IndraStra
www.indrastra.com | ISSN 2381-3652

Fostering Digital Resilience: Strategies for Building Robust Cybersecurity in an Evolving Threat Landscape

indrastra.com/2023/09/fostering-digital-resilience-strategies.html

With relentless technological advancement and digital transformation, safeguarding an organization's digital assets has never been more critical. The cornerstone of an efficient cybersecurity strategy lies in acknowledging the exceptional value certain assets hold for a company. In an age where the digital landscape is continually expanding, striving to provide uniform protection to every facet of an organization's digital realm is simply unattainable. Yet, within this intricate web of interconnected systems and data, trust stands as the bedrock of the digital business model.

Over the past five years, there has been a more than twofold increase in minor and significant system breaches, and these attacks have become more sophisticated and intricate. Although most large enterprises now acknowledge the seriousness of this issue, they still view it primarily as a technical and control problem, even though they admit that their defenses are unlikely to keep pace with future attacks. Furthermore, these defenses often focus on safeguarding business operations' outer boundaries and must be more consistently applied across various parts of the organization.

The upcoming surge in innovation, spanning customer applications, business operations, technological frameworks, and cybersecurity safeguards, should revolve around a business and technical strategy that places paramount importance on safeguarding vital information assets. We refer to this approach as *"digital resilience,"* a multifaceted strategy encompassing identifying and evaluating vulnerabilities, establishing enterprise-wide objectives, and formulating optimal delivery methods. A crucial component of digital resilience involves recognizing and securing an organization's digital assets of utmost importance—these encompass the data, systems, and software applications essential for its operations.

Increasing Vulnerabilities, Limited Resources, and Divergent Priorities

When determining which assets should take precedence in protection, organizations encounter a range of external and internal challenges. Within these entities, business interests, IT departments, and risk management functions often find themselves at odds, grappling with unclear working relationships and conflicting agendas. Consequently, many organizations attempt a one-size-fits-all approach to cyber-risk controls, which can lead to the inefficient allocation of resources—sometimes spending too much in some areas and too little in others. Alternatively, some organizations employ compartmentalized protection measures, inadvertently exposing crucial information assets while concentrating on less critical ones. Moreover, cybersecurity budgets vie for limited funding against technology investments designed to enhance the organization's competitive edge, often introducing new vulnerabilities.

The process of prioritizing assets and risks, evaluating control measures, and formulating remediation plans is time-consuming and labor-intensive. Specialists are tasked with meticulously reviewing a multitude of risks and control mechanisms, assigning ratings based on their individual judgments. Unfortunately, some organizations mistakenly view this work as a mere compliance exercise rather than a vital business process. However, organizations need proper prioritization to deploy their resources effectively to mitigate information security risks. As these risks mount, boards of directors need help to assess the enterprise's overall security or gauge the return on their additional security investments.

Not All Data and Systems Are Equal

The critical assets and their respective sensitivity levels differ significantly across various industries. For instance, in healthcare systems, patient information is typically the most sensitive asset, while information about the functioning of the emergency room may be publicly accessible. The primary risks to these critical data include breaches, theft, and, in some cases, ransom demands, as illustrated by the situation where a top-tier hospital in New Delhi experienced a **ransomware attack.** Hackers demanded a payment of ₹200 crore ($267 million in December 2022) in cryptocurrency to restore control over its systems following a hacker's intrusion.

Conversely, a semiconductor systems design and fabrication laboratory prioritizes safeguarding intellectual property, encompassing everything from system designs to proprietary methodologies. In contrast, a financial services company may require fewer security measures for its marketing materials but faces vulnerability to fraudulent transactions. Additionally, its M&A (Mergers and Acquisitions) database necessitates the highest level of protection available.

Potential attackers can range from individuals to organizations, including criminal syndicates or governments with substantial resources. These attacks can vary in complexity, with objectives spanning from immediate financial gain to gaining a competitive edge or even pursuing geopolitical advantages.

The Cost of Cybersecurity Solutions: The Paradox of More vs. Less

Faced with many diverse threats, organizations often need a clear direction to increase their cybersecurity expenditures.

> A defense contractor may focus on protecting its weapons systems from cyberattacks while failing to protect its supply chain from malware infections sufficiently. This could lead to compromised components being used in critical systems. For example, in 2020, the defense contractor Lockheed Martin was hit by a **cyberattack that compromised the supply chain** of its F-35 fighter jet program. The attack is believed to have been carried out by a Chinese hacking group, which stole sensitive data about the aircraft's design and performance.

