Cyber-Attacks: Why Any Business May Be At Risk And Five Possible Ways To Address The Risks

written by Rory Lodge | March 18, 2016

Recently, interest in cybersecurity has skyrocketed amongst board of directors and executives. According to a survey conducted in 2015 by the information security organization ISACA, among the global business and IT professionals from 129 countries who responded, 86% believe that cyber-attacks are among the three biggest risks faced by organizations today. Their concern regarding cyber-attacks is understandable, as the costs and risks associated with cybersecurity have increased tremendously in the last few years. For example, a 2016 PwC survey indicated that cybersecurity-related incidents had increased by 160% on a year-over-year basis.

In this article, we will focus on five risk factors related to cybersecurity and five corresponding ways to minimize the risk of a cyber-attack.

Part I – Five Risk Factors

1. ***Thinking It Cannot Happen***
   Blindly believing that cybersecurity is not a concern can be problematic as it may condition management into not investigating whether there are any real concerns. According to the 2015 ISACA survey, only 46% of professionals expect a cyber-attack to strike their organization in the coming year, although a staggering 86% of professionals believe that it is one of the biggest threats that their organization is facing. Hence, there is a great discrepancy between how many professionals see cyber-attacks as a threat and how many actually think it will happen to their organization.
   In order to determine if cybersecurity risks should be a concern, the management of a business should consider the three fundamental functions of cybersecurity, namely: confidentiality, integrity and availability.

- **Confidentiality**: This refers to important or sensitive information that a business wants to keep confidential and private and to which only certain people or systems should be given access to. Does the business keep electronic copies

of contracts, call for tenders, bids, lists of employees, credit card numbers, personal identifiable information and so forth? Or, more generally, does the business have any electronic information that stakeholders would not want to be disclosed to the public?

- **Integrity**: This refers to the integrity of the business' systems and its consistency and trustworthiness over time to keep information assets complete, intact and uncorrupted. Are the IT systems secure? Does the business use different types of identification methods (biometry or security tokens, for example)? Do its employees have access to their e-mails on their phones or remote access to their computers? Does management have absolute confidence in the integrity of their systems at all times?
- **Availability:**This relates to the importance of having all IT systems available for the continued operation of the business. Can the business operate without access to Internet or e-mails for a few hours, a day, two days or a week? Can the business operate without access to the information stored on its hardware? How long can the business continue to operate if it lost control of its cyber infrastructure?

If there are any concerns regarding any of the above functions, the management of a business should consider cybersecurity as a risk to be discussed with its legal and cybersecurity professionals.

2. ***Failing To Understand Where The Risks Are Coming From***

Understanding issues with the business' cyber infrastructure is a key component in assessing cybersecurity risks. Being aware of malware, viruses or intrusions, service provider failures, physical security deficiencies (loss or theft of device or equipment), misuse of mobile devices, insider sabotage or misuse or failure of cloud applications is extremely important in detecting and reacting to a cyber-attack. Otherwise, the management of a business risks learning about a cyber-attack on the business' system from a third party such as a supplier or customer which may lead to reputational damage and the loss of goodwill for the business.

3. ***Failing To Take Into Account The Human Factor – The Weakest Link***

When it comes to cybersecurity, "human factor" is the elephant in the room. More and more cyber criminals manipulate unsuspecting employees to gain access to an organization's confidential information. This method of exploitation, known as social engineering, is one of the most common ways of effecting a cyber-breach. According to a 2015 report, 95% of all espionage attacks that occurred in 2015 involved a practice known as a phishing scam which consists of tricking individuals into divulging sensitive information via a website link or through direct response, such as an e-mail.

For example, one can easily imagine the situation where all of the employees of a business receive an e-mail from an unknown source containing either a document or a link and a plausible reason as to why the document should be opened or the link should be clicked on. Is management confident that all of the business' employees would never open such a document or click on such a link? The consequences of even having just one employee inadvertently open the document or click on the link could be disastrous. For example, the business could be out of its e-mail server for numerous days. The fact is that hackers, phishers and malware are sophisticated and can harm, slow down or even paralyze a business.

4. ***Underestimating The Importance Of Preparedness***

Another way a business may be at risk is if its management team underestimates the

importance of being prepared. Being prepared involves both having a plan to prevent a cybersecurity breach (pre-attack plan) and a plan on how to respond to a cybersecurity breach should it materialize (incident response plan). The importance of having both such plans in place is sometimes underestimated by the management of a business even though the consequences of not having such plans can be serious, and can include damages and fines imposed by courts and regulators.

