RBC Global Asset Management

Cyber security and privacy: A material concern for investors

Cyber security, like a never-ending marathon, requires endurance and constant adaptation to changing conditions. News outlets continue to report about attacks in which sensitive information or client data have been misused or made public. The reach of the financial, legal, reputational and even physical impacts can be quite material, which is becoming increasingly clear to business leaders today.

Cyber risk is a business risk

The risk of cyber crime and data breaches has been on the rise. This poses a threat for individuals and their personal data, as well as for the companies that collect and store this information. High-profile cyber incidents have taken place in almost every industry. And the consequences have impacted company bottom lines in at least four different ways:

1. **Cyber crime can disrupt a company's operations and affect how its employees work.**
2. **It may damage the brand, which can lead to a loss of client loyalty and trust.**
3. **It can impact sensitive information related to clients, contractors and suppliers.**
4. **As tighter regulations are being put in place, companies may be subject to lawsuits.**

In other words, cyber security affects the interests of all stakeholders.

According to a 2018 survey by the World Economic Forum (WEF)[1], cyber attacks are the leading threat for businesses in economically advanced regions. The report also states that data fraud or theft is the second-highest risk for doing business in North America. In Canada, about 87% of businesses reported having been victim of a successful breach in 2017. And almost half of those lost sensitive data.

A recent Global CEO Survey[3] by PricewaterhouseCoopers (PwC) revealed that cyber attacks are the greatest concern of CEOs globally. Moreover, 87% of global CEOs say they are currently investing in cyber security in order to build and retain customer loyalty and trust.

The same year, an incident involving U.S.-based Equifax resulted in the world's costliest corporate data breach to date. Hackers stole the personal information of 143 million Americans at a cost of approximately US $600 million. This caused the company's stock price to plummet over 30% in less than a week.[2]

The WEF report also ranked cyber attacks a top risk in developed markets outside North America. Europe was impacted by a series of major attacks in 2017. For example, the WannaCry ransomware attack badly disrupted the UK's health system and Germany's rail system. Estimates from the WEF report suggest that the number of cyber attacks across Europe rose by approximately one-third in the first quarter of 2018, compared to the same period in 2017.

The Asia-Pacific region has also become a target of cyber crime due to the area's rapid digitization and the increasing demand for sophistication in the region's economies.

Top risk for doing business across each region	
Europe	Cyber attacks
Eurasia	Energy price shock
Middle East and North Africa	Energy price shock
Sub-Saharan Africa	Unemployment and underemployment
South Asia	Failure of national governance
East Asia and the Pacific	Cyber attacks
North America	Cyber attacks
Latin America and the Caribbean	Failure of national government

Source: World Economic Forum, 2018

What it means to investors

Weak controls of data privacy and security measures can create a material risk for investors. Data protection has thus become a critical part of the analysis they undertake. Investors are increasingly seeking more information on a wide range of cyber topics, including:

- Corporate awareness and preparedness
- Risk management
- Data protection and post-breach management
- Board-level cyber governance
- Corporate disclosure
- Mergers and acquisitions due diligence
- Regulatory and cyber security developments.

Obtaining and assessing information on cyber risk management is not a straightforward exercise. Today, there are few universally accepted standards and metrics to measure, assess and compare cyber risk. Cyber risks, and therefore cyber security, are constantly evolving. For that reason, investors need to continuously monitor and assess the state of companies' cyber environment by engaging with them and examining their governance practices.

What companies are doing to prepare and protect

Cyber risks should be managed at a senior level. The way the board manages cyber issues is vital as they are ultimately held accountable when those risks materialize. As a result, boards everywhere are committing to cyber risk management, whether or not an issue has materialized.

Buyer – and investors – beware

Here's a prominent example of the material impacts of cyber crime on an investment: the recent Marriott and Starwood hack[4] uncovered in 2018. The hack began in 2014, two years before Marriott International closed on its U.S. $13.6 billion acquisition of Starwood Hotels & Resorts Worldwide. It affected about 500 million records from the Starwood Hotels reservation system – including passport details and credit card information. By failing to conduct a comprehensive due diligence process, Marriott inherited Starwood's exposure to hackers. Immediately after the news was released, shares of Marriott dropped about 7% in pre-market trading.[5]

On the front lines, global spending on data privacy and security awareness training for employees is predicted to reach USD$10 billion by 2027. That's up from around USD$1 billion in 2014[6]. Combatting phishing scams and ransomware attacks are at the centre of much of this training. It is widely reported that more than 90%[7] of successful hacks and data breaches stem from phishing scams. It is thus critical for companies to learn how to identify and react to these threats.

From an investor perspective, the economic and social significance of cybersecurity is clear: data breaches can pose a material financial and social risk that can negatively affect a company's reputation and have large financial implications.

A leader in responsible investment

RBC Global Asset Management Inc. (RBC GAM) believes that being an active, engaged and responsible investor empowers RBC GAM to boost the long-term, sustainable performance of our investments. RBC GAM's commitment to integrate Environmental, Social, and Governance (ESG) factors into the investment process is firm-wide. The investment teams work together with the firm's Corporate Governance and Responsible Investment (CGRI) team to understand and assess issues related to cybersecurity and privacy, as well as other ESG concerns. The CGRI team, formed in 2014, focuses on five things:

1. Engage investee companies on ESG-related issues.
2. Oversee all of RBC GAM's proxy voting activities.
3. Advance the integration of ESG principles into investment analysis.
4. Collaborate with like-minded investors.
5. Engage with lawmakers or regulators.

RBC GAM continuously engages with companies' boards with regards to the oversight of their cyber and privacy risk management. Last year, the Corporate Governance and Responsible Investment (CGRI) team led a successful engagement with a FTSE 100 company as a part of the UN PRI-coordinated collaborative engagement on cyber security. Launched in the second half of 2017, this initiative enabled over 50 institutional investors to collectively engage with companies across sectors. Goals included:[8]

1. Build investors' knowledge of how their portfolio companies are positioned to manage cyber risk (with a focus on companies' policies and governance structures).
2. Establish investor expectations on what companies can and/or should disclose regarding cyber risk governance.
3. Improve the amount and quality of company disclosure on cyber risk and governance.

[1]World Economic Forum, "Insight Report: Regional Risks for Doing Business 2018," 2018.
[2]MarketWatch Inc., "Equifax's stock has fallen 31% since breach disclosure erasing 5 billion in market cap,"2017.
[3]PwC, 21st Global CEO Survey, January 2018: https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2019/gx
[4]Thomson Reuters, "Marriott's Starwood database hacked, 500 million may be affected,"2018.
[5]Bloomberg, "Marriott hit by Starwood hack that ranks among biggest ever," 2018
[6]https://cybersecurityventures.com/security-awareness-training-report/
[7]https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
[8]Principles for Responsible Investment, "Engaging with companies on cyber security," 2018.

Publication date: (October 17, 2019) GUK/19/266/MAY21/A