> A government agency may prioritize protecting its classified intelligence data while failing to adequately secure its public-facing websites and applications, which cyber criminals could exploit to steal personal data or launch denial-of-service attacks. In 2019, the US government was hit by a ***"major cyberattack"*** that compromised the systems of several federal agencies, including the Department of Homeland Security and the Department of State. The attack is believed to have been by a Russian hacking group, which stole sensitive data about US government operations.
>
> A global pharmaceutical giant might emphasize safeguarding its drug discovery and development data, potentially overlooking the need for robust security measures for its manufacturing facilities and clinical trial information. Unfortunately, this oversight could render these areas susceptible to exploitation by cybercriminals, who may seek to pilfer valuable trade secrets or disrupt essential operations. In 2020, IQVIA, a contract research organization helping manage AstraZeneca’s COVID-19 vaccine trial, was hit by a **cyberattack** that compromised its clinical trial data. The attack is believed to have been carried out by an Iranian hacking group, which stole data about AstraZeneca's experimental cancer drugs.
>
> A healthcare provider prioritizes the protection of patient data while neglecting other areas, such as safeguarding confidential financial data crucial for substantial negotiations and defenses against various internal data-related risks. In August 2023, multiple US hospitals were hit by a **ransomware attack** that disrupted their operations for several days. The attack is believed to have been carried out by the Russia-based Conti ransomware gang, which demanded a $50 million ransom payment. The group is known for using a type of attack called double extortion. In a double extortion attack, the attackers encrypt the victim's files and steal sensitive data. The attackers then threaten to publish the stolen data if the victim does not pay a ransom.

These illustrative cases underscore the need for a unified, enterprise-wide approach to addressing cyber risks. Such an approach should involve collaboration among business, risk, IT, and cybersecurity teams. The leaders of these groups must come together to identify and prioritize the protection of the organization's critical digital assets. Furthermore, addressing cyber risk must incorporate technological enablement through the implementation of workflow management systems. Integrating cybersecurity investment into the business budget cycle and making investment decisions more evidence-based and responsive to changing circumstances is paramount.

An Enterprise-Wide Approach Anchored in Business Priorities

The crucial step is to commence by addressing the business issue, necessitating a holistic assessment of the entire organization, followed by the prioritization of significant risks. This undertaking should be carried out by a cross-functional team representing various facets of the business, including individuals from product development, cybersecurity, IT, and risk management. The primary responsibilities of this team include identifying which information assets require top-tier protection, assessing the likelihood of potential attacks, and devising protective measures.

To be effective, this team must engage leaders from multiple domains, working collaboratively to ascertain what holds the highest importance—a challenge in its own right. The optimal approach for initiating this process is to establish the team's foundation on the agreement that cyber risks will be assessed and ranked with a focus on the overall needs of the enterprise. In essence, the team's primary mission is to serve the enterprise's interests. Critical risks, encompassing the potential impact of various threats and their likelihood of occurrence, will be evaluated based on the risks they pose to the organization.

The following principles can serve as guidance to keep companies aligned when adopting a unified approach to prioritize digital assets and assess risks:

1. Commence with a business-oriented perspective and its value chain. It's essential to base this effort on understanding the business and how it operates within its value chain. Often, the CISO's team, particularly when part of the IT department, initiates the process with a list of applications, systems, and databases and subsequently evaluates risks. However, this approach has two major areas for improvement. Firstly, it may overlook significant risks that arise from the interplay between systems. Secondly, the technical jargon can hinder effective engagement with the business for decision-making regarding changes and investments. By starting with a business-centric approach, the team naturally encourages stakeholder involvement, increasing the chances of identifying systemic vulnerabilities.

2. The CISO must take an active leadership role. In addition to facilitating the business's perspective, the CISO should bring their own insights into the company's most vital assets and risks. Through active collaboration with business leaders and other stakeholders as equal partners in thought, the CISO can establish critical relationships for well-informed investments and resource allocation decisions. This shift may lead to a significant transformation in the CISO's role, necessitating adjustments to their role description and skill set.

3. Concentrate on understanding how an information asset could be compromised. Even if a system's primary purpose is unrelated to a particular information asset, assessing the vulnerability of that system in the event of a breach is crucial.

