How to Improve Your Cyber Resilience

We often think of cybersecurity in terms of our physical health—we talk about computer viruses and cyber hygiene.

Cyber resilience is another way to think about your online fitness: just like humans can get sick even if they take precautions like washing their hands, taking vitamins, or exercising, your online systems can be attacked even if you follow cybersecurity best practices. Cyber resilience is how you get better. It might take a bandage or extensive surgery, but you can recover. That's why you should have a plan.

Today, cyber resilience is a critical concept that emphasizes the ability to withstand and recover from cyberattacks, as well as the capability to adapt to new threats. Individuals, businesses, and other organizations can assess their own resilience and bolster their cyber resilience strategies.

Understanding cybersecurity resilience

Generally, cybersecurity resilience is the backbone of an organization's ability to maintain essential functions and swiftly recover from cyber incidents. It encompasses proactive measures, incident response readiness, and recovery strategies.

Resilience goes a step beyond basic cybersecurity measures because cyber resilience emphasizes the ability to operate during a cyber incident as well as recovery. Simply put, it's about staying operational and safeguarding critical data despite cyber threats. It's a way to think "when" instead of "if."

Effective resilience helps minimize the impact of attacks, reduces downtime, protects sensitive data, maintains customer trust, and complies with regulatory requirements. It safeguards an organization's reputation and financial stability.

Assess your personal cyber resilience

While we typically speak of cyber resilience as a strategy for organizations, evaluating your cyber resilience as an individual is a good thought exercise. This can be a first step before embarking on a plan to strengthen your business, nonprofit, school, or group. Consider your own digital habits, security practices, and awareness of potential threats. Ask yourself:

- Do I use long, complex, and unique passwords?
- Do I have MFA enabled for every account?
- Do I regularly update software?
- Do I refuse to click suspicious links or download unknown attachments?
- Do I back up important data and know how to recover it in case of a cyber incident?

Use these questions to guide you in assessing your cybersecurity posture and identifying areas for improvement.

How departments can enhance cyber resilience

Due to their valuable data and assets, departments are prime targets for cyberattacks. A solid resilience plan brings together risk management, incident response, business continuity, and disaster recovery strategies. Here are steps organizations can take to boost cyber resilience:

1. **Conduct a review:** Conducting a cybersecurity resilience review helps identify vulnerabilities, assess current strategies' effectiveness, and determine areas for improvement. This review process ensures that policies, procedures, and technologies are aligned with the organization's resilience objectives.
2. **Develop incident response playbooks:** Create detailed plans outlining how to respond to various cyber incidents. Include roles and responsibilities, escalation procedures, and communication protocols.
3. **Conduct tabletop exercises:** Simulate cyber incidents to test your response capabilities. These exercises help identify gaps, improve coordination among teams, and refine response strategies.
4. **Implement disaster recovery and cyber recovery strategies:** Establish robust backup procedures for data and systems.
5. **Utilize technology solutions:** Leverage automated incident response systems, advanced threat detection tools, and network segmentation to fortify defenses and mitigate risks.

How to measure cyber resilience

Effective cyber resilience means handling cyber incidents smoothly and recovering quickly. Here are some ways to measure how well you're doing:

1. **Mean Time to Detect (MTTD):** This is how quickly you notice that something is wrong, like spotting an exploited software bug or other strange activity on a computer.
2. **Mean Time to Respond (MTTR):** Once you detect a problem, how quickly can you deal with it? This could involve removing malware from a device or restoring data from backups.
3. **Recovery Time Objectives (RTO):** If a cyber incident disrupts your operations, RTO is the goal for how quickly you want to get everything back to normal. It's your plan to get your systems up and running again as soon as possible.

You also want to keep detailed logs of the frequency of how often incidents happen, as well as your response efforts and successes. How well did your plan work? Did you resolve the issue effectively and prevent more damage?

By monitoring these things, leaders can understand how well their organization is prepared. They can strategize and implement improvements to stay resilient over time. Just like a regular checkup, you want to check the health of your digital defenses often to make sure they're strong and ready for whatever comes their way.

Resilience isn't a one-time thing

Cyber resilience is not a one-time effort but an ongoing commitment to preparedness, response readiness, and recovery agility. By assessing individual practices and implementing proactive measures at the organizational level, we can strengthen our collective defenses against tomorrow's cyber threats. Remember, resilience is not just about surviving cyber incidents—it's about thriving with confidence and security.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

STOP | THINK CONNECT™

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.