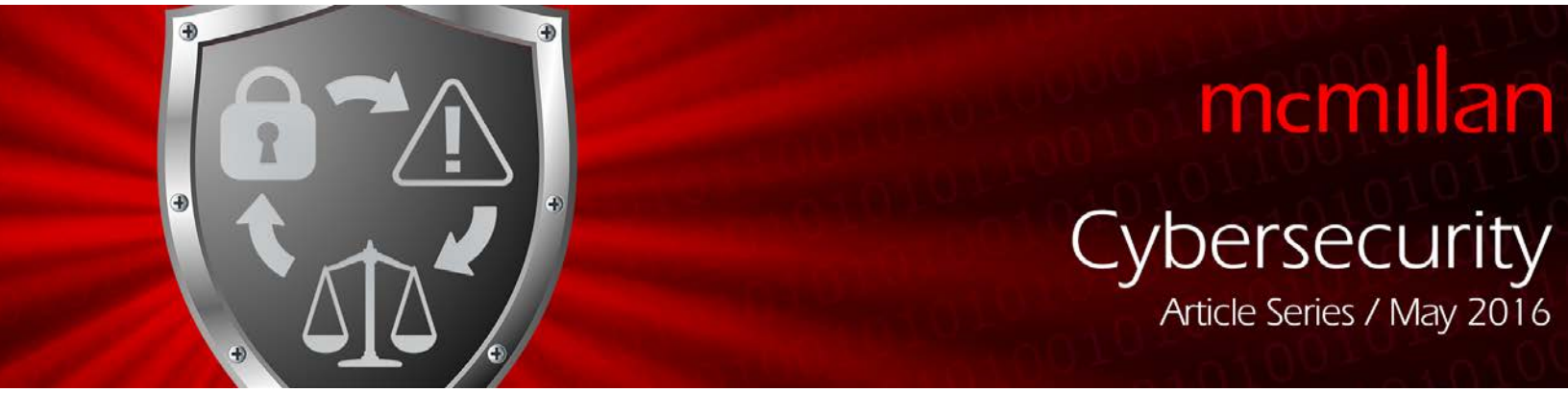

Mitigating Cyber Risk and Cybersecurity Insurance

Introduction

In an era of increasing competitiveness, businesses and organizations are becoming more dependent on digital systems in order to compete effectively and are concentrating their value in digital assets to benefit from the explosive growth of a connected economy. However, concurrent with the exponential growth of the digital economy, cyber attacks have increased at the same or an even greater rate. Perpetrators of cyber attacks range from amateur lone-wolf hackers to sophisticated nation states. The variety of attacks and attackers, and the resources available to attackers, make it impossible for businesses and organizations to be completely breach-proof.

Because of this, business and institutions must put in place systems and procedures to protect their digital systems and assets, and take initiatives to mitigate their exposure to cyber risk. This article will highlight some common forms of cyber attacks, some common best practices tips to reduce your exposure to cyber risk, and lastly discuss the availability and limitations of cyber insurance to mitigate cyber risk.

Common Forms of Cyber Attacks

To begin mitigating cyber risk, businesses and organizations need to have at least a preliminary understanding of the threat landscape. However, this is challenging as each business and organization is unique, and consequently may be exposed to unique forms of cyber

attacks. Furthermore, cyber attacks can result from a combination of many of the categories of attacks described below. In general though, the three broad categories of cyber attacks are: to attack the members of the business or organization, to attack the digital systems of the business or organization, and lastly to attack the suppliers or customers of the business or organization.

The first category of cyber attack is through the use of social engineering or similar methods to obtain confidential information directly from individuals, typically employees or customers, of a business or organization. Below is a description of several of the more common methods used:

- **Phishing** – A phishing attack usually involves the attacker sending an email from either a recognized or professional sounding business, with a link or attachment which either contains or directs you to malicious software[1]. Phishing emails are typically sent to large groups of recipients with the expectation that some will open the link or attachment; however, cyber criminals have used targeted phishing emails directed at individuals as well.
- **Baiting** – Involves leaving physical media storage devices (typically USB keys) in a location where they are sure to be found. Curiosity then propels a person to examine the contents of such a device resulting in malware gaining access to their computer systems.
- **Pretexting** – This type of attack involves a misrepresentation by a person, typically the impersonation of a respected individual or business, to obtain private information. It is similar in concept to phishing but is typically more targeted. For example, victims have received calls from cyber criminals impersonating technical support staff at major technology companies who claim the victims have been affected by malware and the victim must