5. ***Blindly Believing That The Business Has Adequate Insurance Coverage***

In Canada, the cyber insurance market and its products are relatively new and still developing and evolving. As such, navigating through multiple policies, from general commercial liability policies, to errors and omissions, to network security and privacy policies can often be challenging. One common oversight is believing that traditional policies will provide the business with adequate coverage in case of a cybersecurity breach or a cyber-attack. In general, such policies may only cover some of the risks associated with cybersecurity. Most of the time, data and other non-tangible goods that can be stolen in a cyber-attack may not be covered, meaning that many businesses may not understand the true cost of a cyber-attack to their bottom line. The true cost may not be negligible considering that cybercrime costs an aggregate of US $375 to $575 billion every year globally and that according to a 2015 study by the Ponemon Institute, the average consolidated cost of a data breach in Canada was CAD $5.32 million per occurrence.

To illustrate, imagine the situation where an employee takes a USB key containing over 1000 customer files in order to work from home, puts the USB key in his car and on his way home stops for lunch, then comes back to the car, and the USB key is gone. Traditional policies would normally cover the tangible object, the USB key itself. However, what is on the USB key and clearly what is more valuable, the intangible (the data), is typically not covered. Any damages associated with such a loss of data would also generally not be covered and could be devastating both from a reputational and a financial perspective.

Part II – Five Ways To Address The Risk Of A Cyber-Attack

There is no way to guarantee 100% protection against cyber-attacks, but cyber risks can be controlled and mitigated by any business. Whether each of the following methods is appropriate or necessary for a given business will depend on management's appreciation of the facts and circumstances surrounding the business.

1. ***Consider Raising Awareness***

Raising awareness with regards to cybersecurity within the entire business may minimize the risk of a cyber-attack. As mentioned in our previous article, cybersecurity is not only an IT issue. It is becoming an enterprise-wide issue that can require an interdisciplinary approach, including comprehensive governance commitment to ensure that all aspects of the business are aligned to support effective cybersecurity practices as well as regular training of all stakeholders including employees. For example, businesses can raise awareness by educating employees on common ways to gain entry to the business' system, such as phishing and phony e-mails, which in turn may reduce the likelihood that its employees will become attack vectors, the term commonly used in the industry to describe the means by which a hacker gains access to the business' network. Indeed, proper training can help reduce some of the risks associated with human factors.

To that effect, the *Investment Industry Regulatory Organization of Canada* (IIROC) issued in December 2015 a **Cybersecurity Best Practices Guide**. Although the guide is designed for IIROC dealer members, it contains several tips and guidelines that could

be useful for any private or public company that wishes to raise awareness internally.

Furthermore, to raise awareness, a business can conduct various tests on its cybersecurity infrastructure to determine its vulnerability to cyber-attacks, either in-house or through the use of an external security service. Cybersecurity professionals from external firms, such as most of the large accounting firms, employ a wide array of tests that they can conduct on your systems to determine your vulnerability to an attack. The two most common tests are the "White box" and "Black box" tests. In a "White box" test, cybersecurity professionals will require some information on the business, examine its systems and determine its vulnerabilities by simulating a cyber-attack. In a "Black box" test, cybersecurity professionals will act as if they were hackers, meaning that they will not require any information or examine the business' cyber infrastructure before trying to hack into it; they will only simulate an attack to determine where and how its system is vulnerable and what kind of information would have been stolen or compromised had it been a real attack.

2. ***Consider Adopting a Robust Policy Targeted at Employees***

In addition to raising awareness, another way a business may address the risks associated with the human factor is by elaborating a comprehensive policy that informs employees on how to deal with the business' technology, its devices, its web applications (including e-mail) and its electronic information as well as any personal devices that come into contact with the business' IT infrastructure. In elaborating such a policy, management may consider:

- using language that is easily understood by all employees – not only technology or security specialists;
- specifying what constitutes intellectual property, confidential information, sensitive business information, and other assets which the policy seeks to protect;
- emphasizing the importance of cybersecurity and explaining the potential risks to allow employees to understand what is "at stake" by using real life examples to which employees can relate to;
- specifying what can or cannot be done with the business' technology, devices, web applications (including e-mail) and electronic information;
- specifying who is responsible for the policy specifically or cybersecurity generally;
- specifying the hierarchy of who to contact if there are any questions or incidents as well as how to contact such persons; and
- specifying the costs and consequences to the business and individual employees who fail to respect the policy.

In order to ensure that such policy is an effective tool, a business may consider regularly reinforcing its application through information sessions and internal communications (i.e. e-mails, videos, portal) and its compliance through proper audit and monitoring.

Furthermore, before drafting or adopting a cybersecurity policy, a business may consider using guidelines provided by the National Institute of Standards and Technology (NIST) in its **Framework for Improving Critical Infrastructure Cybersecurity**. The framework provides many practical and interesting tools and ideas for implementing, maintaining and managing robust cybersecurity policies and processes.

