Get Smart About Cybersecurity:

10 Tips That Will Improve Your Security Resilience on Any Budget

CompliancePro™ SOLUTIONS
A Genzeon Company

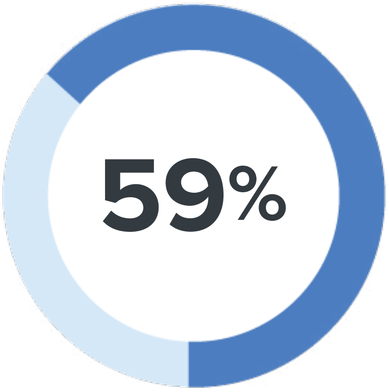
Introduction

“He who dies with the most toys wins.”

A while later, someone added, “But he’s still dead.” The same concept might be applied to cybersecurity: He who is breached with the most security tools is still breached. The mightiest cybersecurity isn’t born from “the most” tools, the most hi-tech, or the most expensive.

Formidable cyber resilience comes from knowing how to use what you have, using it wisely, and realizing that your tools are never infallible. And the latest state-of-the-art tools cannot conquer a careless or malicious employee who defies best practices or ethics. Nor can an organization stand strong if it fails to align its tools and protocols with current attack strategies. A complete security fortress calls for proactive protocols, reactive defenses, employee education, and current attack knowledge—all of which should be part of a documented, tested cybersecurity program.

This whitepaper will review eight critical strategies organizations can pursue to improve their cybersecurity resilience, even on a small budget.



Between 2020 and 2022, 59% of organizations have altered their cybersecurity strategies to meet evolving needs, but they’ve barely gained greater efficacy.

Source: State of Cybersecurity, Imprivata

CompliancePro™ SOLUTIONS
A Genzeon Company

10 Tips to Improve Your Security Resilience

The global price tag for a data breach is $4.35M; in the U.S., it more than **doubles to $9.44M**. And the healthcare industry continues to take the brunt of breach costs, with the highest average 12 years running. However, the price of a breach isn't just financial. A breach can also cost you your business reputation, client loyalty, and enterprise data.

01 PRIORITIZE PREVENTION

02 KEEP IT SIMPLE, KNOW YOUR TOOLS, AND RESIST OVER CONFIDENCE

03 PREVENT THREATS FROM WITHIN

04 DON'T FIRGET ABOUT PHYSICAL SECURITY

05 BE SELECTIVE WITH THIRD-PARTY VENDORS

06 KNOW YOUR CYBER ENEMY

07 ESTABLISH AND DOCUMENT A CYBERSECURITY PROGRAM

08 DON'T DISCOUNT YOUR ORGANIZATION'S SIZE

09 LEVERAGE AUTOMATED TOOLS

10 ENLIST THE HELP OF SECURITY CONSULTANTS

1 Prioritize Prevention

“An ounce of prevention is worth a pound of …” remediation. Or rather thousands of dollars in remediation. The cost of recovering from a data breach—if a company can recover—will most likely far exceed the cost of ongoing prevention.

Also, cyber insurance can’t repair your tarnished reputation or depleted customer base. And data back-ups can’t retrieve your sensitive information from the hands of bad actors—4**4 percent of companies** in 2022 said they lost confidential data because of a breach.

Organizations should always prepare and document incident responses and remediation plans, so they are ready to navigate a breach quickly and easily. But the more effort and resources put into prevention, the more resilient your organization can be to ward off cyberattacks before they happen.

Tips for Prevention

- **Keep software patches up to date** – Out-of-date software causes roughly 30% of data breaches.
- **Perform regular risk assessments** – Internal and third-party risk assessments should be a part of every prevention program to identify weaknesses before they can be exploited
- **Penetration tests and vulnerability scanning** – These tests take a deeper, more thorough dive into an organization’s digital weak spots.
- **Network monitoring** – Monitoring network activities and user behavior can help detect suspicious activities.
- **Employee education** – Staff negligence caused 63% of data breaches in 2022.

Failure to conduct a thorough and accurate risk analysis cost a research university $875,000 in fines and exposed the EPHI of 279,865 patients.

