ONTARIO TEACHERS'
PENSION PLAN – RÉGIME DE RETRAITE DES ENSEIGNANTES ET DES ENSEIGNANTS

CYBERSECURITY AND PRIVACY:

Don't Be a Target

INTRODUCTION

Today the question is not will a firm be breached but how can an organization manage a broad range of cyber risks, including data breaches. New technology and novel applications of existing technology are enabling companies to respond to customer needs in ways that have not previously been possible, creating value for customers and investors. However, this has led to the emergence of new risks that can have devastating impacts, as illustrated by the high profile data breach experienced by Target in 2013, which is estimated to have cost the U.S. retailer over $250 million (see page 2)[1]. Cybersecurity and its associated risks exist in the virtual online world, but have very real consequences for companies, including the ones in which Ontario Teachers' invests.

In today's world, nearly every company is affected. In the last five years, the World Economic Forum identified cybersecurity-related concerns among its top 5 risks in terms of likelihood and, according to the U.K. Government, 90% of large organizations and 74% of small businesses experienced a security breach, ranging from unauthorized access to information to malware attacks, in 2015. Large or small, public or private, local or global, most companies are exposed to these risks, and the financial and reputational impacts that can result.

The challenge is that currently few companies are managing these new risks effectively. Nearly 70% of companies do not assess their suppliers or customers for cyber risk and the median time between the occurrence of a breach and discovery of the breach is 146 days[2]. With the average financial loss due to cybersecurity incidents in 2016 estimated at $4 million[3], cyber risks are too costly to ignore. The following section provides an overview of six key cyber trends. These trends impact nearly all of Ontario Teachers' investments, but in different ways and to various degrees.

1 Krebs on Security "The Target Breach, By the Numbers" (2014)

2 Mandiant "Mandiant Consulting M-Trends Special Report" (2016)

3 Ponemon Institute "2016 Cost of Data Breach Study" (2016)

Mobile Devices

There are now more mobile-connected devices than people on Earth. In the U.S., 90% of the adult population has a mobile phone, and global mobile data traffic is expected to grow at a compound annual growth rate of 57% between 2014 and 2019[4]. Mobile device, software and service companies are benefitting from this trend, but they are not the only ones. Retailers, financial services firms, and media companies have also ridden the mobile wave to offer their products and services anytime, anywhere.

Companies are increasingly allowing employees to use their own mobile devices for work purposes. However, employees' personal devices may not have adequate security protocols in place, leaving company data exposed and at risk. Yet many companies do not have a data loss prevention program in place or provide adequate training to their employees.

The business opportunities created by the widespread use of mobile devices and social media continue to be numerous and varied, as are the risks. To mitigate these risks, companies must actively manage the vulnerabilities they are exposed to from use of mobile devices and learn to navigate situations where the legal requirements and social expectations do not align.

Electronic and Mobile Payments

Electronic payments via point-of-sale terminals, websites, or mobile apps are continuing to grow in frequency around the globe. Electronic payments are experiencing double-digit growth across Thailand, Indonesia, China and India and mobile transactions outnumber transactions done through desktop platforms in some Asian markets[5].

Electronic transactions involve the transfer of sensitive information, such as payment card data or personal identification information, which can fetch large sums of money on the black market. Payment card data was the primary target in 95% of incidents within the retail industry in 2015[6]. The retail and financial services sectors are particularly at risk, as are any businesses that transact with customers online.

One of the recent high profile and large scale data breaches is the Target breach that occurred in late 2013. Hackers stole 40 million credit and debit cards, and accessed 70 million records including names, phone numbers, email addresses, and mailing addresses of Target customers[7]. The breach was achieved through a third party contractor that had access to Target's systems. This vulnerability allowed the hackers to install malware on Target's point-of-sale system in approximately 1800 of its stores. The breach is estimated to have had a financial cost of $252 million, in addition to compromising customer trust and tarnishing Target's brand. The CEO at the time of the breach was dismissed as a result of this incident, demonstrating that cybersecurity is a board-level, organization-wide issue.

Big Data and Privacy

The collection and analysis of customer information is not new; however, the massive quantity of data available today via mobile devices, social media and digital transactions is unprecedented. Big data is not only defined by the quantity of data available, but also by the new types of data and the rapid speed at which the data is being generated. It enables companies to develop granular insights into customer behaviour and to predict and even influence purchasing decisions. This data enables companies, with the analytical capabilities to derive meaningful insights, to establish a competitive advantage.

The benefits of big data depend on access to the data. Since the revelations made by former NSA contractor, Edward Snowden, in 2013, the public is more aware of personal privacy. There is growing concern regarding the collection, storage and use (or misuse) of personal data. For example, over half of app users have uninstalled or decided not to install an app due to concerns about their personal information. Maintaining consumers' trust is essential for the continued access to their information.

Healthcare, financial services and telecommunications sectors are particularly active in big data analytics, with access to large data feeds from their customers. When investing in these sectors, investors should ensure robust diligence is done on the target company's ability to manage these risks and the evolving regulatory landscape.

