

SIA CYBERSECURITY ADVISORY BOARD

Recommendations for Initiating an Enterprise Cybersecurity Strategy

The SIA Cybersecurity Advisory Board offers these executive-level recommendations as a solid starting point for developing a comprehensive cybersecurity strategy to mitigate business risk. These recommendations are intended to drive discussion within an organization.


There are many other sources of information for in-depth guidelines for developing an enterprise plan; but this document can help to identify areas where more targeted research may be needed within your business.

1. Decide who is in charge of information security.

- a. Whether it is a single point of contact, a team or a department, there must be a leading voice within the enterprise for cybersecurity. While cybersecurity is everyone's responsibility, the training, drilling and consequences for poor cyberhygiene should come from a recognized cybersecurity spearhead entity that is led by the business leadership and informed and guided by security, legal and information technology leadership.
- b. Ensure that information security is a mandate from the operational head, not just a requirement from the security department—and that the mandate is measureable and enforceable and that compliance failures have known and appropriate consequences.

2. Determine organizational risk following a prescribed order. An organization must first identify critical assets, threats to those assets and vulnerabilities, and then quantify risk.

- a. Assets: Determine what you are protecting and know your valuables. Identify the organization's information assets. The purpose of cybersecurity is to protect your critical data, financials and processes from modification, theft or destruction. The corporation must determine which of these internal (and external) dependencies are critical. In retail, it may be customer data; in pharmaceuticals, it may be test results; in physical security, it's customer content, location of critical assets and VIPs—and in the worst case, compromise of employee and/or account holder personally identifiable information (PII), denial of service and full system compromise. It's important to understand that as we move to an interconnected environment where IT, industrial control systems (ICS), personal data systems, physical security systems and healthcare systems are converging. The use of IT devices and methodologies that provide improved operational intelligence, convenience and efficiency must be evaluated as to the value provided and the risks attendant to their implementation.
- b. Threats: While it is tempting to focus on external actors, it's important to note that most threats derive from witting or unwitting insiders who take actions that can lead to a breach. The likelihood that threats will be effective can be significantly reduced through the implementation of a mature,



regularly reviewed and exercised cybersecurity program that minimizes the number of untrained users (unwitting insider threats) and frustrates the efforts of internal and external malicious actors. Threats can be classified in two ways, the distinctions reflecting differences in the scale of potential economic damage and liability:

- iii. **Opportunistic Threats:** These are more common and generally less costly to an organization. They occur when an attacker exploits well-known vulnerabilities to attack unspecified resources. If an attack fails, the attacker moves on to the next victim. Opportunistic attacks primarily target untrained users and poorly configured systems.
 - iv. **Targeted Threats:** A targeted attack typically involves reconnaissance, observation, planning and the development of an attack infrastructure, including command and control elements. These attacks are usually executed by organized groups who focus on a specific target to achieve a specific objective. These attacks may exploit either known vulnerabilities or Zero Days. Targeted attacks are considered more dangerous as a single successful attack often results in a significant loss of value. However, the prolific nature of opportunistic attacks means that they represent a greater overall loss value.
- c. **Vulnerabilities:** Vulnerabilities are reflections of an enterprise's overall security posture. For example, are all systems patched and up to date? Has two-factor authentication been enabled on all servers? Is all internally developed code verified to be written in such a way to mitigate cross-site scripting and buffer overflow attacks? Are all default passwords changed upon installation? Additionally, vulnerabilities can be derived from sources that are external to the enterprise. Have the vendors validated and updated their systems and training? Are the enterprise's cloud vendors certified? How often are they audited? What is the bring your own device policy for employees, partners and visitors? How is it enforced?
 - d. **Risks:** Once threats and vulnerabilities are understood, they can be correlated to identify risks. Risks must then be correlated to specific assets and evaluated as to the likelihood or probability of occurrence. Based on a combination of asset-based valuation and probability of occurrence, a value can be assessed with respect to resources to be allocated to mitigating the risk. Cyber-threats bring risks that can have financial, technical, programmatic and reputational impacts.

3. Implement a comprehensive security framework based on a combination of the probability of cyber-risk realization, asset value and resources available for mitigation efforts.

- a. The framework should include the policies specific to your organization and should be based on national standards, such as those promulgated by the U.S. National Institute of Standards and Technology. Note that compliance is the foundation, not the end point.
- b. The framework should cover the full cybersecurity lifecycle from internal training through incident response. Additionally, implementation must be continually tested to ensure that it is effective, that the organization is resilient, and that response and recovery procedures are well understood. This requires investments in activities like penetration testing, anti-phishing exercises and social engineering red-teaming that covers all staff, including C-suite and IT employees. Engage in regularly scheduled tabletop exercises organization wide.

- c. Ensure that IT policies include vendors to ensure they are aware of and have mitigated all Common Vulnerabilities and Exposures (CVEs) for all their devices within their systems. Most vendors will publish these vulnerabilities and the firmware patches to defend against them, but it's important for integrators and system managers to know where to find regular patches and updates as part of regular, long-term IT management policies.
- d. Initiate good security citizenship programs that reward those individuals and departments that perform well on internal stress tests as well as identify people and organizations in need of improvement. These programs can include bounties for the realization and reporting of cyberthreats to the enterprise. At the same time, sanction departments or individuals that consistently underperform in these areas.

4. Promote security as a culture.

- a. "Minimum Privilege" and "Need to Know" are not just for the government. Segregate sensitive information and use access control systems to enforce "Need to Know" policies.
- b. Monitor, log and audit all access to and operations on sensitive data.
- c. Avoid over-reliance on tools. Tools make some things (like auditing) easier, but processes and training must be kept up to date, tools must have relevant information and ultimately the data produced by the tools should support executive decision making.

5. Obtain legal and financial assurances.

- a. Ensure that executive decision makers are aware of the regulatory and legal requirements with respect to cybersecurity, data breaches and the protection of sensitive information such as PII and protected health information (PHI).
- b. Ensure that the enterprise explores ways to mitigate cyberdamage with insurance policies and other financial mechanisms. Understand what insurance policies are available to indemnify the enterprise against losses resulting from breaches and other cybersecurity incidents? Review coverage regularly to ensure that it is up to date and financially adequate. Insurance vendors often offer incentives to organizations that enforce cyberpolicies and use cyber-risk mitigation methods. Note that these incentives require that mitigations must be applied to all enterprise systems.

The SIA Cybersecurity Advisory Board's mission is to enhance SIA's cybersecurity posture and to guide the industry ahead of potential cybersecurity issues in an increasingly networked world.

Composed of several SIA Board of Directors who are cyberexperts both internal and external to the electronic physical security industry, the SIA Cybersecurity Advisory Board provides educational resources to security industry stakeholders and coordinates with other cyberforward organizations.