Source: Health and Human Services

2 Keep it Simple, Know Your Tools, and Resist Over Confidence

Blowing your security budget on the latest trending cybersecurity tools can reduce your resiliency if you don't use them correctly or if they don't coordinate with your unique framework and requirements. An abundance of random tools can lead to fragmentation and incongruity in your security processes and protocols. In fact, 65 percent of organizations pointed to fragmented IT and security infrastructure as a cause for their weakened cyber resiliency.

An IBM study from 2020 discovered that using too many tools—more than 50—may reduce an organization's ability to detect and guard against threats. Interestingly, the following year's report showed that the number of organizations that used between 51 and 100 security tools stayed the same (23 percent).

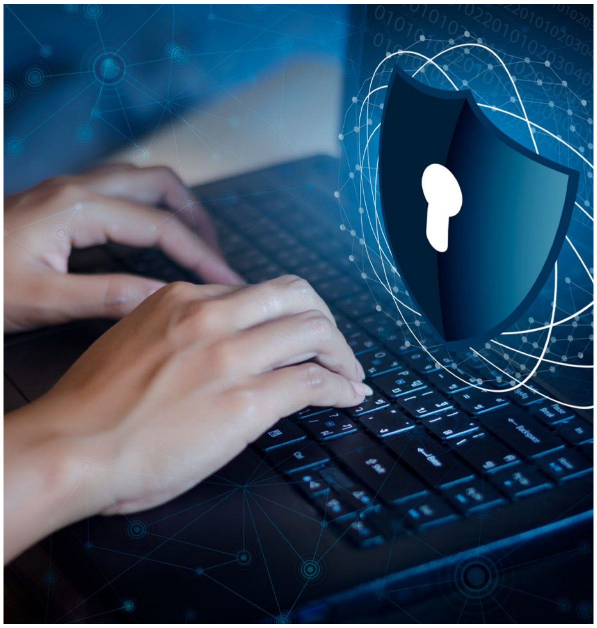
Organizations should first evaluate their needs and goals, research tools that will best align, and then learn to use them most effectively to gain optimal cyber resiliency. However, too much confidence in security tools can be a tempting trap. Cybercriminals continue to prove that security tools aren't infallible, and internal threats often bypass any tools laid in place—such as losing a work device or signing onto an unsecured Wi-Fi connection.

"Far too often, we see clients with good security tools in place, but no one is looking at the output or logs." said Michael M. Nelson, Managing Partner, Cybir. "Often a managed approach can help supplement an overburdened team or bring the specific skills needed to understand the threats that are being detected."

On average, enterprises deploy 45 cybersecurity-related tools on their networks.

Source: IBM Study

3 Prevent Threats from Within

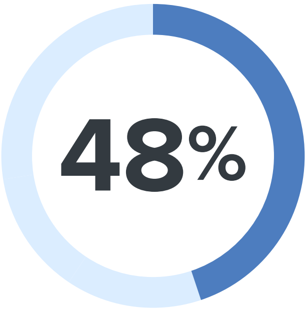


Insider threat incidents have sky-rocketed 44 percent from 2020 to 2022. And their cost per incident ballooned more than a third to **$15.38 million**.

Internal breaches can spawn from employees, temp workers, business partners, and vendors through negligence, inexperience, or maliciousness—and most incidents are not malicious. Compromised credentials took first place as the most common reason for internal data breaches, as there are several ways they can be misappropriated: Employees can expose their credentials through phishing attacks; or staff can exploit their access privileges for illicit conduct; hackers can gain access to unused but open users accounts (stale accounts)—60% of companies have more than 1,000 stale user accounts.

Abused credentials also took the longest to detect—**an average of 327 days**. That lengthy timeframe cost approximately **$150,000 more per breach** than other types of breaches.

One of the most effective ways to combat breaches born of negligence or inexperience is to educate employees. But not a one-time, new-hire cyber instruction. Frequent, routine cyber training accomplishes two critical goals: ensuring employees are up to date on current cyberattack trends and keeping security best practices at the forefront of their minds. A worker who just completed the third simulated phishing test of the year is less likely to fall victim to a real phishing attack in the near future than an employee who hasn't had training since onboarding two years ago.