3. ***Consider Employing Safeguards in Contracting Processes***

One of the major subjects treated by recent guidelines from regulators throughout Canada and the United States is third-party services and suppliers' contracts. In fact, "the number of security incidents at companies attributed to partners suppliers and third-party vendors has risen consistently, year on year". A business may wish to consider employing safeguards in its contracting process such as:

- developing policies designed to assess and verify third party service provider's or supplier's cybersecurity infrastructure's performance;
- exercising careful due diligence before entering into an agreement with third party service provider or supplier;
- assessing the kind of information that the third party service provider or supplier will have access to and identifying such information as confidential and protected information in the contract with that party;.
- requiring the third party service provider or supplier to provide adequate representations, warranties and covenants regarding its cybersecurity processes (including ongoing and regular testing and improvements) so as to have a contractual recourse in case of a cybersecurity breach that is attributable to the third party service provider or supplier;
- giving priority to third party service providers or suppliers that have rigorous cybersecurity policies in place, as these relationships ultimately influence a business' risk profile and, where applicable, the premium of a business' cyber insurance policy; and
- assessing whether its cyber insurance policy provides it with adequate coverage in case of a cybersecurity breach that is attributable to the third party service provider or supplier.

4. ***Consider The Need For Cybersecurity Insurance***

Insurers in Canada recently started to provide clients with the possibility of subscribing to stand-alone cyber insurance policies, either by directly underwriting with insurers or through a brokerage firm. Cyber insurance is modular; there are various cybersecurity policies (information security and privacy liability, privacy breach response, media liability, just to name a few) that can be adapted to a business' needs. To better understand the type of insurance a business needs, insurers and/or brokers will typically circulate a questionnaire comprising of 40 to 50 questions to identify a business' strengths and weaknesses. Generally, the more robust the cybersecurity infrastructure and governance structure of a business, the less expensive the premium it will have to pay.

Also, management may consider consulting with legal professionals and cybersecurity specialists to help them with the process of subscribing to a cyber insurance policy. Many problems may arise from cyber insurance policies if they are not reviewed by seasoned professionals. For instance, the way one circumscribes the definition of "sensitive information" in a policy is very important because it might exclude some of the key assets and/or data of the business. Another example is that cyber-attacks are sometimes state sponsored or otherwise and therefore may be excluded if it falls under the classic "terrorism" exclusion. Additionally, exclusions must carefully be examined when dealing with a traditional policy.

5. ***Consider Legal Disclosure Obligations***
6. **a) Digital Privacy Act**

In addition to continuous disclosure obligations of listed issuers, which we have already discussed in a previous article on cybersecurity, management may wish to consider legal disclosure obligations related to a cyber-attack.

In June 2015, the ***Digital Privacy Act*** (DPA), was adopted to amend the ***Personal***

Information Protection and Electronic Documents Act (PIPEDA) to, among other things, require organizations to notify the Privacy Commissioner and affected individuals of any breach of security safeguards involving personal information under an organization's control, if it's "reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual." A business can be fined up to $100,000 if it fails to inform customers of the breach in a timely manner. In addition, the DPA will require that organizations keep and maintain a record of every breach of security safeguards involving personal information under the organization's control. Even though the obligation to notify will not come into force until related regulations are adopted, the adoption of the DPA itself sends a message to business and organizations to be vigilant.

1. **b) Various United States Bills Adopted or Proposed**

A first bill to adopt the *Cybersecurity Disclosure Act of 2015* was proposed by Senators Reed and Collins of the U.S. Senate on December 17, 2015. The bill purports to promote transparency in the oversight of cybersecurity risks of publicly traded companies. In the form of "comply-or-explain", this bill proposes to require public issuers to disclose which member of its board has cybersecurity expertise or explain why such expertise is not deemed necessary at the board level. As of today, nothing of this nature has been proposed in Canada but it will be interesting to follow any development regarding the proposed U.S. bill in the coming year, as there is always the potential that Canadian regulators may follow suit.

The *Cybersecurity Information Sharing Act of 2015* was adopted on December 28, 2015. This new act gives companies legal immunity if they share data threats and defensive measures with the federal government. As of today, no equivalent act has been adopted in Canada.

In conclusion, navigating the cybersecurity world is not always an easy task. From the testing of cyber infrastructure, to the education of employees, to the drafting of agreements with third party service providers and suppliers, to selecting a cyber insurance policy, many questions and uncertainties may arise. Being ready is key to fighting the cyber war. With trusted professionals at its side, a business may find that addressing this risk may be easier than it seems.

Article by Vanessa Coiteux