mcmillan Insurance Bulletin

October 2014

Cyber-Risk – The Electronic Ebola of the 21st Century

For good reasons, the most significant concern for CEOs and Boards today is cyber-risk. How should a company prepare for it? How should a board deal with it? What mechanisms are available to minimize or transfer the risk? What are developing best practices?

Taking into consideration the interconnectivity of companies via the internet, the ever changing number of actors in the "attack chain", and the increasing sophistication and availability of "attack tools", cyber attacks are akin to the Ebola virus but commercially more dangerous as the attack need not involve crossing physical borders or even leaving one's computer.

The risk of a cyber-attack or incident has increased over the years in terms of frequency and the profile of the attackers has also changed. Years ago, the greatest risk was perceived to be a disgruntled insider, such as an employee. That is no longer the case. Cyber-attacks have become an industry. Toolkits for hacking are available and are being sold online. There are groups that collect information from hacked sites. They package and sell the information to third parties/organizations. Additionally, cyber-attacks are now part of the "arsenal" of state organizations. They are used much the same way as military power.

How is an organization to respond to these threats/risks? While there is indeed much to be concerned about, there have also been recent developments and initiatives that can help you assess and address the potential danger.

As was the case with the internet and technology development in general, both the private and government sectors of the United States are leading the way. President Obama's 2013 Directive[1] recognized the importance of this threat and mobilized the resources of the US government to respond. It has been said that currently more resources are being devoted to cyber-security than to combating terrorism. Your organization should tap into some of these initiatives. As an example, the National Institute of Standards and Technology (**NIST**) recently published its *Framework for Improving Critical Infrastructure Cybersecurity*.[2] The NIST framework provides a useful approach for companies and organizes the response around key overriding principles: Identify, Protect, Detect, Respond and Recover. In addition, the SEC recently hosted a roundtable discussion[3] of experts (both from government and the private sector) to discuss cyber-security matters, the response and some of the available learnings and resources.

Adopting the NIST framework's key principles approach, in **identifying** your company's vulnerabilities, ensure that **all** access and linkages are identified. This goes well beyond employees to suppliers, customers and everyone else who has access to your facilities both physically and electronically. The weakest link in these relationships can become the source of the attack. If you have affiliates in other jurisdictions, their vulnerability as well as those they interact with all need to be considered. As a Swiss-owned insurer found out to its chagrin, its South African affiliate, to whom data processing was outsourced, did not have sufficient approaches to discipline or security. The remediation costs, fines and reputational hit were borne by the UK company. The identification analysis should also include links where your organization holds and

[1] PPD-21 - February 12, 2013. See *http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil*.

[2] Issued February 12, 2014. See *http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf*.

[3] See *http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml*.

is responsible for data of others including those to whom you provide services as well as information held under Non-Disclosure Agreements.

As in the case of other compliance programs, the culture of the organization and the "tone from the top" will be fundamental to establishing how robust, deep and widespread your company's **protection** is. Every employee has to understand the importance of vigilance and care. This requires training. A real live example involved thumb-drives containing malware being left behind. If an employee inadvertently puts that thumb-drive into a company computer, the attack may be initiated.

None of these areas remain static. Technologies, tools, vulnerabilities, approaches and threats evolve over time and morph just like real viruses. The risk management approach has to be refreshed, rebroadcast and re-taught continuously. Organizations at the leading edge simulate attacks, assess responses, and recalibrate approaches. They treat it very much like fire drills.

The **detection** and **response** needs to be not only robust, it must be organized. Escalation thresholds and protocols for tracking, assessment and response need to be thought out ahead of time, rehearsed and ready to be implemented. Expertise, including technical, legal and public relations has to be identified, prepared and available. The very worst time to try and plan a response is in the middle of crises.

