Building Resilience in Security Architecture

Achieving a resilient security infrastructure requires a proactive and strategic approach to cybersecurity.

As cybersecurity risks continue to rise, the most imminent threats are often the most concerning.

But the energy spent reacting to potentially urgent immediate issues can take time away from analyzing and addressing more significant risks within your organization.

For many chief information security officers (CISOs) and chief information officers (CIOs), this is a common problem preventing the necessary focus and emphasis on building a resilient cybersecurity program. With so many cyber issues to react to, it can be difficult to take a step back and look at the wider, long-term view of cybersecurity.

Developing a strategic security solution requires prioritization of investments in alignment with the key business goals and objectives of the organization. This involves technology, people, processes, and policies and requires consistent visibility into your organization's security weaknesses and the threats it faces. True resilience cannot be attained without a strategic and comprehensive approach to security.

Education and Awareness

For many organizations, the creation of a resilient security architecture involves an organization-wide cultural shift. It is imperative that organizations intentionally create a reporting structure spanning business lines that encourages communication and collaboration. CEOs and other senior leaders must be able to digest the information at a high level and drill down for details so they can be made aware of the true level of risk the organization faces. Organizations that take a siloed approach to IT and security don't have a clear pathway for obtaining the necessary investments to reduce risk.

The need for an integrated security architecture is being reinforced by new regulations demanding that company boards become more involved in matters related to cybersecurity. The US Securities and Exchange Commission (SEC) will soon require organizations to disclose their cybersecurity governance capabilities[1], including:

- The board's oversight of cyber risk
- The relevant expertise of those involved
- A description of management's role in assessing and addressing cybersecurity risk
- Management's role in implementing their cybersecurity policies, procedures, and strategies

These stricter regulations are intended to require senior executives to have increased accountability for cybersecurity.

Identifying and Filling Gaps in Resilience

It's important to go beyond merely reacting to imminent threats or performing the simple task of maintaining compliance, and adopt a more forward-thinking, holistic strategy for cybersecurity.

A key first step is to gain an understanding of your highest-value assets and data. Identify your mission-critical assets first, then use that knowledge to apply zero-trust principles to secure them.

To get further ahead of the curve, and begin to fill the most common gaps in modern cyber resilience, it's wise to start by taking the following steps:

1. Use real-life examples to communicate and demonstrate the true level of risk to the CEO. Most business leaders underestimate the severity of cybersecurity issues. To gain the necessary investment required to build greater resilience, inform leaders about the potential impact. Using relatable examples that will resonate directly with executives is the most effective way to achieve this.
2. Understand that compliance alone does not equal resilience. Many organizations have incomplete cybersecurity policies and procedures and don't realize more is needed in today's volatile cybersecurity landscape.
3. Make proactive efforts to gain visibility into everything that is touching your network. Asset intelligence is vital to resilience because you can't secure what you're not aware of.
4. Increase collaboration in your organization to gain value from all the data that is available. Data sharing and analysis across departments can enable better strategic decisions about your current and long-term cybersecurity. Strong reporting flows and data visibility will drive more risk-informed decision-making.
5. Implement the right tools and automated processes to consistently detect, monitor, analyze, and mitigate potential security threats. This will include tools for security information and event management (SIEM), enterprise risk management (ERM), data loss prevention, intrusion detection, monitoring, and so on. Use the power of automation to your advantage.
6. Ensure you have the capacity to retain logs and records appropriately to monitor security, as mandated by industry log retention standards and legal guidelines[2]. Logs serve as valuable resources when investigating potential incidents.
7. While compliance alone isn't enough to build true resilience, it's still an important priority. Keep security policies up-to-date and reinforced, especially as new laws and regulations continue to emerge in this ever-shifting global climate.
8. Invest time to understand the skills required to prepare for and respond to cybersecurity attacks. From there, you can adjust both your hiring strategy and your training of existing staff to focus more on these capabilities.

Benefits of a Comprehensive Approach to Resilience

Developing organizational capabilities to support a resilient security infrastructure can yield many advantages, including:

- Reduced impact of cybersecurity incidents
- Improved business continuity
- Enhanced capabilities to handle incidents quicker and more effectively
- Increased collaboration across the organization
- Optimized reporting flows within the organization
- Protected revenue and profits
- Safeguarded organizational reputation

Knowledge-sharing is imperative as it will help your workforce recognize threats.

Culture Is Crucial to Building Future-Proof Resilience

It is essential to establish a clear, intentional method of informing the relevant stakeholders of the level of risk the organization faces. However, risk awareness should not be limited to the C-suite and senior leadership.

To foster an enterprise-wide culture of safety, vigilance, and proactive behavior, the entire organization should be made aware of the damage cyberattacks can inflict. Knowledge-sharing is imperative here, as it will help your workforce recognize threats and understand the importance of following best practices. Placing some of the responsibility for resilience and security in the hands of the workforce will help you address the challenges discussed earlier.

In today's volatile environment, organizations must go beyond a reactive, compliance-focused approach to actively strengthen their entire organization's security posture. Taking a strategic approach that involves the entire organization is critical to building true resilience in the modern cybersecurity landscape.

[1] "Cybersecurity", n.d., SEC.gov | Cybersecurity.
[2] "NARA Updates Cybersecurity Log Retention Rules ", January 11, 2023, NARA Updates Cybersecurity Log Retention Rules – MeriTalk.

Contacts

Nong Nai, Director
Cybersecurity
nnai@guidehouse.com

Paymon Hashemi, Associate Director
Cybersecurity
phashemi@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 17,000 professionals in over 55 locations globally. Guidehouse is led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit guidehouse.com.

guidehouse.com/services/cybersecurity

@GHTechSolutions linkedin.com/showcase/guidehouse-technology-solutions/

© 2023 Guidehouse Inc. All rights reserved. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. GH-276 WP Building Resilience in Security Architecture