WeirFoulds LLP

WeirFoulds Technology Insights: "Compliance and Security Standards"

August 9, 2022

By James G. Kosa, Cassie Chaloux

Cybersecurity is one of the greatest threats facing modern businesses. As a result, it is important that organizations monitor, regularly assess, and audit compliance with their cybersecurity strategy. Choosing a cybersecurity strategy that works best for your business and implementing and maintaining the appropriate IT Security Standard can be key to saving you and your business future headaches.

An Introduction to Compliance with Security Standards

Organizations face a variety of sources of cyber risk including expanding technology, evolving business models, data growth, and motivated attackers. There are three main lines of defence to these risks:

1. i) **business units**: Business units integrate risk management into day-to-day decision making and operations. This can include something as simple as opening emails from unknown senders.
2. ii) **information and technology risk management leaders**: Information and technology risk management leaders establish governance and oversight, monitor security operations, and act as needed under the direction of superiors, such as a chief information security officer.

iii) **internal/external audits**: internal/external audits are independent reviews of performance and measures. Audits play an integral role in assessing and identifying opportunities to strengthen enterprise security.

Together, these tools can make a world of difference in your business' cybersecurity presence and strategy.

IT Security Standards

There are a variety of IT security standards that have been developed by independent associations, industry members, and governmental agencies. Organizations can adopt these standards to ensure they maintain a minimum level of security.

The ISO 27001 is an example of a standard developed by an independent association. It details specifications of an Information Security Management System (ISMS) which organizations can implement to improve the state of its information security. Certification to the ISO 27001 is recognized worldwide as an indication that a business's ISMS is aligned with information security best practices. The ISO 270001 can also be used by internal and external parties to assess an organization's ability to meet the organization's own information security requirements.

The PCI Data Security Standards (PCI DSS) is an example of a standard that has been developed by industry members. The PCI DSS applies to all entities that store, process, and/or transmit cardholder data, and it consists of steps that mirror privacy best practices. For example, PCI DSS involves installing firewalls to protect cardholder data, encrypting cardholder data in public networks, protecting

systems against malware by regularly updating anti-virus software, regularly testing security system and processes, and more.

The National Institute of Standards and Technology (NIST) is an example of a standard developed by a governmental agency (the United States Department of Commerce). The NIST framework provides voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risks. It is composed of three primary components: i) Core; ii) Profiles; and iii) Implementation Tiers. The Core framework consists of five current and continuous "functions". These include: i) identify ii) protect iii) detect; iv) respond; and v) recover. It is important to note that NIST does not provide certification, but merely provides guidance for how an organization can manage and reduce risks that the particular business can then adapt.

The purpose of these standards is to allow an organization to point to objective requirements demonstrating compliance. This makes it possible for an organization to say that it is meeting industry standard and can also be a defence to claims of negligence when handling data and maintaining security. Standards also inherently evolve overtime, so referencing a standard allows an organization's obligations to evolve in step with threats the industry identifies.

Audits

One of the ways organizations identify how they comply with a standard, or security obligations under a contract, is by allowing for the performance of an audit.

Generally, cybersecurity audits focus on cybersecurity standards, guidelines, and policies. The focus is on ensuring that all security controls are optimized and that all compliance requirements are met. The typical areas that an audit evaluates can be broken down into five key components: i) operational security; ii) data security; iii) system security; iv) network security; and v) physical security.

Audits may be completed by internal or external auditors, and the choice between the two will depend on your business' needs. If your business chooses an internal audit, you should confirm that the internal audit function regularly reviews cybersecurity controls, that it is up to date on the latest developments, and that it includes issues featured regularly on its agenda. If your business chooses an external auditor, the wealth of experience that external auditors bring can be a valuable source of information for your business on cybersecurity issues.

Regardless of which form of audit your business chooses, you may also want to consult with external cybersecurity specialists who can review the business's security and privacy programs, identify, and confirm that weaknesses have been addressed, and provide a benchmark for your business in relation to your competitors.

How often an IT security audit needs to be scheduled will depend on a variety of factors, including the size of the business and the complexity of its IT system. Some businesses prefer to schedule audits on a monthly or quarterly basis, while others schedule audits semi-annually. It is typically recommended that an IT security audit is performed at least twice a year.

Key Takeaways

Regardless of which IT Security Standard your business chooses, it is important to conduct frequent audits, and to be aware of your business' vulnerabilities. Doing so can guard against possible attacks and optimize your business' opportunities for growth.

WeirFoulds Technology Insights is a monthly issued newsletter that discusses the meaning of cybersecurity, the privacy frameworks that mark the boundaries of the cyber domain, the basic of technology contracting and the types of contracts to consider, security compliance, security reporting obligations and mechanisms, and the dark web. To receive the email newsletter, click here and subscribe to our "Intellectual Property and Technology" list.

The information and comments herein are for the general information of the reader and are not intended as advice or opinion to be relied upon in relation to any particular circumstances. For particular application of the law to specific situations, the reader should seek professional advice.

For more information or inquiries:

James G. Kosa

Toronto
416.947.5043

Email:
jkosa@weirfoulds.com

James Kosa is a partner at WeirFoulds with a practice focused on information technology and intellectual property law. He is the Co-Chair of the firm's Technology & Intellectual Property and Privacy & Access to Information Practice Groups, and Co-Chair of the Blockchain and Digital Assets Practice Group.

Cassie Chaloux

Toronto
416.619.6286

Email:
cchaloux@weirfoulds.com

Cassie is an Associate in the Construction Practice Group at WeirFoulds.