The **response** must not only consider matters within your IT department or company, it must consider the company's customers and regulators. Privacy has become an important consideration worldwide and most jurisdictions have laws requiring disclosure to customers and privacy regulators if personal data is compromised. For those companies in the financial services, health and education sectors – the ones considered to be among the biggest targets for cyber-attacks – other regulators will also be involved. Publicly-listed companies and organizations dealing with the public are required to provide disclosure where personal information has been compromised. Hence your organization needs to be aware of the different legal regimes across the jurisdictions in which you operate or that apply to you, because the disclosure/reporting requirements and timelines will undoubtedly vary. You need to think through before-hand what needs to be disclosed, by whom, to whom, when and what needs to be protected and how. Legal privilege can be an important protection against providing ammunition to those interested in suing you, for example, class action plaintiffs and their lawyers.

The **recovery** plan must not only consider the rehabilitation of the IT systems but also the company's reputation with its customers, regulators and indeed the public. Unfortunately, the reporting and the aftermath of the attack will remain on the company's record, potentially forever available to anyone doing an internet search.

From an operational and governance perspective, the expectation and the requirements have also changed. No longer is it reasonable to add this to the responsibility list of those who deal with the physical security of your operations. While the IT department and the CIO have an important role to play, cyber-risk must be part the organization's **enterprise risk management** approach. Some organizations have a Chief Risk Officer and a special risk committee of the board. The board's responsibility for overseeing management of the company clearly encompasses this threat. If you are a publicly-listed company or a financial institution, your regulator has specified cyber-security as a board responsibility. Some forward thinking organizations have at least one board member familiar with this area who can lead the board/committee on a knowledgeable exercise of its oversight function.

No matter how good your planning and risk management systems are, there will undoubtedly remain a residual risk of the unexpected – the black swan. This is an area where insurance can provide a means by which your organization can transfer some of these residual risks in the same manner as it transfers other residual liabilities. However, this has become a specialized area and your normal property and comprehensive general liability insurance coverage will not respond. Both now contain exclusions for cyber attacks and you need a specialized form of policy to cover the risk. Insurance companies have fashioned policies that cover the first party damage you may suffer including remediation, business interruption and income loss; the third party liability stemming from harm suffered by third parties; funds required to be set up by regulators to compensate the public; and defence costs to respond to lawsuits. The types of coverage provided highlight the types of risk that you face in this area: Security and Privacy Breach; Network Business Interruption; Cyber Extortion; Event and Crises Management; Regulatory Proceeding; and Consumer Redress Fund.

The currently available insurance policies are based on a combination of errors & omission and directors & officers policies. As such, they are "claims made", responding only to events giving rise to claims occurring and reported during the policy term. The policy may or may not contain terms that are suitable for your organization. For example, if your organization stores data in the cloud, is that covered? Are attacks by government organizations covered? Will you have carriage of the defence to any claim or regulatory proceeding or will that be under the control of the insurer? What remediation costs are covered and what are excluded? How do the wrongful acts of employees, senior officers or directors affect the coverage? When can a notice of a claim or possible claim be given? When **must** it be given? What is the effect on the coverage of an acquisition – a change of control–?

As with all other important commercial contracts that your organization enters into, it is important to understand the coverages, exclusions, terms and notification requirements of your insurance policy. Your broker and legal adviser should both be involved in assessing the effectiveness of the policy and its terms. The policy as presented need not be the final contract. Insurers are willing to amend terms if a proper case is presented to them.

Just as the threat of Ebola has recently commanded our attention, the threat of a cyber-attack on your organization cannot be ignored. It must be understood and managed on a continuous basis. Hardening your organization against such an attack must be your first line of defence. Having a robust plan to respond in the case of an attack is also important. This is an enterprise wide responsibility from the board to the lowliest employee – all have a role to play. While preparedness and prevention are key, prudence dictates that you at least consider insurance to cover any remaining risk. The terms of the insurance policy, the appropriateness of the coverage to your organization and the identification of any gaps should be carefully considered.

by Frank Palmay

For more information on this topic please contact:

Toronto	Frank Palmay	416.307.4037	frank.palmay@mcmillan.ca

a cautionary note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.