. Cybercriminals work all year round and security professionals must as well.

Scanning and testing frequency will depend on the amount of change introduced into your particular network since your last check. You may be able to gain executive support by demonstrating how assets can be compromised by the types of changes that happen regularly in today's systems. You might also point out that having a regularly tested incident response (IR) plan reduced the cost of a breach by an average of $2.7 million or 58%, according to Ponemon.

STEP 3

Being Strictly Defensive

The best defense is a good offense, and wouldn't it feel good to know your security had already been tested and weathered the storm? By all means, use all the defensive measures available. But you can't just sit back and wonder if you've plugged all the holes.

Regular, proactive penetration (pen) testing and red teaming can find unaddressed weaknesses and give you the peace of mind of knowing your defenses are solid. Pen tests can show whether your security measures will hold up in the real world and a red team of smart, determined pseudo-adversaries may find weaknesses your plan didn't account for.

Develop and implement the strongest plan your team can conceive. Then look for weaknesses. Plug those holes and test again. An ongoing, iterative approach is your best bet for staying ahead of cyber thugs.

If your company is relying solely on firewalls and external network scanning, you may have a false sense of security and be caught unaware. **Pen testing** and **red teaming** can help you more fully understand the security posture of your networks so you know where to invest to shore up your defenses.

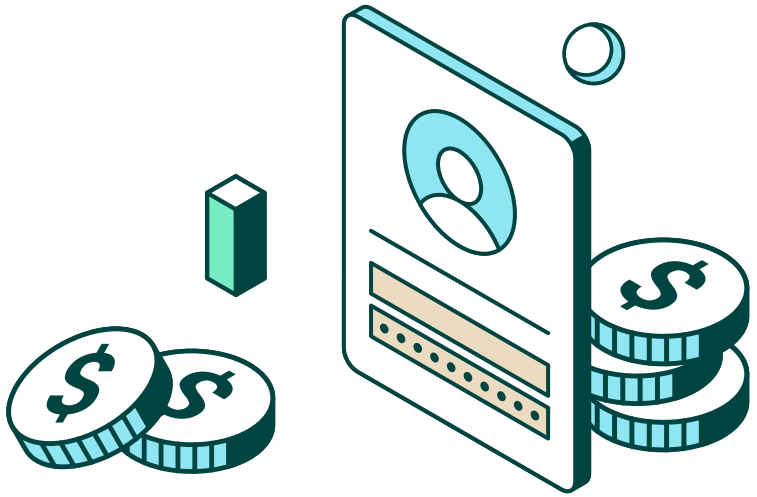
STEP 4

Overlooking The Human Element

Businesses often spend thousands of dollars on network security only to have crucial access data accidentally given away by an employee. Today's data protection technology has advanced, making it more difficult for hackers to 'get in', but human nature and a person's willingness to be helpful have not changed. Social engineers are always working smarter by exploiting basic human trust to get at the information they seek.

The top attack vector last year was stolen or compromised employee credentials, according to the Ponemon report. It even outpaced phishing, the previous top threat.

Employees are often the first place attackers go when trying to breach your systems, making them the first line of defense. To protect your data, train all employees to recognize an attempted attack and fight back. Make sure they know what to do at the moment and where to report any attempts. Don't neglect this crucial asset by leaving them unprepared.



