CYBALT

Developing An Effective Cybersecurity Strategy By The Numbers

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

discover@cybalt.com

Developing an Effective Cybersecurity Strategy by the Numbers

3 Need-to-Knows

First, let's begin this discussion on cybersecurity by saying, that if you don't have one already, it's time to develop a cybersecurity strategy, and one that's effective. A cybersecurity strategy is a blueprint of how you plan to protect your organization's assets and minimize cybersecurity risks.

Second, do it now.

Third, because the technology behind cyberattacks and cyber attack methods changes unpredictably and frequently these days, you (and your organization) need to review your cybersecurity strategy and update it regularly. Having effective cyber security is key to your ability to protect your organization's assets, including its reputation, intellectual property (IP), staff, and customers. It is important to note here that organizations are linking more and more of their operational processes to their cyber infrastructure.

4 Fundamental Questions

To counter the ever evolving cyber threats facing organizations today, you, as an IT and business leader, must ensure you have an integrated approach to cybersecurity tailored to your particular business and risk profile. You need to address not only the technical aspects of your cyber defense, but also the people and organizational elements.

There are four fundamental questions that you, and your team, need to answer as part of your cybersecurity strategy development process:

1. Have we first understood the cybersecurity risk in relation to our organization and critical business operations?
2. Can we integrate across personnel, technical security, information assurance, and physical security?
3. Are we able to establish protective monitoring to prevent and deter the insider threat?
4. Despite all measures and controls, are we ready to accept that some attacks will breach our defenses?

Let's remember the purpose of a cybersecurity strategy is to have high-level planning and to develop the roadmap to secure your data, assets, and organization from cyber threats. It is critically important to have a proactive security approach to prevent your organization from next-gen cyberattacks and also to effectively handle a cyber incident.

A high-level cybersecurity strategy can protect your organization from small-to-large cyberattacks, so you can preserve its reputation and reduce harm to the organization and its employees, customers, partners, and others.

5 Key Cybersecurity Steps

So what are the key steps that you, and your organization, can take as part of your cybersecurity strategy? Let's take a look.

Prepare: Ensure your employees are properly trained regarding their incident handling roles and responsibilities in the event of data breach. Develop cyber attack drill scenarios and regularly conduct mock data breaches to evaluate your incident handling plans. Ensure that all aspects of your incident handling plan (training, execution, hardware, and software resources, etc.) are approved and funded in advance.

Prevent: Your (and your organization's) next goal is preventing any security breach from happening to begin with. This is your first line of defense. Your actions in this category should be directed at preventing payload delivery and execution and stopping unauthorized access.

Contain and Mitigate: Your next goal is to limit the damage if your first line of defense fails and there is a security breach. Most organizations have robust security measures that focus on prevention but have little to no defense if their network is breached.

Recover and Restore: The next goal is to have the ability to quickly regain access to and functionality of your IT infrastructure after cyberattacks. This is a critical security goal that aligns with business goals of operating with little to no downtime.

Lessons Learned: Your last goal is that once the incident is over, hold an after-action meeting with all Incident Response Team members and discuss what you've learned from the data breach. This is where you should analyze and document everything about the breach. Determine what worked well in your response plan, and where there were holes. Lessons learned from both mock and real events will help strengthen your systems against the future attacks. You also need to check what changes need to be made to security. Should employees be trained differently? What weakness did the breach exploit? How will you ensure a similar breach doesn't happen again?

Your Next Step

Your next step in creating an effective cybersecurity strategy is to contact our dedicated team of experts to help you plan, prepare, and defend your organization. For more information about cybersecurity, call at +1-855-324-9909 or email us at **discover@cybalt.com**.