BUILDING A STRONG SECURITY FOUNDATION THROUGH CYBER RESILIENCE

xamin

Cybercrime is a $6 trillion annual industry, affecting all businesses and individuals. Global cybercrime costs are expected to grow 15% per year over the next 5 years, reaching $10.5 trillion USD annually by 2025. For comparison, the cost was $3 trillion USD in 2015.

For CPA firms, the cost of forensic discovery, remediation, requirements, and legal fees can be up to $300,000—not to mention the revenue lost from clients who no longer want to stay after their data is compromised. Only one thing can help decrease these costs: cyber resilience.

Whereas cybersecurity focuses on the protection of computer systems and networks, cyber resilience looks further: When met with adverse conditions, how capable of thriving is your organization? How will you continue to operate when your cybersecurity measures aren't enough?

CYBER RESILIENT STRATEGIES EVERY FIRM SHOULD ADOPT

1. Get in the mindset of "when" not "if"

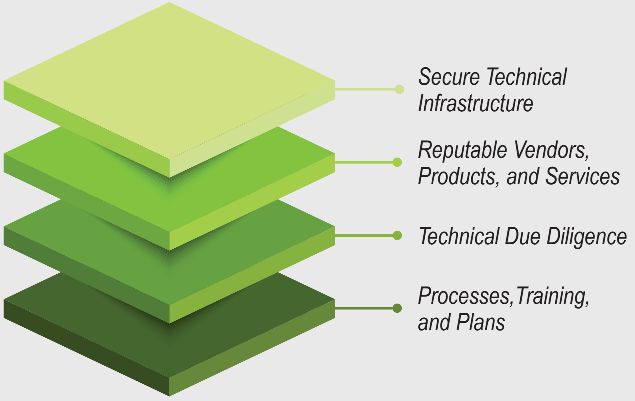
Every 11 seconds, there is a ransomware attack on a business, yet the likelihood of detection and prosecution of cybercriminals is only 0.05%. Cyberattacks continue to rise in frequency every year, and every organization is at risk. In order to keep your organization secure, you need to think in the mindset of "when" not "if" a breach will happen.

By understanding how a cyberattack will impact your organization, you can better develop proactive and systematic processes like business continuity and recovery plans. You can create or hire a cross-functional team to plan for threats and attacks—and implement strong cybersecurity measures to prevent them.

When the threat is at your door, you can rapidly restore your organization's function with a proper incident response plan to avoid interruption to your operations. Just as threats continue to develop, so, too, must your cybersecurity. Make continuous improvements to the plans you have in place to support your organization and thrive in evolving conditions.

2. Build a layered cybersecurity approach

Mitigate your organization's risk of attack by building cyber resilience through ongoing cybersecurity and risk assessments. Because potential security risks can occur at a variety of levels, you need to set up security measures that provide multiple layers of defense against these risks. This includes:


Secure Technical Infrastructure
Reputable Vendors, Products, and Services
Technical Due Diligence
Processes, Training, and Plans

3. Train your employees

However, none of this matters if end users aren't educated on how to help the business protect its company, employee, and client data. Human error is the driving cause of 95% of cyber security breaches. Implement Security Awareness Training to keep your employees aware of potential attacks—and teach them what to do when they encounter vulnerabilities.

4. Purchase cybersecurity insurance

Cyber insurance helps recoup losses, pay for investigations, cover legal costs, and it gives you the resources to get your organization back in business following a cyber-attack.

Any business that deals with sensitive information—including credit card numbers, medical information, social security numbers, or any other personal information—should have cyber insurance to protect customer information, industry relations, and business reputation.