Managing Emerging Risk in the Modern Enterprise

Puneet Mehta, VP and Chief Technologist, Practice Lead - GRC, Technology

SDG

[technology + passion] - risk

Managing Emerging Risk in the Modern Enterprise

Gaining visibility and control on the multitude of internal and external risks is one of the top priorities of corporations today. With a recent jump in regulatory mandates and increasingly active shareholders, many organizations have become sensitized to identifying areas of risk in their business: whether it is financial, operational, IT, brand, or reputation related risk. These risks are no longer considered the sole responsibility of specialists - executives and the board demand visibility into exposure and status so they can effectively manage the organization's long-term strategies. As a result, companies are looking to systemically identify, measure, prioritize, and respond to all types of risk in the business, and then manage any exposure accordingly.

"To have any hope of protecting your organization's critical assets, both the business and security teams need to understand where your information lives, inside or outside.

Most IT organizations struggle with ensuring visibility and control on IT risks due to the complexity of IT environments in large corporations. It is a challenge to ensure consistency in measuring and managing risk on an ongoing basis continually assessing the impact of IT risks in the disparate areas of the organization. Moreover, linking IT risk and compliance life cycles together is critical as a mechanism to interpret control failures within the context of overall business risk and performance, allowing for more effective prioritization and allocation of resources to address IT control deficiencies.

To have any hope of protecting your organization's critical assets, both the business and security teams need to understand where your information lives, inside or outside. Identifying what your organization classifies as its most important information and applications, where they reside and who has, or may need access to them will enable the business to understand which areas of the security program are most vulnerable to attack.

After understanding where information resides, assessing the threat landscape and developing predictive models can highlight your real exposures. The following represent some of the more relevant threats that today's organizations face:

Internal threats. The recent Snowden case is an excellent example of malicious attacks from within. But the threat doesn't stop there. Insider threats are even more prevalent than outsider threats, either accidentally or intentionally. Organizations have failed to understand the importance of internal threats for far too long – this risk will only increase if it isn't addressed now.

Cloud computing. Lately, organizations are increasingly turning to cloud computing providers because of several potential advantages, including significantly less initial investment, fewer skilled internal IT resources and lower operating costs. However, for all the intended benefits, cloud services raise security risks and regulatory challenges as personal information and intellectual property potentially cross borders. Since not every country has stringent rules around information protection, security and privacy, the ability to adhere to many of the regulations is daunting. Additionally, concerns are being raised regarding the core security practices that the cloud providers follow.

Mobile devices. The technological advancement in mobile devices has dramatically altered the flow of information in and out of organizations. Employees commonly use media-enabled smartphones and tablets – often owned by the individuals – to access company information anywhere and anytime. While this may increase employee productivity, it raises a number of threats and risks. While some organizations may think that banning use these devices is the answer to reducing risk, but in reality, such restrictions may only increase their use. The real answer is to enable them with the right security protections.

Cyber-attacks. While organizations for so long have been dealing with opportunistic cyber-attacks for years, many now find themselves the target of more sophisticated and persistent efforts. The attacks have become more objective and focused often lasting over a long period of time and until the desired target is obtained. The attacks are designed to remain hidden to acquire as much sensitive information as possible and they leave no or few signs of breach. In our experience, the ones at greatest risk are information-intensive entities or organizations with intellectual property. Unfortunately, many organizations have no idea they are compromised until it is too late.

Social media. The use of social media is now more popular than ever and as the technology evolves, the difference between personal and professional interactions will increasingly blur. Users need to be made aware as to how their use of social media could jeopardize the organization's security and success. Unfortunately, information loss is often an unintended consequence of an employee's behavior. Organizations need to implement enterprise-wide awareness programs for employees on their personal responsibility for protecting the organization's intellectual property. Ultimately, information security is everyone's responsibility.

So how can organization's deal with these emerging risks?

Know your program's weaknesses and get ahead of both the internal and external threats to your organization's network, information and brand:

- **Define the organization's risk appetite.** An organization's risk appetite depends on its risk culture. By effectively understanding an organization's culture, you can align its potential exposure to the risk it is willing to take.
- **Identify the most important information.** It's not good enough to make an educated guess. Identify, inventory and prioritize the information's value. Placing a value on information based on the organization's broader business strategy will enable you to prioritize the assets that matter most.
- **Assess the threat landscape.** Today's security assessments need to focus on knowing where the information resides, who has or needs access to it and how it could be compromised. Understanding how information is used helps to identify the threats against it. For example, a national health care organization recently sent people into the field to determine how employees and third-party suppliers were using information. By actually seeing how information was shared, the organization could identify areas of security risk and take appropriate action.
- **Develop predictive threat models.** Once your security team identifies the areas of risk, it is useful to run through threat scenarios. These exercises help you understand and quantify the probability of a breach occurring in each specific risk area, the size of the vulnerabilities and the level of damage a security breach could cause.
- **Determine appropriate protection mechanisms.** Use the threat model that has been developed to apply controls commensurate with the level of risk.

Conclusion

In today's highly interconnected business environment, information security and Risk management can no longer be an isolated endeavor, and it must be the responsibility of an entire business ecosystem or value chain.

About SDG

SDG is a leading provider of technology, consulting and risk management solutions to strengthen enterprise businesses while managing IT risk. We focus on six practices: Risk and Security; Identity and Access Governance; Digital Collaboration; Quality Assurance; Mobility and Cloud. In addition we offer a GRC solution, called TruOps, to manage enterprise IT risk and compliance.

"SDG helps enterprises realize their dreams by helping them develop, manage and deploy solutions with acceptable risk."

For over two decades, SDG has enabled enterprises to realize their dreams by helping them develop, manage and deploy solutions with acceptable risk. We combine technology, thought leadership and a relentless passion for customer success. SDG partners with enterprise brands, but we specifically focus on mitigating client IT risk. Our ultimate goal is to help enterprises realize the opportunity of technology, increase innovation, improve speed-to-market and maximize returns on investment.