SECROM

RISK MANAGEMENT

Transitioning from security awareness to a risk-conscious enterprise

RISK MANAGEMENT

TRANSITIONING FROM SECURITY AWARENESS TO A RISK-CONSCIOUS ENTERPRISE

> “
>
> Every choice that organization makes explicitly or implicitly requires risk management.
>
> But the increasing volatility, complexity and ambiguity of the world leaves considerably less room for error.
>
> ”

Today, managing risk, which is both an art and a science, lies at the center of our economy and business affairs. Every choice that organization makes explicitly or implicitly requires risk management. From day-today operational decisions to the fundamental trade-offs in the boardroom, dealing with risk while making choices is a part of decision-making.

Our understanding of risk and our practice of enterprise risk management have improved greatly over the years. But the increasing volatility, complexity and ambiguity of the world leaves considerably less room for error. Stakeholders are seeking greater transparency and accountability for managing risks while demanding active pursue of new opportunities. Even success bears a risk downside; for instance, managing growth, scaling operations, sustaining the quality standard, etc. Organizations encounter challenges at all times and at all

maturity stages that impact reliability, relevancy, trust, and other important aspects.

The optimal risk management cannot be achieved without effective communication and fundamental changes in enterprise culture. Creating a true enterprise risk management culture requires stakeholders responsible for security, compliance, planning and business development, continuity, operations, support, and other critical business functions to follow the industry best practices when it comes to creating a risk conscious enterprise.

> “Nevertheless, it is common that benefits of risk management are not fully understood and even less understood are the critical processes required for effective and efficient risk management.”

Companies, depending on the business culture, business maturity and regulatory requirements, designate individuals and procure services and technologies to manage security, business continuity, provide disaster recovery, compliance, and other functions with sole purpose to manage risk. Nevertheless, it is common that benefits of risk management are not fully understood and even less understood are the critical processes required for effective and efficient risk management. Even more so, since the industry offers a number of well-developed and seasoned risk management frameworks aimed at organizations with different risk management needs; for instance:

- CNSS Policy 22, developed by the Committee on National Security Systems (CNSS), and it provides guidance to organizations that handle data critical to the national security.

- NIST Special Publication 800-39, developed by the National Institute of Standards and Technology (NIST), and provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems.

- Enterprise Risk Management—Integrating with Strategy and Performance risk management framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and it focuses on the importance of considering risk in both the strategy-setting process and in driving performance.

- Managing for Enterprise Security is another risk management framework developed by the Carnegie Mellon University, enabling organizations to manage security in a systematic, predictable, and adaptable way

that fits their unique strategic drivers regardless of which practices, standards, or guidelines they choose or are required to use. The framework approaches security on an organizational scale.

The apparent difference between said frameworks is their application. The CNSS Policy 22 is intended for protecting National Security Systems (NSS) that generally require more stringent security because their compromise, for instance, may cause exceptionally grave damage to the national security. Other frameworks have in mind less stringent security needs since they are intended for organizations that do not handle critical national security functions. The tradeoff is usually that such requirements are easier to implement and it is less expensive to maintain compliance—in other words, the value of information does not warrant the cost. Therefore, different policies and frameworks are required and one could be no better than the other, depending on the organizational mission, function, and specific requirements.

> “
>
> The apparent difference between said frameworks is their application.
>
> All the above frameworks provide a structured approach for monitoring and managing risk in an enterprise.
>
> ”

All the above frameworks provide a structured approach for monitoring and managing risk in an enterprise. The frameworks, however, differ in methods and the level of detail. For instance, the COSO's Enterprise Risk Management—

> “
>
> A cultural change is required to achieve enterprise wide understanding of security, compliance, continuity and privacy—and their impact on risk and risk management.
>
> ”

Integrating with Strategy and Performance framework focuses on enterprise-wide risk management, identifying five integrated components: governance and culture; strategy and objective-setting; performance; review and revision; information, communication, and reporting. These components accommodate different viewpoints, operating structures, and enhance strategies and decision-making.

The frameworks are generally similar in their approach—integrated, top-down risk management for supporting enterprise missions and functions; and all require that risks be defined and quantified, for example, using a mission-impact assessment of risk.

A cultural change is required to achieve enterprise wide understanding of security, compliance, continuity and privacy—and their impact on risk and risk management. It is often not a step-by-step process, but a number of parallel systematic efforts, requiring consistent enterprise-wide application of a number of best practices, including a risk management framework. One of the key challenges that organizations face is that such change requires that risk managers earn the trust of many stakeholders, convincing them that understanding risk will benefit the organization, as well as them personally and professionally.

The transition from security awareness to a risk-conscious culture eventually creates a qualitative change in the organization’s security posture. Extending risk management beyond regular security measures requires a comprehensive change in corporate culture and organizational and individual behaviors. Effective risk management also requires that line of business managers that own systems and data take ownership of the associated risks. A risk aware organization must develop a competence that would help the organization to understand and monitor risks, as well as develop and implement an organization-wide, comprehensive risk management strategy to effectively and efficiently mitigate organizational risks.

CORPORATE HEADQUARTERS

1895 Preston White Drive
Suite 101
Reston, Virginia 20191

EMAIL: info@secrom.com