STEP 5

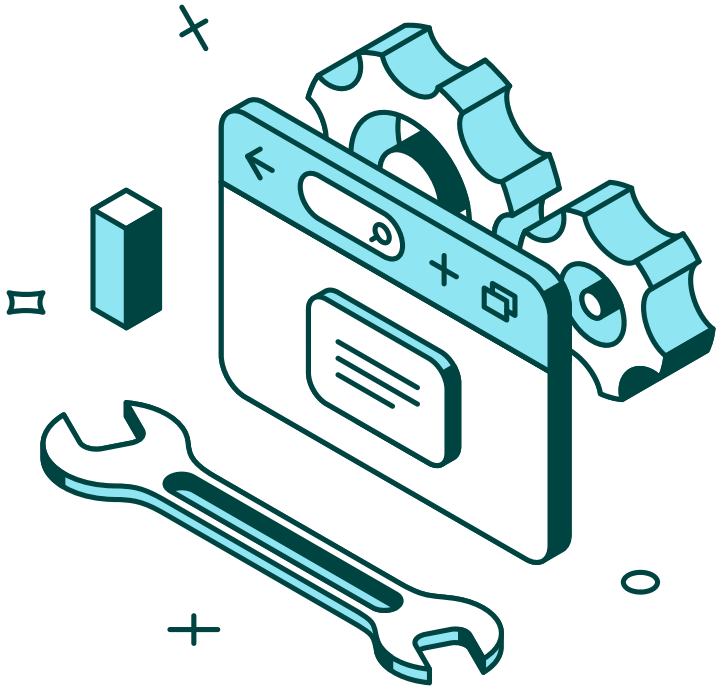
Investing In the Wrong Tools

Using technology to secure your systems makes sense. So does trying to save money by purchasing sophisticated tools that promise plug-and-play functionality. But all too often, IT teams wind up needing more personnel, weeks of training, or both to operate a system that was supposed to save time and money.

When looking for a way to secure your network without adding hard-to-find IT pros, focus on user-friendly tools and responsive vendors who will provide excellent customer service or professional services to get you up and running and answer all your questions. Read the fine print and make sure a human will be available to help when you need it. And don't forget to conduct a risk/reward analysis before committing to a new tool.

Cybersecurity pros are in short supply these days but you can find powerful tools that are simple to operate and vendors that understand how to provide the support you need.

Cornerstone security practices, like vulnerability management, can be high maintenance if the wrong tools are in place. You need **enterprise-grade features in a user-friendly format** that empower your team to identify and prioritize vulnerabilities accurately and efficiently, without weeding through mountainous reports that offer no context or prioritization.



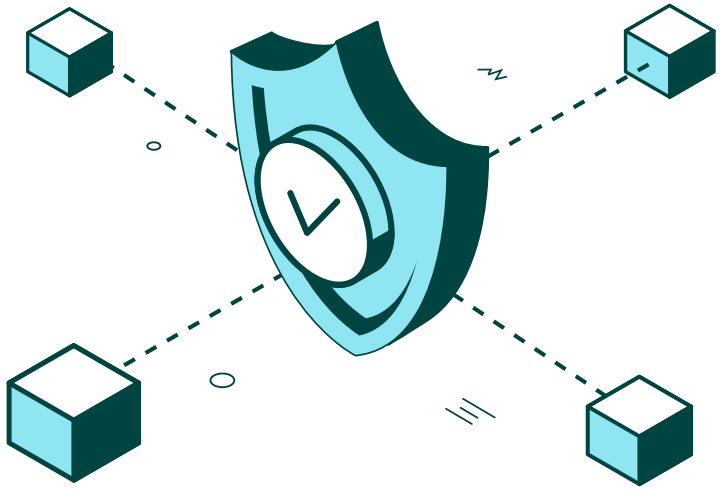
STEP 6

Assuming Compliance Equals Security

Many companies faced with a breach often have difficulty fully understanding the incident, wondering, “How could this happen? We passed our compliance requirements/audits.”

It is important to appreciate the benefits of compliance based reviews such as **SOX**, **HIPAA**, **HITECH**, **PCI DSS**, and others, while also understanding that compliance does not equate to security. Some compliance requirements are broad in nature and can be left open to interpretation by the organization, auditor or compliance officer performing the review.

There’s a difference between what regulators require as compliance minimum and best practices to keep your networks secure. Even if your budget doesn’t allow for all the bells and whistles, it’s still important to identify your company’s highest risk targets and do everything you can to protect them.

