CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

On the Radar

Cybersecurity Bulletin for Directors

This Cybersecurity Bulletin provides insights into five current security and privacy themes directors should be aware of in 2019.

Theme 1: Cyber Threats to Operational Technology (OT) and the Internet of Things (IoT):

The threats to Information Technologies (IT), such as customer data theft, are well publicized. However, directors should understand that many parallel cybersecurity threats are facing their companies' operations as well.

Manufacturing lines, power generators, warehouse climate controls, Supervisory Control and Data Acquisition (SCADA) systems, and transportation assets are all examples of OT assets, systems, and networks. Years ago, many OT networks were isolated (air-gapped) and not connected to IT networks. But to operate more efficiently and effectively, these OT environments have become increasingly digitized and connected, which makes them susceptible to cyber attacks. As IT and OT systems and networks converge, hackers are better able to navigate digitally through organizations.

Because many companies are dependent on OT in unexpected ways, threats may blindside directors. In the banking industry, for example, algorithm-driven systems such as trading platforms and compliance programs could be susceptible.

Below are some statistics collected from PwC's Global State of Information Security® survey 2018:

- Few respondents say their organizations plan to assess risks to the Industrial Internet of Things (IIoT) across the business ecosystem.

- The ownership of responsibility for emerging technologies like IoT, IIoT, and OT security varies with the organization:
  - 29% of companies give OT security to the Chief Information Security Officer (CISO)
  - 20% to the engineering staff
  - 17% to the Chief Risk Officer.
- To support internal business operations:
  - 52% employ a CISO
  - 47% employ dedicated security personnel
  - 45% employ a chief security officer.
- Cybersecurity executives are still absent in many organizations.

These statistics highlight the reality that many organizations do not have a clear line-of-sight as to which systems are likely to be compromised, the operational impact, or who is responsible.

Cyber Threats: Tips for Directors

Attacks on OT systems can cripple an organization's core functions. Shutting down an electrical grid, blocking the ability to process global consumer purchases, terminating a manufacturing plant, and compromising mining operations are all real examples of OT hacks in recent years.

Adequate cybersecurity controls are lagging within many OT environments. Hackers are aware of this gap and are targeting OT infrastructures at growing rates. The following are steps directors can take to provide effective OT governance:

- Ask the management team how they are identifying and mitigating OT risks.
- Look for evidence that cybersecurity teams possess, or acquire, specialized OT security specialists who can design effective operation security programs.
- Confirm that management creates accountability for cybersecurity of OT, IIoT and emerging technologies.
- Certify that management teams build and maintain an inventory of their critical OT assets along with a network diagram of their OT networks.

Theme 2: Mandatory Disclosure of a Cybersecurity Breach

According to the Office of the Privacy Commissioner of Canada, as of November 1, 2018, organizations subject to *The Personal Information Protection and Electronic Documents Act* (PIPEDA) will be required to:

- report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm (RROSH) to individuals
- notify affected individuals about those breaches
- keep records of all breaches.

This will require changes to existing breach management and privacy practices for affected organizations. Non-compliance could result in negative regulatory impacts, unwanted media attention, proactive investigation/review of breach records by the regulator and fines of up to $100,000. These costs are in addition to any remediation steps taken after the breach. (According to the third annual report conducted by the Ponemon Institute, the average cost of a data breach to Canadian companies in 2017 was $5.78 million.) Having a fully functional incident response (IR) process in place can reduce the overall cost and reputational impact of a breach.

The quantity and sophistication of cyber attacks is increasing. To prepare an adequate response, organizations are developing cyber breach IR teams made up of many stakeholders, including:

- business continuity management
- security (IT and OT)
- legal counsel and regulatory compliance
- customer and public relations
- operations
- human resources
- government relations (for attacks from foreign nation states)
- third-party cyber-breach specialists.

Proactive Steps for Directors: Breach Disclosure

- Be familiar with your organization's disclosure responsibilities.
- Confirm management has an overall IR plan along with specific cyber "playbooks" to respond to scenarios such as ransomware, loss of operations, data loss, etc.
- Inquire whether your organization has an internal breach-response team in place, along with an agreement with third-party companies for support in the event of a breach.
- Confirm that the public/investor relations department is prepared with an approved media release to help quickly mitigate the reputational impact of a breach.
- Confirm that management performs tabletop exercises annually (at a minimum) to ensure all stakeholders are well versed in their duties.
- Be satisfied that management is capable of effectively restoring lost data and corrupted systems from stored backups within desired timelines.
- Additional information is available from the Office of the Privacy Commissioner of Canada at www.priv.gc.ca/en/privacy-topics

Theme 3: Third-Party Cybersecurity Risk

Consider the number of external business relationships your organization relies upon to be efficient and competitive. Which of these have access to your organization's data, networks, applications, or operations that represent a potential threat to your security? The answer may be surprising. Contractors, logistics companies, building facilities, telecommunications, and data storage centres are all examples.

A notable number of cyber breaches originate by first compromising suppliers or contractors and then migrating to the larger clients they serve. Attackers know that smaller service companies (who often have access to their client's networks) may lack rigorous security controls. By compromising these easier targets, attackers can gain access to the larger client domains. In 2014, the large U.S. retailer Target Corporation was breached. The attack originated with a small air conditioning contractor's IT system where hackers penetrated the smaller company in order to access Target. The resulting breach caused an estimated $162 million in damage to Target.

