TOPICS COVERED
// Data Security & Risk

LOST IN A CYBER SECOND

Protecting Information & Mitigating Cyber Risk

Written by Pamela Passman

Imagine this scenario: *A Wall Street Journal* reporter is on the phone and wants to know how a trove of your company's confidential data—including customer credit card information, employee social security numbers, confidential emails, and future product plans—ended up on the dark web. What steps do you take? What notifications need to be made? Who do you bring into the room to address this issue?

Each day, companies around the world are facing this crisis scenario in a variety of ways. Cyber threats are on the rise, and risks will inevitably increase exponentially with the surge of new access points created by internet-connected devices (the "Internet of Things"), the advance of trends such as the digital supply chain and artificial intelligence, and ongoing vulnerabilities identified in silicon chips, software, and systems.

At the same time, regulations around data protection and cybersecurity are increasing. Most notably, the European Union (EU) General Data Protection Regulation (GDPR), effective on May 25, 2018, extends the scope of the EU data protection law to include all foreign companies processing data of EU residents. Among other requirements, companies must appoint a data protection officer and report to the Supervisory Authority within 72 hours after becoming aware of a data breach.

How do you know if your organization is doing enough to mitigate risks? As a starting point, here are five questions to consider.

1. Who is responsible for information security?

Cybersecurity is no longer the sole domain of the Chief Information Officer (CIO) or information technology (IT) department. Breaches—and the threat of attacks—touch on many stakeholders throughout an organization, from legal teams to risk managers, communications, IT, and human resources. Given new and existing regulations around cyber breaches, legal and compliance professionals have an important seat at the table and are increasingly playing a visible role in their organizations on cybersecurity. Before a breach ever happens, you should have already assembled a cross-functional team involving those who can help to ensure controls are in place, legal requirements are being met, and there are communications and training for employees and other insiders about their role in promoting effective cybersecurity.

What information is most important and, if misappropriated, would be most damaging to the organization?

2. What are your risks?

Consider the possibilities and potential impacts of losing critical corporate data. What information is most important and, if misappropriated, would be most damaging to the organization? In many companies, cybersecurity is treated as one element of the broader enterprise risk management (ERM) landscape. This risk-based approach is a good one and helps to focus resources on top priorities. As part of this process, consider the threat actors—from nation states, to malicious insiders, criminal organizations, competitors, and hacktivists—who are most likely to value your confidential information for competitive or political gain.

3. Where are top information assets located and what controls are in place?

For many companies, identifying sensitive information is a challenge. Do you have a process to identify and categorize sensitive information, and to know where these key assets are located and who has access to them? Is access given on a need-to-know basis? Are there policies and procedures specific to protecting this information?

4. Do all insiders know their roles and expectations about protecting sensitive information?

Insiders are the most likely source of a cyber breach, and they are also your first line of defense. Many companies are accomplished at informing and training employees on cyber hygiene, but then they fall short when it comes to other "insiders"—contractors, consultants, business partners, and other third parties. Anyone with network access should understand your company's policies about information security and at a minimum should be trained on the most common ways breaches can occur. There should also be systems in place when onboarding and offboarding employees, contractors, and others. In some cases, contractors have used old credentials to access corporate systems and steal information after a project is completed. To avoid this risk, you must have a contract in place and a sywstematic way to terminate network access at the end of employment.

5. Does your cybersecurity approach align with external standards and best practices?

Cybersecurity is now considered a top risk for companies and, as a result, a key focus of boards and the C-suite. For legal, IT, and compliance teams reporting to senior management, a useful approach is to frame communications about the maturity of company cybersecurity programs in the context of established guidance and standards. The NIST Cybersecurity Framework—a voluntary, flexible approach consisting of standards, guidelines, and best practices to manage cybersecurity-related risk—is gaining momentum around the world. It defines 98 categories of "people, processes, and technology" controls that should be in place. The approach is risk-based and can be adapted to a company's risk profile and business priorities. The International Organization for Standardization (ISO) 27001 Standard is also widely used (and is referenced in the NIST Framework). It specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system. The NIST Framework and ISO 27001 are designed to be applicable to a range of organizations. Mapping to the NIST Framework or other established standards offers a way to validate a company's cybersecurity approach and also measure maturity across an organization in a consistent way over time. Boards and senior management are increasingly aware of the NIST Framework as leading guidance for information security.

Sensitive corporate information is at greater risk than ever before. Asking the tough questions and taking a proactive approach to addressing the "people, processes, and technology" elements of cybersecurity won't necessarily stop a breach from occurring. However, it will help to mitigate impacts and foster resilience if disaster does strike.

Resources

ADDITIONAL RESOURCES AVAILABLE FOR DOWNLOAD AT WWW.CREATE.ORG:

- *Overview of the NIST Cybersecurity Framework: An eBook for the C-Suite, Boards and Others Involved in Protecting Confidential Corporate Assets*
- *The Importance of Cybersecurity for Trade Secret Protection: Developments in Trade Secrets Cases and the Growing Role of the NIST Framework*
- *Cyber Risk: Navigating the Rising Tide of Cybersecurity Regulation*
- *Protecting Trade Secrets from Cyber and Other Threats*
- *Safeguarding Trade Secrets and Mitigating Threats*

Author Biography

Pamela Passman *is President and CEO of the Center for Responsible Enterprise And Trade (CREATe.org) and its wholly owned subsidiary, CREATe Compliance Inc., two entities with a common mission to promote leading practices in cybersecurity, intellectual property (IP) and trade secret protection, and anti-corruption. Passman is also co-founder of The Cyber Readiness Institute, launched by CREATe.org and The Center for Global Enterprise to enable the private sector to better address cybersecurity risk management across value chains.*

Prior to founding CREATe in 2011, Passman was Corporate Vice President and Deputy General Counsel, Global Corporate and Regulatory Affairs, Microsoft Corporation. From 2002 to 2011, Passman led Microsoft's global public policy work and regulatory compliance across a range of issues, including privacy, security, and cloud computing issues.