[1] This includes any form of malicious software (or more commonly known as "**malware**") such as viruses, worms, and lyphen Trojans. Malware is short for malicious software and includes essentially any unwanted computer code. A virus is a form of malware that is a self replicating program that attaches itself to another program or file to reproduce. Similarly, worm's are another form of malware that are self-sustaining programs and can replicate independent of another program. Lastly, Trojans are a form of malware that appear to act like a normal program, but secretly perform unwanted activity.

provide the support staff with remote access to their computer so they can remedy the situation. Once the fraudster has remote access they can upload malware onto the victim's computer.

- **Waterholing** – This type of attack involves compromising an existing website or setting up a fictitious duplicate to obtain users' private information.

The second category of attack focuses on exploiting vulnerabilities in the digital systems of the target. Some examples of these types of attacks include:

- **Denial of service** – This type of attack is designed to obstruct legitimate users from gaining access to a website by repeatedly trying to access a website through the use of multiple access requests which utilizes all of the website's available bandwidth. Consequently, users that try to access this site may find the website takes an exceptionally long period of time to load as the website tries to manage the overloading number of access requests.

- **DNS spoofing** – This type of attack involves corrupting the server the website is hosted on so that users who try to access the website are instead diverted to another website (which may or may not contain other malware).

- **Smurf attack** – This type of attack involves sending the target's internet address to a large network of computers who then respond back directly to the target thereby slowing the targets computer as it becomes overloaded with data traffic to the point that it becomes non-functional. This is similar to the denial of service attack.

- **SQL Injection** – This attack is used on websites that typically request data from users. SQL stands for Structured Query Language and is the language used in digital database management. Websites that manage data from users typically build their databases through SQL. An SQL injection involves the insertion of malicious data into available data fields designed to corrupt the targeted database. This can result in the database being nonfunctional or releasing information available in the database.

The last broad category builds off the first two categories outlined above. Businesses and organizations should be aware that they are not the only target of cyber attacks. Their customers or suppliers may have been attacked using any of the methods described above, and also many others not described. Customers and suppliers who have been attacked may not be aware that their digital systems have been compromised and may unknowingly send malware or provide access points for cyber attackers into your business' or organization's digital systems.

Consequently, businesses and organizations must remain vigilant, not only about their own systems but also in managing their digital relationships with both consumers and suppliers. Risk mitigation starts with identifying the risks in each of the three broad categories outlined above. Businesses and organizations should then take steps to identify and implement the measures they can put into place to manage their risks, and explore the availability of insurance.

Best Practices for Mitigating Cyber Risk

A good cybersecurity program requires involving all aspects of a business. Businesses and organizations need to take an enterprise wide approach to cyber risk management. As shown above, attacks can come from both internal and external sources. As a result, businesses and organizations should look at revamping their internal policies to protect against cyber attack from members of their business or organization, their technical infrastructure to protect against external attacks, and lastly should look at what cyber security policies and systems their customers and suppliers have in place.

There are a number of best practice guidelines available for businesses and organizations looking to develop their cybersecurity. For example, some common and helpful guidelines include:

1. Framework for Improving Critical Infrastructure Cybersecurity by the National Institute of Standards and Technology;[2]

[2] *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, Version 1.0, February 12, 2014. *http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*

2. Cybersecurity Best Practices Guide for IIROC Dealer Members by the Investment Industry Regulatory Organization of Canada;[3]

3. Cyber Incident Management Planning Guide for IIROC Dealer Members by the Investment Industry Regulatory Organization of Canada;[4]

4. Get Cybersafe Guide for Small and Medium Businesses by the Government of Canada;[5]

5. Cyber Security Self-Assessment Guidance by the Office of the Superintendent of Financial Institutions Canada.[6]

In particular, below are some of the more common best practices for mitigating cyber risk:

- Establish a governance framework to manage cybersecurity risk. The framework should create a cross-organizational committee of senior executives with a full range of enterprise knowledge and capabilities to assist in the development of a cybersecurity program, particularly the identification of known risks and established controls;

- Identify a company's crown jewels and allocate the highest protection to the most important/valuable data;

- Develop an enterprise wide cybersecurity risk profile and a target cybersecurity risk profile the business or organization wishes to achieve. Decide which risks the businesses can afford to protect against, which it is willing to accept, and which it needs to mitigate and consider cybersecurity insurance accordingly;

---

[3] *Cybersecurity Best Practices Guide for IIROC Dealer Members,* Investment Industry Regulatory Organization of Canada, December 21, 2015. *http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf*

[4] *Cyber Incident Management Planning Guide for IIROC Dealer Members,* Investment Industry Regulatory Organization of Canada, December 21, 2015. *http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf*

[5] *Get Cybersafe Guide For Small and Medium Businesses*, Government of Canada, last modified March 3, 2015. *http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/smll-bsnss-gd-eng.pdf*

[6] *Cyber Security Self-Assessment Guidance*, Office of the Superintendent of Financial Institutions Canada, October 28, 2013. *http://www.osfi-bsif.gc.ca/Eng/Docs/cbrsk.pdf*

- Ensure that cybersecurity is on the board agenda and that access to cybersecurity expertise is available;
- Adequately staff and budget for cybersecurity risk according to the value of an enterprises digital systems;
- Constantly review the operational environment to determine the likelihood of a cybersecurity event and the impact it may have;
- Make cybersecurity training and awareness mandatory for all personnel, and ensure that all personnel understand their roles and responsibilities with regard to cybersecurity;
- Consider the following technical best practices:
    - Application Whitelisting – This involves permitting only those applications that have been approved by the business or organization to operate on their networks;
    - Application Security and Operating System Patching – This involves effectively deploying new security updates for applications or operating systems in a timely fashion; and
    - Limiting Administrative Privileges – This involves allowing only a group of trusted personnel configure, manage and monitor the digital systems and networks of a business or organization.
- Consider conducting vendor cybersecurity assessments. The Cybersecurity Best Practices Guide for IIROC Dealer Members provides a useful sample vendor assessment;[7]
- Do not focus on just preventing of cyber attacks, also consider policies and procedures to detect cyber intrusion and to remove any malicious code; and
- Ensure your company consistently and frequently creates backups to safeguard information in the event of a cyber-attack.

These are only a sample of the some of the many best practices for mitigating cyber risk available. Businesses and organizations must

[7] See appendix B of 3.

remember to frequently review their policies, procedures, and digital infrastructure with respect to cybersecurity as the threat landscape is constantly evolving and historic methods become outdated leading to vulnerabilities. While the above best practices provide some guidance on mitigating your cyber risk, a careful consideration of available cyber insurance coverage should be part of any risk mitigation practices.

Cyber Insurance

The frequent incidences of cyber breaches and cyber crime and related news reporting has greatly increased awareness of the existence of the cyber risk threat and the need to find solutions, including insurance. Insurance brokers, eager to "fill the need," are leading the charge by providing a host of cyber risk related services, including performing comprehensive analyses of the types of risks that their clients are exposed to, matching the risk profile to the insurance available, and providing education on risk management and risk mitigation efforts that can help reduce not only the risk of loss, but potentially the cost of insurance. In this sense, cyber insurance considerations are one of the drivers for improvements in cyber risk management processes.

On the positive side, cyber risk insurance is a growing industry in Canada, the United States and Europe and coverage is becoming increasingly available and affordable. On the other hand, coverage is not currently available for all types of cyber risks.[8]

Available Cyber Insurance Coverage

Most commercial general liability policies now specifically exclude cyber risk. However, specialized cyber risk insurance policies are available and may be specifically designed to respond to a number of losses due to a cyber attack or data security breach. The scope and limits of coverage will necessarily be subject to the insurer's overall risk appetite and ability to quantify the nature and extent of the risks it is assuming.