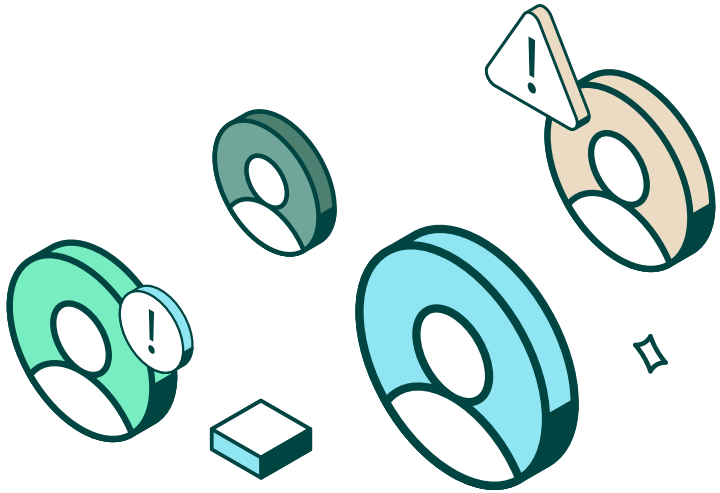


STEP 7

Apathy and Indifference

A common mistake made by understaffed and overwhelmed organizations is security apathy and indifference. The leadership at these organizations makes the case that, if the bad guys want in, they will find a way and there is nothing that can be done to stop them.

This type of apathy provides a prime target for a cybercriminal looking to gain access. Although there is no silver-bullet solution when it comes to security, there are very cost- and labor-effective security solutions that can be implemented. With adequate resources and a proactive approach, the chance of a breach can be greatly reduced.



STEP 8

‘It Can't Happen To Me’ Mentality

Whether it's thinking they are too small or in the wrong industry to be a target or that multi-factor authentication (MFA) and off-the-shelf antivirus software is enough, many companies think they aren't at risk or that they've mitigated all the risks. To a cyber criminal, the industry, size of the business, or tools employed don't matter. All organizations are a target.

No matter if your company has 20 or 20,000 employees, a proactive approach to security is imperative. That's not to say that MFA and software tools aren't important. They just aren't enough. And an "I'm totally safe" mentality isn't helpful because it can breed apathy. (See #7.)

Today's information security threats demand constant vigilance. Hackers, misinformed employees, and lax security – any of these can put your critical business operations, profits, and reputation at risk. In essence, organizations must conduct regular security risk assessments, awareness education, pen testing, and red teaming to ensure both networks and staff are secure.

STEP 9

Weak Supply Chain Security

Many organizations do background checks on employees but fail to do a comprehensive review of third-party organizations that have the potential for significant harm. Risks associated with vendors vary but all have the potential to bring about financial and reputational harm through error, data loss, breach of contract or confidentiality, and more. The same can be said of data partners. Basically, anyone who has access to your systems could cause problems.

Proper vetting can go a long way to alleviate this risk. Business leaders should perform due diligence on potential vendors to better understand backgrounds, performance history, and risk management practices. Supply chain security should not be limited to an annual audit. Organizations that hope to mitigate risk should conduct ongoing background checks on vendors and partners, especially as their personnel change.

In addition to proper screening, organizations should ensure that their supplier contracts include the appropriate control language requiring suppliers to institute regular security testing and an ongoing commitment to keeping sensitive data protected. If you can't trust the participants in your supply chain to do their best to protect your assets, it's not worth doing business with them.