4 Cisco "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014-2019" (2015)

5 McKinsey "Insights from McKinsey's Asia-Pacific Payments Map" (2012)

6 PwC "Managing cyber risks in an interconnected world" (2015)

7 Krebs on Security "The Target Breach, By the Numbers" (2014)

Cloud Computing

Cloud computing refers to the practice of storing data and programs on a network of remote servers via the internet rather than on a dedicated, physically proximate hard drives. The cloud can be used to store computer system infrastructure, platforms, or software, essentially transforming functionality that used to only be available in product form into services. The ability to access this functionality via the internet provides companies with increased agility and flexibility. Companies are rapidly adopting cloud technology; spending on cloud computing is expected to grow at a 30% compound annual growth rate (CAGR) from 2013 to 2018[8].

Data stored on the cloud is not legally protected in the same way as data located on personal storage devices, and law enforcement agencies are requesting specific data stored on the cloud for use in their investigations. As noted in the previous section on big data and privacy, public concern regarding privacy and government surveillance has increased over the past few years. Companies that offer cloud-based solutions and companies that use cloud services should understand the legal implications of using the cloud, as well as the concerns that their customers may have.

Internet of Things

Smart consumer goods and industrial equipment, such as intelligent thermostats and smart agricultural machines, make up the internet of things (IoT). While these enhancements create new functionality for users, they also result in new vulnerabilities that need to be managed. People are accustomed to installing security software and subsequent updates to their computers, but may forget to do so for items such as baby monitors and thermostats, leaving themselves exposed to cyber-attacks.

In July 2015, two cybersecurity experts demonstrated that they could hack into the wireless communication system of a Jeep Cherokee and control the vehicle remotely, prompting Fiat Chrysler to recall 1.4 million vehicles. At around the same time as the Jeep incident, a bill was introduced to the United States Senate that proposes minimum cybersecurity standards for vehicles. As the internet of things continues to expand, new regulation may be introduced to set standards aimed at protecting consumers from cyber risks. To mitigate reputational risks, companies should make informed judgements about the sufficiency of current legislation and assess whether the public's expectations exceed regulatory standards.

Hacktivism and Cyberterrorism

Hacktivism refers to the act of breaking into a computer system for the purposes of advancing a political or social agenda. In contrast, cyberterrorism is usually characterized by the intent to inflict fear and disrupt civil society. These risks are infrequent relative to other cyber threats, but are growing and are noted here as a key trend due to the potential scale of impact if they were to materialize.

Infrastructure assets are common targets for hacktivists and cyber terrorists, who attempt to gain access to a facility's internal control systems to either halt operations or force it into unsafe operational conditions. In 2014, the Korea Hydro and Nuclear Power Company experienced a cyber-attack and partial blueprints of the company's nuclear power plants were leaked via Twitter. Responsibility for the attack could not be proven; however, there were indications that it was the work of North Korean hackers or an anti-nuclear group protesting against the use of nuclear power.

Although the likelihood of experiencing a hacktivism or cyberterrorist attack is low, infrastructure companies should have response plans in place in the event that one should occur.

The Way Forward

Cybersecurity is a board-level issue for companies. It affects almost every business unit for nearly every type of company and it is no longer the sole responsibility of the IT department. It requires constant vigilance and the overarching best practice is effective governance, through sufficient attention from the board. This attention can be focused on three principles: understanding the company's valuable assets, deciding the

8 Goldman Sachs "Battle of the Cloud Titans Has Just Begun" (2015)

risk tolerance, and developing an appropriate strategy. These principles reflect a risk-based approach, which addresses risks that may not be reflected in current regulatory requirements and tailors risk mitigation efforts to the specific and unique risks that a company may face.

The first step is to understand where the value is in the business. For example, does the company's revenue stream depend on confidential intellectual property? Does the company collect customer information that must be kept private and secure? Or perhaps the company provides essential services that must be online and operational every day of the year? Cybersecurity risks are not the same across business units and may warrant or require different solutions.

Next, the board must decide how much risk is acceptable. Cybersecurity controls often require trade-offs between risk mitigation and productivity, and come with upfront and ongoing costs. A company's approach to cybersecurity should reflect its strategic priorities and involve a cost-benefit analysis.

Once the value has been identified and the risk tolerance has been determined, the company is positioned to develop policies and select tools that will provide the appropriate amount of protection.

Ontario Teachers' Approach

The starting point for risk management is the investment strategy. As directors of an investee company's board, portfolio managers review the strategy and identify the risks associated with its execution. For example, if a core part of the strategy is growth by acquisition, then diligence of targets' people, processes and systems is done for each new entity brought on board. Additionally, third party experts may be brought in for deeper analyses of system vulnerabilities, and ongoing dialogue with management helps monitor operational performance and trends.

CONCLUSION

The six trends of mobile, big data, electronic payments, internet of things, cloud computing, hacktivism and cyberterrorism bring about value creation opportunities for Ontario Teachers' and our investee companies, as well as exposure to new risks. Cybersecurity risks are increasingly relevant to the plan's investments, with incidents like data breaches becoming a reality of doing business today. These risks are manageable through effective governance. Ontario Teachers', as an engaged owner, continues to translate the trends into value and leverage best practices across the portfolio.