COMPUGEN

Innovate. Inspire. Impact.

Why You Need a Sound Cybersecurity Strategy

TABLE OF CONTENTS

COMPUGEN

Innovate. Inspire. Impact.

The Identity Theft Research Center (ITRC) reports a record number of data compromises in the U.S. in 2021, a 68% increase from 2020. Accenture found that insurance, followed by consumer goods and services and telecommunications, are the top industries under ransomware attacks.

Meanwhile, the cost of data breaches continues to skyrocket. According to a global study sponsored by IBM Security and conducted by the Ponemon Institute, the average cost rose from $3.86 million in 2020 to $4.24 million in 2021. Cybersecurity risks and business disruption are the top two business risks of 2022.

In today's digital business environment, where data is corporations' lifeblood, cybersecurity is critical to survival. But information security is a complex discipline—you must address multiple moving pieces to ensure they work together seamlessly to achieve your security goals.

This white paper will explore the what, why, and how of the cybersecurity trifecta: policy, culture, and insurance to help you strengthen your defense.

SET YOUR STRATEGY

A cybersecurity strategy is a high-level plan that helps organizations manage risks associated with the use of data. It should be a living and breathing document to help you stay relevant and competitive as technologies, threat landscape, and business and regulatory requirements evolve.

The Benefits of a Sound Cybersecurity Strategy

Cybersecurity is complex—everything must work together seamlessly to cover the ever-expanding attack surface created by increased digital transactions, remote working, cloud computing, etc. You can't implement a few disparate tools and hope the pieces will fall into place.

Here's why you should start with a solid cybersecurity strategy:

- It gives you a bird's-eye view of what skill gaps you must fill and identify the right resources to execute the appropriate security protocols.
- It helps you map all your business-critical information and customer data so you can implement security solutions to protect them.
- It guides you to allocate resources strategically to prevent attacks and breaches, which can tarnish your reputation, diminish customer trust, and lead to the loss of business.
- It lays out the tools you need to stay current with emerging threats, so you can take a targeted approach to protect your digital assets.
- It enhances visibility into your IT infrastructure to increase the flexibility and scalability of your systems while supporting key trends such as remote working.
- It addresses the delivery of staff training to ensure everyone is aware of the latest threats and taking the right action to protect company data.
- It ensures that you comply with various data privacy regulations (e.g., GDPR, CCPA, PCI-DSS, HIPAA, etc.) to avoid legal ramifications and hefty penalties.
- It provides guidance to handle potential breaches and limit damages associated with an attack (e.g., by reducing costly downtime caused by the loss of data.)
- It helps you take a proactive security approach while being better prepared to respond to incidents to prevent minor ones from festering into devastating issues.

How to Cultivate a Cybersecurity Mindset

Creating a cybersecurity strategy starts with understanding your cyber threat landscape and evaluating your current cybersecurity maturity. Since it's almost impossible for any organization to address every risk all at once, the insights can help you prioritize resources and resolve the most urgent vulnerabilities.

Next, design or improve your cybersecurity program to address compliance requirements, identify the cybersecurity tools you need, and determine the best practices to follow. You should also regularly conduct risk assessments and update your security plan, policies, and procedures to stay current.

Here are the key components to include in your cybersecurity strategy:

Security Frameworks and Compliance Standards

You don't have to start from scratch—you can leverage various cybersecurity frameworks, such as NIST-800, ISO 27000 family, SOC 2, CIS v7, and COBIT as the foundation. Then, layer on requirements specific to your industry and business model, including PCI-DSS, FISMA, HIPAA, etc., to outline your security roadmap.

Cybersecurity Maturity Assessment

Regular risk assessments help you understand your company's cybersecurity maturity and see how you can improve your cybersecurity posture. The evaluation should cover data governance policy, cybersecurity tech stack, incident response processes, etc.

Cyber Threat Landscape

Develop a broad understanding of the company's operating environment and how your organization situates within the latest threat landscape. For example, what vulnerabilities are present at customer touchpoints? Who could benefit most from hacking into your network? What are the methods criminals use against companies in your industry?

Data Security Policy

Based on various requirements and standards, you can develop guidelines and policies to set employee expectations and detail the consequences of violation. These include workstation policy, acceptable use policy, remote access policy, and bring your own device (BYOD) policy.

Roles and Responsibilities

Cybersecurity has many components, and the complexity means it's easy for things to fall through the cracks. Clearly defining roles and responsibilities is key to establishing accountability and ensuring that everyone in the organization does their part to keep your business-critical information safe.

Employee Onboarding and Education

Your security policy is only as good as your employees' ability to follow it. Plus, it takes only one person to click on one malicious link or attachment to infect your entire network. Implementing a comprehensive employee onboarding and training process is critical for covering all the bases.

LIVE YOUR POLICY

Did you know that the average organization is targeted by over 700 social engineering attacks yearly? Social engineering and phishing attacks are responsible for 70% to 90% of malicious breaches, costing companies an average of $130,000 per attack.

By tricking employees into giving away their login credentials, criminals can access an organization's critical business information (e.g., intellectual properties) and sensitive customer data. Hackers increasingly target individuals with high access privileges to exfiltrate a large amount of valuable data.

Therefore, companies must ensure that everyone with access to their systems and networks—including employees, partners, vendors, and contractors—is aware of their cybersecurity policies and take the necessary precautions to protect their credentials and accounts from prying eyes.

You most likely have a security policy, and every employee and contractor has signed their name on the dotted line to say they've read it. But that isn't nearly enough—your security policy is only as good as the end-users' ability to adhere to it and apply the guidelines to their day-to-day activities.