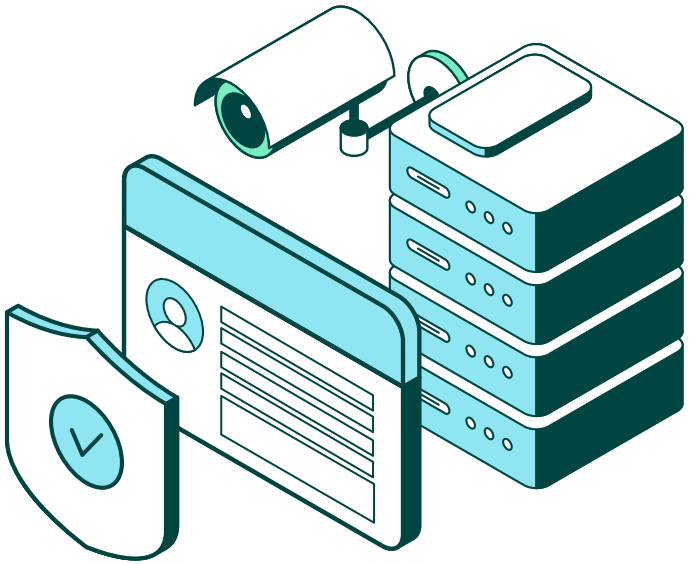
STEP 10

Poor Physical Security

Physical security is the protection of personnel, hardware programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Having strong physical security does not require a great deal of technical knowledge and can be one of the most impactful areas within an organization's security strategy.

Your Site Could be a Security Risk

- Do windows have glass break sensors?
- Are physical network access points/jacks secured to prevent an intruder from simply connecting their own device to the network?
- Is a valid proof of identification, such as a driver's license, required when a guest signs in?
- Is there camera coverage of facility dumpster/waste bins?
- Can badges easily be counterfeited by a social engineer?
- Are your employees friendly and helpful if someone without a badge wants access to the building?



Virtual pen testing is a great security practice for your digital assets and physical pen testing can protect your physical assets. Train employees on the proper actions to take if they find a USB drive on company grounds, notice someone without a badge loitering inside, see someone trying to follow them or another employee in through a secure door, or anything else suspicious. Cover the ways a clever criminal could use social engineering to gain entry. Once everyone is trained, conduct a **social engineering pen test** to be sure your physical security is as good as your cybersecurity. Address any issues and test again. It's an ongoing process.

Corporate Cyber-Hygiene Best Practices

We've all been using computers to get nearly everything done at work for some time now. We know not to repeat passwords or use overly simple ones. We may have even seen the phishing drill emails from our IT department. A lot of good cyber hygiene practices now seem like basic common sense. Here are a few more things your organization can implement to reduce your risk. Some have been mentioned above but bear repeating.

- Update software and systems. Make sure every device in your network receives regular updates, including any Internet of Things (IoT) or Industrial Internet of Things (IIoT) devices. Apply patches as necessary. Use an accurate and easy to use vulnerability management solution to help identify missing patches and prioritize them appropriately using risk context.
- Do the Little Things. Improve password security at all levels of the organization. Use MFA for password security. Employ firewalls and VPNs. Vet vendors to ensure strong cybersecurity at their organization.
- Train everyone. Make sure every employee, even the CEO, and every vendor participates in cybersecurity training. Keep security awareness top of mind year round by reminding staff to be on the lookout for phishing and social engineer attacks.
- Check social. Remind employees that attackers can gain inside knowledge from posts and out-of-office messages. Tell them not to share personal information in online forms. Unsolicited phone calls and alarmist emails should be treated with suspicion. Monitor social media for hostile mentions about your company or industry.
- Watch your data. Understand your landscape and where data goes if/ when you terminate service or a provider goes out of business. Backup your data and have a data retention policy in place to purge unnecessary data.
- Remember the physical world. Make sure entrances are secure and no one is allowed to 'tailgate' in. Documents should be shredded and trash handled in a secure manner. Encrypt laptops and have a strict policy for the handling of USB drives and portable media.
- Get help.. Use a third-party to conduct pen testing and red team testing. Employ intrusion detection systems (IDS) or intrusion prevention systems (IPS), network access control (NAC), and data loss prevention (DLP) systems.

Good cybersecurity isn't just one training a year or checking off a box and moving on. But it also doesn't have to overwhelm already stressed IT teams. The simplest approach is to cultivate a security-minded culture through training, reminders, testing, and remediation. Build layers of protection and employ offensive security tactics as well as defenses.. Hopefully this guide will help you keep your assets safe.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-dg-gd-0623-r1-79d