48% of data breaches in healthcare facilities are caused by insiders

Source: Finances Online

4 Don’t Forget About Physical Security

Strong data security isn’t just about firewalls, passwords, and tools. Preventing physical access to your organization, its data, and devices is just as important as preventing virtual access. Cybersecurity and physical security should not be siloed, but rather thought of as two prongs of the same fork.

Tips for Physical Security

- Prevent unauthorized access to your building or offices
- Secure all device storage areas and server rooms
- Shred all documents no longer in use
- Require log-on credentials for all devices
- Limit copying and sharing of sensitive files

5 Be Selective with Third-Party Vendors

Third-party risks are another type of internal threat but can be the most difficult to control. Your organization is at risk if just one of your vendors lacks strong cyber protection. One study predicted that by 2025, 60% of organizations will use cybersecurity risk as a decisive factor for third-party engagements.

Third-party vendors can include billing and distribution services, supply chain vendors, software vendors, internet service providers, cloud providers, and security and other technology partners. And now, with the proliferation of third-party software applications and an increasingly global supply chain, controlling third-party vendor risk is at its most challenging. Thirty-nine percent of organizations pointed to vendor support issues as a key factor in improving security frameworks.

Risk assessments prove to be one of the most crucial shields against third-party threats. However, 54 percent of businesses fail to conduct these assessments for their vendors. Here are just a few other steps organizations may take to protect themselves from third-party risks.

- Assess potential vendors before onboarding
- Include risk management in contracts
- Document every vendor and regularly update inventory
- Monitor vendors’ security controls and performance
- Restrict vendors to only necessary data and network access—principle of least privilege
- Investigate fourth-party risk—your vendors’ vendors
- Talk to vendor’s previous and current customers and read reviews
- Review NIST Cybersecurity Framework and Center for Internet Security controls for better understanding of cyber risk management and available tools

Even small organizations that lack the resources for a massive vendor management program can still carry out most of the above to protect their cyber integrity from unsafe third parties. With 56 percent of organizations stating that a third-party cyber breach effected misuse of their confidential data, security leaders must make third-party vendor protection a priority, particularly leaders within healthcare—55 percent of healthcare organizations revealed that they suffered a breach by a third party.

48% of organizations don't have a comprehensive inventory of all third-party access to their network.

Source: State of Cybersecurity, Imprivata

6 Know Your Cyber Enemy

How can you defeat an enemy if you don't know who he is or his methods of operation? Your employees and IT teams should stay abreast of cybersecurity and attack trends to understand who and what they must defend against.

For example, the proliferating ransomware-as-a-service attack model has granted novice bad actors the potential to execute breaches that previously only savvy cyber thieves could pull off. So, now career criminals looking for a big payday aren't the only villains on the prowl—a first-timer might be perfectly content to infiltrate a small, fledgling company with weak security.

Cybercriminals constantly alter and refine their attack methods. Security leaders must track and monitor their tactics to keep an organization's cyber protocols and employee education in step.

> *"The key to an effective defense strategy is defining **who the threat actor is and what threats they are making**. This means tracking the threat actors' tactics, threats, and procedures to learn more about them. Organizations must [also] act on the intelligence they have, including using it to hire appropriate cybersecurity professionals."*

Colonel (res.) Shmulik Yehezkel, Chief Critical Operations Officer at CYE,
Source: Cyber Defense Magazine, 2022

7 Establish and Document a Cybersecurity Program

An IBM report from 2021 report noted: “Since different breeds of attack require unique response techniques, having pre-defined playbooks provides organizations with consistent and repeatable action plans for the most common attacks they are likely to face.” Unfortunately, 74% of respondents said their cybersecurity planning is insufficient—they have no plans, ad-hoc plans, or their IT staff is inconsistent.

Cybersecurity programs can help an enterprise better understand how their security protocols work—or don’t—and view their security more as a systemic game plan rather than fragmented miscellaneous pieces. A documented program will also help enforce crucial consistency and visibility for the organization.

