Cyber Attacks Are Inevitable — So Stop Preparing For If One Happens and Start Preparing For When One Will

Opinions expressed by Entrepreneur contributors are their own.

In 2024, organizations faced an average of 1,308 cyber attacks per week in Q1, a 28% rise from the previous quarter and 5% year-over-year. And what's even worrisome is that cybercrime losses reached $12.8 billion in 2023 and are expected to hit $23.84 trillion by 2027.

Undoubtedly, securing your business in today's digital business landscape isn't just about protecting against cyber threats — it's about resilience.

You can always fall for the latest threats since cybercriminals are becoming increasingly sophisticated while sneaking into business networks. Hence, you need a more robust cybersecurity plan backed by cyber resilience that goes beyond conventional cybersecurity strategy.

Cyber resilience isn't a buzzword; it's a necessity and a proactive approach that goes beyond conventional security. It ensures your organization withstands and recovers from potential threats without much impact on your business.

In a nutshell, cyber resilience is about building walls of protection and having the resilience to bounce back stronger.

Let's discover why embracing resilience should be a top priority for businesses to ensure continuity and future

success in the ever-expanding cybersecurity landscape.

Related: There’s No Margin for Error in Cybersecurity – Here’s How to Build a Strong Online Defense through Everyday Habits

Why your business needs cyber resilience

Cyber resilience is your organization’s ability to prevent, withstand and smoothly recover from various cybersecurity incidents. Cyber resilience isn’t about preventing cyberattacks – it’s about ensuring your organization can swiftly recover and continue to operate after an incident.

Nobody can predict the next threat to your organization and customers, especially in an era where machine learning and artificial intelligence have broadened the horizons and increased threat vectors.

Hence, a robust incident response plan is undeniably the need of the hour for businesses that are about to reinvent their cybersecurity posture.

Remember, a cybersecurity strategy lacking a robust incident response plan is good for nothing since cybercriminals are already exploring new ways to target end users and customers to exploit their personal information and gain access to sensitive business details.

On the other hand, cyber resilience not only ensures stringent cybersecurity against immediate threats but eventually mitigates long-term costs. Hence, investing in cyber resilience would surely safeguard your business from financial devastation and ensure smooth continuity.

Now that we’ve learned about cyber resilience and its importance, let’s emphasize how you can incorporate it into your business.

Related: 3 Reasons to Increase Your Cybersecurity Protocols in 2024

Is your organization truly protected?

Most businesses mistake cyber resilience for cybersecurity. However, they are pretty different and hold their own importance at different levels.

Securing your organization against modern threats is crucial, but it’s also important to prepare for the worst. For example, you must have a plan to deal with a data or privacy breach.

If you wish to protect your organization from the latest threats, your cybersecurity must include a comprehensive cyber resilience checklist.

Whether it is regular audits, employee training, or advanced threat detection through technology, you must always be geared up to handle any cyber incident.

Your cybersecurity checklist to supercharge your cyber resilience

1. Regular security audits

Scheduled audits are crucial to uncover potential threats and vulnerabilities before cybercriminals can exploit them. Addressing the issues well in advance can help you prepare a solid plan for the worst-case scenario and bounce back stronger.

Here’s what you can do:

- **Look for outdated software:** It’s crucial to check and

update your defense software and firewalls since outdated software is more susceptible to ransomware attacks and other threats.

- **Incidence response drill:** Organizing an incident response drill will help identify gaps in your communication protocol and eventually help you overcome the delayed response time during a cyberattack. Hence, scheduling quarterly incident response drills is crucial once you've completed the security audit.
- **Engage third-party experts:** Involving third-party cybersecurity experts can provide an unbiased evaluation of your security measures and help create a robust cyber resilience program. Experts can uncover vulnerabilities your internal teams might overlook and help prepare an action response plan accordingly.

2. Strengthening your human firewall through employee training and awareness programs

Human error leads to cybersecurity breaches. Ensuring your employees are well-trained to handle any vulnerability is critical to building cyber resilience.

- **Regular training sessions:** Regular training and updating your employees on the latest threat vectors and best practices are essential. Using real-world scenarios to illustrate various threats and their corresponding responses would shield your organization from potential threats and minimize losses during an unforeseen event.
- **Phishing simulations:** Implementing phishing simulations to test your employees' ability to recognize and respond to phishing attacks is crucial for safeguarding sensitive information. Using the results to identify improvement areas will help tailor training to minimize human error.

- **Clear policies and procedures:** Establishing clear cybersecurity procedures and policies within your organization is crucial to building resilience. Ensure the policies are easily accessible and understood by everyone in the organization.

3. Building a robust incident response team is your frontline defense

A dedicated incident response team is all you need for swift and effective action during a cybersecurity incident. This will help minimize the impact, leading to fewer financial and reputational losses.

- **Define roles and responsibilities:** You must clearly define roles and responsibilities for every team member regardless of their job title and experience. It's crucial to ensure that everyone knows their duties and responsibilities promptly during an incident and the situation.
- **Invoke the potential of modern tools and technologies:** Using threat intelligence tools, data encryption, multi-factor authentication (MFA), and Zero Trust architecture can reinforce your overall cybersecurity resilience program.
- **Continuous improvement:** Conducting a thorough review to identify areas for improvement after every drill and incident. This will help you continuously update your incident response plan based on the recent findings.

Final thoughts

In this modern digital business landscape, the increasing cyber threats and sophistication of cybercriminals demand next-level security – cyber resilience.

Cyber resilience is a vital strategy for businesses to ensure they stay up and running even in the event of a cyber incident and can quickly contain a breach without financial and reputational losses.

Hence, embracing cyber resilience shouldn’t be a luxury; it must be an essential pillar of your cybersecurity foundation.

https://www.entrepreneur.com/science-technology/cyber-attacks-are-inevitable-so-stop-preparing-for-if/476591