4. Prioritize over pursuing precise quantification. The team only requires sufficient information to make decisions regarding priority assets. Excessively precise risk quantification is often challenging and doesn't significantly impact the decision-making process when selecting investment options.

5. Dive deeper when necessary. Not all risks demand the same level of analysis. Deeper analyses should be reserved for exceptionally high-impact or complex risks. The team should determine the necessary information to make more informed investment decisions in such cases.

6. Adopt the perspective of potential attackers. During risk reviews and vulnerability assessments, it's essential to broaden the focus beyond just the value of the information to the company and the identifiable gaps in its defenses. Consider the profiles of potential attackers: Who seeks the organization's data? What skills do they possess? Evaluating likely attackers can help identify new vulnerabilities and guide investments to protect the information most valuable to the most capable adversaries.

A Systematically Adaptable Approach with a Well-structured Framework

The enterprise-wide strategy aims to pinpoint and address deficiencies within current control and security systems that impact crucial assets. Based on our experience, the solution will likely involve a comprehensive process, potentially requiring multiple developmental iterations. This process would entail a thorough assessment of numerous assets. An ideal tool for supporting this intricate process would be a workflow system coupled with an asset database, enabling a focus on risk prioritization. An online application that is flexible, scalable, and secure can facilitate ease of use while effectively managing inventory and data mapping, rigorous risk and control evaluations, sector-specific methodologies, and justifications for each risk level. Additionally, this platform can provide in-depth data when the team analyses high-priority assets and gaps, subsequently making recommendations that will shape remediation efforts.

In crafting this approach for clients, McKinsey experts in 2019 outlined the following five crucial stages:

1. Determine and chart digital assets, encompassing data, systems, and applications, throughout the entire business value chain. This process can be expedited by employing a generalized-sector value chain and a shared classification system for information assets, tailoring them to fit the organization's unique context.

2. Evaluate risks associated with each asset, utilizing surveys and executive workshops. This analysis is guided by the asset's significance to the business, effectively identifying its critical components.

3. Identify potential threat actors, assess the accessibility of assets to authorized users, and review the existing controls and security measures safeguarding the systems that grant access to these assets. This step also relies on surveys and workshops similar to step two.

4. Pinpoint areas of vulnerability surrounding the most critical assets (often referred to as *"crown jewels"*) and establish the necessary protective measures by comparing the findings from these assessments using dashboards.

5. Develop a series of actions to mitigate the most critical risks and address control deficiencies. Executing these measures will require a multi-year strategy with established schedules for subsequent evaluations. Following the initial assessment, this strategy evolves into a dynamic document routinely updated to incorporate fresh information, new systems, applications, emerging risks, and their assessments, along with advancements in resolving known vulnerabilities.

Conclusion

The above-suggested process fosters cyber-risk clarity, addressing stakeholders' fundamental inquiries: What are our inherent information-related risks? Where are the vulnerabilities in our organization? What is the remaining exposure, how extensive is it, and in which areas? Which remedial actions should we give precedence to? How can we determine the effectiveness of our efforts? The notion of trading information risks can be delineated by considering the perspective of the value put at risk across the entire company. This facilitates discussions on information security risks at the executive and board levels. It enables a transparent examination of the risks they are willing to tolerate and the reasons behind these decisions.

The outcomes of this process influence budgeting and investment choices, ensuring alignment with regulatory requirements and shareholder expectations. Costs are effectively managed by concentrating investments on safeguarding the most sensitive digital assets while enhancing the organization's digital resilience. Additionally, this process can aid organizations in integrating digital resilience into their day-to-day operations by establishing periodic assessments to highlight emerging trends and identify new vulnerabilities. Subsequently, risk managers can formulate new initiatives that prioritize the global needs of the enterprise.

NOTE: *Organizations characterized by advanced digital capabilities, such as financial services, manufacturing, and healthcare, stand to gain the greatest advantages from this methodology. They grapple with the formidable challenge of safeguarding their utmost critical resources without impeding the progress of business innovation. Striking this equilibrium necessitates collaborative efforts from various organizational domains, including business operations, IT, risk management, and others.*

About the Author:

Rahul Guhathakurta (ORCID: **0000-0002-6400-6423**) is a strategic management consultant. A primary investor in IndraStra Global — a US-based publishing company.