Cyber risk

what should you consider?

Evolving effects of cyber risk

The frequency and severity of cyber attacks are increasing all the time. In January 2019 alone, the breach identified as Collection #1 revealed that 773 million records were exposed.[1]

Cybersecurity is not just an IT issue or a matter that results only in information loss. It affects a company's reputation and has resulted in theft of protected or sensitive information – including intellectual property, credit card and personal information – and the disruption of computer-controlled operations or access to online systems. A single breach can be very costly to fix.

Cybersecurity is a broad business risk that affects most companies. The 2019 Global Risk Report issued by the World Economic Forum includes cyberattacks among the top 10 most concerning global risks.[2]

As attacks continue to evolve, so will their effect on the organization as a whole.

While many of the recent highly publicized attacks do not appear to have been directly targeted at financial systems, the access gained by the attackers enabled them to:

- Manipulate or modify financial records, such as billing/cost, interest rates
- Modify key automated business rules
- Modify automated controls relied upon by management

In the first half of 2018, 3,353,172,708 data records were compromised – an astonishing 214 records per second. It was found that 65% of these cases were related to identity theft incidents.[3]

Starting on 1 November 2018, the *Canadian Personal Information and Electronic Documents Act* (PIPEDA) was amended to make data breach notification mandatory under certain circumstances.[4]

[1] The 773 Million Record "Collection #1" Data Breach, **https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/**.

[2] The Global Risk Report 2019, World Economic Forum, **http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf**.

[3] The Reality of Data Breaches, infographic, **https://safenet.gemalto.com/resources/data-protection/breach-level-index-2018-h1/**.

[4] Office of the Privacy Commissioner of Canada, **https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/**.

EY

Building a better working world

What to look for

It's critical for you to receive regular (e.g., quarterly) updates from management on cybersecurity and data privacy that's both meaningful and actionable.

The EY 2018 Global Information Security Survey found that 83% of Canadian respondents say their information security function is only partially meeting their organization's needs and improvements are needed.

When evaluating your cybersecurity and data privacy risks, consider the following important actions:

Identification

What are the top three to five threats that are most relevant to your organization given its particular characteristics?

Protection

Summarize the actions your management team has taken to manage these threats. Summarize what other actions were considered but not pursued. Associate this to your risk appetite, tolerance and capacity.

Detection

What mechanisms are used to detect incidents? How does management evaluate and categorize incidents identified and determine which ones to elevate to senior leadership? What activity has been seen since your last update?

Response and recovery

How did your organization respond to higher risk incidents?

Value generation

How are cybersecurity and data privacy adding value to your organization? Is this only through risk reduction? Have efficiencies been implemented on integrating these functions to your enterprise risk management program? Is your organization using protection by design (including privacy and cybersecurity)?

Education

What initiatives are being managed to educate your staff on cybersecurity and data privacy matters?

Other critical questions for you to consider

- How are your company's most critical information assets being identified, inventoried and protected? Have the related cyber risks been prioritized?
- Are incident-response plans in place in your organization should a material data breach occur? Is your organization ready to respond to the data protection regulations in jurisdictions where the company operates? Has management practiced its incident-response plan and developed a crisis management plan for this type of breach?
- Have you considered the talent implications and re-evaluated the enterprise level at the company to effectively manage cybersecurity risks?
- Do you understand the insurance coverage in place and its impact on potential claims?
- How are your employees trained and made aware of their role in managing cybersecurity risks? Are internal threats appropriately considered?

We can help

To learn more about how our Private Client Services professionals can help you protect your business, contacts us at privatecompanyinfo@ca.ey.com.

Visit us at ey.com/ca/private.