---

[8] Insurance Institute, "Cyber Risks - Implications for the Insurance Industry in Canada" (Emerging Issues Research Series)

By way of example, a tailored cyber liability insurance policy may cover:

- loss of income due to the incident (e.g. cyber attack or privacy or data security breach);
- loss of profits that the organization would have earned had the incident not occurred;
- in the case of an interruption in business, recoupment of expenses that must be paid even though the business is not operating;
- costs for notification to customers and/or others for privacy and data security breaches, certain associated legal costs and, where applicable, costs related to monitoring the credit of affected customers and/or others for a period of time following the incident;
- costs incurred to avoid claims that, if made, would be covered under the policy;
- where legally permitted, costs of regulatory actions and investigations; fines and penalties;
- legal liability to third parties arising from hacking attacks or malware as well as due to a privacy or data security breach; and
- cyber extortion, such as “ransomware” (a type of malware that prevents an organization from accessing its own computer system until a ransom is paid).

In applying for coverage, organizations should be prepared to demonstrate to the insurer that cyber risk is an integrated part of their overall enterprise-wide risk management framework and that appropriate risk management tools and processes are in place. Insurers, brokers and other specialists will be involved in the process in order to analyze and assess the potential risk and the effectiveness of the measures in place to mitigate losses.

Some insurers and insurance professionals (e.g. brokers) also offer cybersecurity risk related services for after an event, including through third-party service providers such as breach consultation,

forensic analysis, notification services, call centre services, credit and identity theft monitoring, fraud consultation and credit and identity restoration services.

Limitations and Challenges for Cyber Risk Insurance

If insurers cannot reasonably calculate the potential quantum of a loss, they will not accept the transfer of the risk. Currently, there is not enough historical data and other information available to permit insurers to quantify certain cyber risks, such as cascading losses arising from cyber theft of trade secrets or from cyber crime resulting in disruption to or destruction of major infrastructure (such as a power plant). Consequently, such risks are generally not insurable. Until modern history records enough data on which insurers can rely to assess their potential exposure to such risks, insurers will not be in a position to assume them. By way of comparison, insurers have many years of experience estimating and quantifying probable losses from such varied perils as automobile accidents, home and industrial fires and even earthquakes – at least, enough to enable them to model, be prepared for, and price the corresponding potential losses accordingly. For this reason most available cyber insurance coverage is currently restricted mainly to losses relating to data breaches and cyber extortion. Nevertheless, it may be possible to work with a broker and the insurance market to attempt to design a policy that addresses your organization's vulnerability to other specific cyber risks. But, even if the insurance coverage is available, the policy is likely to be costly and subject to strict limitations.

Possible Future Development of Cyber Insurance Coverage

Stakeholders (e.g., in the United States) have advocated for mandated, widespread cyber incident reporting and the creation of a central repository of data and information relating to cyber breaches and attacks and associated losses and other fallout. This could assist insurers in evaluating and quantifying insured losses.

If implemented, over time, more comprehensive coverage could become available and/or more affordable. In addition, it is possible that, if enough pressure is brought to bear, a cyber risk insurance scheme may be legislated. For example, such a scheme may involve a government back stop, similar to the programs that have been set

up in the United States, Europe and elsewhere to cover terrorism risk. Such a government-initiated or public-private program would likely be called for in the event of a credit crunch e.g. where lenders require organizations to have comprehensive cyber risk insurance protection that is otherwise commercially unavailable.

Conclusion

In conclusion, businesses and institutions need to be aware that cyber criminals have a wide variety of tactics available. Cyber criminals can target an organization's employees to obtain access to digital systems or they can target the digital system directly. Organizations need to focus on identifying where their vulnerabilities are, develop their own optimal risk portfolio, put in place policies and appropriate safeguards to protect critical digital systems and consider the extent to which they can use cyber insurance to mitigate cyber risk to help reach their optimal risk portfolio.

by Carol Lyons and Jeffrey Nagashima

For more information on this topic, please contact:

Toronto	Carol Lyons	416.307.4106	carol.lyons@mcmillan.ca
Toronto	Jeffrey Nagashima	416.865.7136	jeffrey.nagashima@mcmillan.ca