Elements of a Comprehensive Cybersecurity Program

Here are a few critical elements that every strong security plan should contain. This is not an exhaustive list.

- Documented and tested policies and procedures
- Incident response and disaster recovery plans
- Routine employee training
- Frequent risk assessments
- Regular vulnerability assessments and penetration tests
- Stale account audits
- Password parameters
- Email filtering
- Tabletop testing

> *“A documented cybersecurity program allows a company to* ***more easily identify and react*** *to the ever-evolving tactics that bad actors use.”*

Chris Lyons, Director of Cybersecurity, CompliancePro Solutions

8 Don’t Discount Your Organization’s Size

For the average cybercriminal, size doesn’t matter. Most bad actors are looking for the easiest way in. Often that most vulnerable ingress lies within a small-to-medium (SMB) that thought their company was too small to draw the attention of cyber thieves. Fifty-four percent of SMBS think they’re too small for a cyberattack—which might be why breaches on new small businesses **exploded by 424 percent** in 2022.

Small business cyber breaches exploded by 424% in 2022.

Bad actors know that many SMBs—especially fledging businesses—work with limited budgets and often don’t allocate much of that shallow well towards cybersecurity. They also understand that staff within a new SMB may lack the experience and knowledge to follow cybersecurity best practices and that leaders may lack the expertise to establish robust security protocols, including employee security training. Researchers at Barracuda Networks analyzed millions of emails within thousands of organizations and concluded that companies with less than 100 employees experience 350 percent more social engineering attacks than larger businesses.

The cybercrime focal point has shifted from targeted attacks on major corporations perpetrated by well-seasoned criminals to random attacks on SMBs by opportunistic cyber muggers—and smaller organizations must approach their cybersecurity accordingly. Remember, strong security doesn’t require a big budget.

9 Leverage Automated Tools

Automation can save organizations 3.05 million by detecting breaches 28 days faster than companies that don’t use it.

Organizations are already bumping up their use of automation to improve operational efficiency, reduce overhead, and stay competitive. They are also discovering that automation can fortify their cyber resiliency: One study found that 66 percent of organizations use automation to improve security resiliency. Another report declared that a fully deployed automation program enabled companies to detect and contain a breach 28 days faster than enterprises that didn’t use automation—potentially saving $3.05 million.

For organization with limited staff, automation can help pick up the slack and relieve stretched IT teams of certain tasks. It can also help with prevention, like setting up alert notifications for regular assessments, software updates, etc

10 Enlist the Help of Security Consultants

Seeking advice from a reputable, experience cybersecurity consulting service can help an organization get a clearer understanding of their unique needs and how best to approach stronger cyber resilience.

A third-party professional can be more objective about an organization's current security state and may see gaps or weaknesses that even IT leaders may miss. When staff is stretched thin, they often don't have the band width to focus fully the way a consultant can. Organizations with smaller budgets can get advice about how to create the most effective cyber program with minimal financial output. Security consultants can also help with risk assessments, pen tests, and vulnerability scans.

Conclusion

Potent cyber resilience isn't devised from big spending, trendy technology, or an abundance of tools. It comes from intelligence: acquiring tools and protocols that best align with your organization's needs and using them wisely; educating employees so they are aware of and ready to defend against the latest attack methods; beefing up preventative measures; scrutinizing third-party vendors; and establishing and documenting a cybersecurity security program, which includes best practices, and an incident response plan.

No cybersecurity tool or program is infallible. But with careful thought, planning, and guidance, organizations can fortify their cyber resilience to their utmost ability and defend against bad actors.

Enlisting the help of security professionals can make certain that your cybersecurity efforts are on target and as potent as then can be.

CompliancePro™
A Genzeon Company
SOLUTIONS

CompliancePro offers the healthcare industry's only comprehensive solution to automate security, privacy and compliance. Our SaaS platform, along with consulting and advisory services, can help organizations of all sizes reduce both costs and risks. CompliancePro is a subsidiary of Genzeon.

CompliancePro Solutions

(833) 677-0108
info@complianceprosolutions.com
complianceprosolutions.com

559 W Uwchlan Ave
Suite 120
Exton, PA 19341