The topic of third-party security risk has become very active in the past year.

Key Questions Directors Are Encouraged to Discuss with Management

- How can management teams assess and mitigate the cyber risk presented by third parties?
- How can the organization assure external parties are adhering to their contractual security obligations?
- If the organization experiences a breach by way of a third party, where will the legal liability and responsibility reside?

Directors are advised to inquire whether management teams have implemented the following controls to mitigate third-party cybersecurity risk by establishing:

- contracts with third parties that identify the obligations of each party to defend against breaches, and the liability related to non-compliance with the agreement. (Bear in mind that, despite all reasonable efforts to prevent a cybersecurity breach, compromises can still occur. Liability may not be present in some cases.)
- an assurance process to validate that contractual security agreements are being upheld. (The ability to receive desired levels of assurance may vary by third party.)
- the minimum acceptable level of access to be granted to third parties (i.e., providing access only as required).

Theme 4: Talking to the Board about Cybersecurity Risk

How can cybersecurity leaders effectively articulate security strategies and decisions to their board of directors? And conversely, how can the board better understand the organization's technology and cybersecurity strategy?

Discussing a technical and complex cybersecurity plan with boards can be challenging. In fact, describing the intricacies of network segmentation models to a board is both unnecessary and unadvisable. If we pause to understand a director's governance role, then an alternative way of discussing cybersecurity emerges.

The solution is to address "cyber risk reduction" rather than discussing technical approaches or solutions. Reviewing how much cybersecurity risk the organization currently has and agreeing on target thresholds of cyber risk will result in very practical discussions.

EXAMPLE

Directors could ask for an overview of the current level of risk of data loss. Management would respond with a risk-assessment report describing the likelihood and impact of a cybersecurity breach that would result in a meaningful loss of data. They would also communicate a desired risk-target level (e.g., move the risk from high, to medium-low on the assessment scale). Then it would be the CISO's role to give the board comfort that appropriate security controls could be applied to lower the risk to desired levels. If the board desires more validation, then management could engage third parties to review the CISO's plan to confirm that sound technical decisions are being made. In this way, the discussion focuses on risk and avoids complex technical language.

The above risk dialogue, however, does not absolve directors of the responsibility for their own cyberliteracy. Directors should continue to educate themselves on cybersecurity (and privacy) topics. Boards are also advised to have at least one director with a deeper knowledge of the subject. This will facilitate effective cyber-risk discussions and oversight. The audit committee is one example of a board committee that needs to be closely connected to the cyber-risk assessment. Its oversight responsibilities for securities filings and required disclosures make it clear that committee members must understand both the cyber risks and the resulting regulatory requirements.

Boards should adopt a cybersecurity governance framework to provide a taxonomy and process for assessing cyber risk within their organization. These frameworks raise questions and topics that can adequately cover the important areas of cybersecurity risk. (PwC's Board Cybersecurity Governance Framework is one example of such a framework.)[1]

1 Board Cybersecurity Governance Framework, PwC: www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf

EXAMPLE

One cybersecurity risk transferal technique is cybersecurity event insurance. In recent years, insurers of corporate cyber risks have heightened their requirements for insurance. Directors should seek independent advice regarding the structure and scope of their organization's cyber insurance coverage. Additional insights will be provided in the upcoming CPA Canada "20 Questions Directors Should Ask About Cybersecurity" publication.

Theme 5: Convergence of Cybersecurity and Privacy

Organizations have traditionally managed cybersecurity and privacy processes separately. Cybersecurity has typically been led by technical teams, while privacy has been the domain of the legal, compliance, and human resource departments. Collaboration between security and privacy teams has often been ad hoc.

More recently, however, cybersecurity threats and breaches have required these teams to collaborate more actively. The problem is that the language of privacy law and policy are distinct from the technical language spoken within IT departments. Only a few organizations have created integrated privacy and security teams. However, the need for integrated policies, processes, and resources is growing as compliance requirements increase.

At the end of September 2018 the United States, Canada and Mexico finally concluded the Canada-United States-Mexico Agreement (CUSMA – also known as USMCA). This may significantly impact current cybersecurity and privacy programs. Chapter 19 of the Agreement sets a goal of creating a continental free-trade zone in digital goods and services. This places heavy emphasis on the development of privacy regulation and seeks collaboration among the three countries in the areas of personal information protection and also cybersecurity. Notably, it largely prohibits data localization requirements and favours a free flow of cross-border data.

Challenges and opportunities for organizations operating in North America (and globally) include:

- strengthening cybersecurity capabilities to protect personal data
- facilitation of "privacy rules flow with the data," which requires that recipient of foreign-country data to apply the originating rules for data use and protection when data is received; this will motivate all three countries to harmonize data privacy laws where possible
- leveraging recognized data management frameworks to create confidence in customers and regulators, and to fully leverage a free market in digital goods and services.

In light of the above, organizations should consider it a leading practice to establish a privacy and security steering committee with the mandate to create policies and processes that consider both the legislative and technical requirements to store, transmit, and dispose of data effectively.

For greater insights on this topic, watch for CPA Canada's "20 Questions Directors Should Ask About Cybersecurity" publication launching in Fall 2019.

About the author: Richard Wilson is a Cybersecurity & Privacy partner with PricewaterhouseCoopers LLP in Canada. Richard specializes in cybersecurity and privacy governance for boards. Richard can be reached at **richard.m.wilson@pwc.com**