So how can you ensure that everyone is living your security policy?

It starts with a security-focused culture where everyone understands the importance of protecting business-critical data and customer information. Implement employee awareness training and education to ensure end-users understand what to watch out for and how to stay safe. Then, provide the right technical support to help them correctly configure their hardware and software according to your security requirements.

How to Bring Your Security Policy to Life

Building a culture of security and providing employee awareness training can bring a lot of benefits to organizations:

- **Prevent the high cost of data breaches:** Cyber attacks can result in costly downtime, loss of business, tarnished reputation, diminished customer trust, penalties for regulatory violations, etc.
- **Turn people from vulnerability into your first line of defense:** Ongoing training helps employees gain the knowledge and skills to become part of the security solution instead of a liability.

- **Maximize your security technology investment:** From firewalls to multi-factor authentication, these technologies are only as effective as your employees' ability to use them.
- **Build customer trust and confidence:** Consumers expect businesses to protect their privacy. Employees who are proactive about safeguarding customer data can help you build trust with customers and improve your brand's reputation.
- **Achieve regulatory compliance:** Organizations must adhere to increasingly complex data privacy laws. Getting employees' corporations allows you to achieve compliance cost-effectively.

Why Employee Awareness is Critical

Ensuring employees adhere to your security policy in their day-to-day activities requires a multi-prong approach. Here are some key components:

Make Security Training Accessible

Your training materials should be relatable and actionable. Use easy-to-understand language and illustrate the guidelines with scenarios relevant to the audience. Tailor specific content for employees based on their roles and responsibilities to help them envision how they can apply the security policy to their jobs.

Provide Ongoing Training

Security awareness training isn't a one-and-done exercise. Criminals deploy new techniques every day while business requirements are changing rapidly. You must provide frequent updates and reinforcement to ensure that cybersecurity stays top of mind for everyone in your company.

Encourage Cooperation Through Communication

Security should be a two-way conversation. Promote a sense of responsibility and belonging to rally employees around your security policy and encourage timely incident reporting. Also, avoid using a punitive tone or incomprehensible jargon in your messaging, which may create resistance.

Eliminate Shadow IT

Shadow IT—using unsanctioned software to handle company data—often result in information security risks. But instead of cracking it down with an iron fist, understand what employees need to do their jobs and give them the right tools so they won't go behind IT's back to install unapproved applications.

Get Leadership Support

Leadership must be part of the cybersecurity conversation to get everyone rowing in the same direction. Not to mention, top-down support ensures you have the budget and resources to implement the right technologies and deliver the appropriate training for ongoing success.

INSURE YOUR BUSINESS

A strong defense starts with a robust strategy supported by security-first company culture. But in today's environment, it's not a matter of if but when your company becomes a target—even if you check all the boxes.

The right cybersecurity insurance gives you peace of mind by knowing that you won't incur devasting losses if cybercriminals succeed at infiltrating your network and stealing valuable data. The plans cover various consequences arising from cyberattacks. Some may even include hardware damages or business income loss.

Cyber insurance has become increasingly popular among organizations. Its market size is expected to reach $70 billion by 2030 as companies seek to shield themselves from the high cost of attacks not covered by commercial liability policies and traditional insurance products.

A comprehensive policy can help you recover after a data breach and mitigate the costs associated with revenue loss, business disruption, hardware damages, legal fees, forensic investigations, and sending mandatory notifications to affected customers. The coverage could mean the difference between staying in business and shuttering your door.

Cyber insurance is a safety net to mitigate losses caused by a cybersecurity incident and should not be used to replace an effective and robust cybersecurity strategy. Your insurance policy should complement your security processes and tech stack as part of your overall cyber risk management plan.

But getting the right coverage can be challenging for some companies.

Your insurer will analyze your cybersecurity posture to determine the cost and coverage of your policy. A robust data security strategy and ongoing enforcement of your policy are the keys to getting better coverage at a lower price. In fact, without the appropriate security policies and solutions, you may not qualify for cyber insurance.

Partnering for Strength

Now you know how to protect your organization. But do you have the internal expertise and resources to implement the strategies and training and set a solid foundation for getting the right cyber insurance coverage?

Cybersecurity is a multi-faceted discipline. Even companies with a large IT team find it challenging to cover everything internally. Working with the right cybersecurity partner can help you access the latest best practices, strategies, and technologies without the high cost of hiring an in-house team.

So how to find the right partner for your cybersecurity needs?

Your partner should have the knowledge, experience, and resources to help you design and implement an effective and robust risk management strategy. It should provide full services to cover all the security risks that can threaten your business. It should also target strategic areas to improve your cybersecurity posture to help you get the cyber insurance coverage you need.

To address all the pieces essential for keeping your systems, networks, applications, and data secure, you need a partner who has a proven approach to strengthen your defense systematically.

At Compugen, we help our clients improve their cybersecurity posture with our trusted Cybersecurity Lifecycle Framework (CLF.) Our layered security solution is crafted from internationally recognized standards and security frameworks to support the implementation of cybersecurity strategies.

CLF guides companies through the continuous process of detecting, preventing, analyzing, and responding to information security threats. Our professional and managed service capabilities help organizations maintain business continuity, ensure regulatory compliance, and bolster in-house security expertise. We also target critical areas that cyber insurance providers evaluate to ensure you can get the right coverage at the lowest cost possible.

Be ready. Schedule a Vulnerability Assessment.

Schedule Vulnerability Assessment

COMPUGEN

Innovate. Inspire. Impact.