IT'S TIME FOR YOUR COMPANY'S CYBER-HEALTH CHECK-UP

Posted on July 12, 2016

Categories: Insights, Publications

Watch a video synopsis of this article here

Human nature being what it is, it's far too easy to put off medical checkups. For many of us, we tend not to see our doctor or optometrist until we feel ill or we notice we are having trouble reading traffic signs while driving. If we are lucky the illness is treatable or we get new glasses before having an accident. The same principle applies with keeping our computer systems secure. Imagine you are the CEO of a hospital and arrive at work. Your day starts badly when you are unable to log into your computer. Shortly thereafter you learn that the hospital's enterprise-wide information system has been compromised. All electronic communication within the hospital, including all administrative functions, have been locked down. Medical staff cannot access patient records and are forced to revert to paper based systems. This is not a farfetched story but rather a real series of events. On February 5, 2016, Hollywood Presbyterian Medical Center, an LA hospital, fell victim to a ransomware attack.[1] The malware locked the hospital's computer systems by encrypting the hospital's files. The perpetrators demanded ransom in order to obtain the decryption key.[2] The ransom paid was 40 Bitcoins, at that time equivalent to approximately $17,000 USD but the initial demand was for 9,000 Bitcoins or $3.7 million USD.[3] Although law enforcement was notified and the hospital engaged a team of computer security experts, ten days after the attack the organization decided that "the quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key."[4]

While organizations would ideally not wish to resort to dealing with criminals, in this case it appeared to be the easier solution. In addition, although in this incident it did not appear that the delivery of patient care was compromised, consequences could have been catastrophic had that occurred.

With the rapid rise in frequency, sophistication and virulence of cyber attacks, information security should be at the forefront of concerns across enterprises. A cyber breach can expose an organization not only to financial risk, for instance in terms of unauthorized access and theft of key company assets (such as confidential information and trade secrets) but also to regulatory risk and can also have a serious negative impact on customer and investor confidence. Increasingly cybersecurity incidents are becoming widely publicized leading to greater reputational risk for organizations and an increase in class action litigation both in Canada and abroad.[5] These can amount to substantial risks for organizations.

A report by Deloitte Centre for Financial Analysis[6] measuring attack success rate in the financial services sector (that is the time from first malicious act until data is negatively affected) found that in 2013, 88% of attack success occurred in less than a day, with 34% of them being successful within seconds. On the other hand, discovery success (measuring time from initial compromise to discovery of the incident) found that only 21% of attacks were discovered in less than a day, with only 40% restoration success in that time frame.[7] The increased speed of cyber attacks and longer discovery and response times highlights the complex set of challenges that companies face in protecting their information assets from malicious actors.

Companies, particularly those dealing with sensitive customer information, should consider developing and implementing sound cybersecurity models that adequately address today's cyber threats. Such a model ought to be sufficiently documented and revisited regularly due to the dynamic and evolving nature of the cybercrime landscape.

We developed a checklist as a starting point for conducting a cyber assessment of your organization's cyber wellness. While this is not intended to be a comprehensive list, it highlights relevant issues to be taken into consideration in assessing your organization's cyber preparedness and risk management strategy.

1. Have you developed a cyber profile for your organization?

Understanding and keeping abreast of the rapidly changing threat landscape is critical in today's electronic age. As the size and complexity of the digital environment grows, so do the attack techniques used by cyber criminals to penetrate corporate networks and systems. The digitization of business and increased dependence on technological innovation for businesses to remain relevant and competitive can leave some businesses and organizations more exposed to cyber threats than ever before. This is particularly true in light of the vast amounts of data that are being collected, combined and stored in the course of service provision.

Further, as recognized by the Office of the Privacy Commissioner of Canada, organizations are increasingly striving to reach consumers on mobile communication devices, resulting in cyber threats progressively moving into the mobile sphere.[8] Bring Your Own Device programs, remote employee access, cloud services, Internet of Things and the use of free public Wi-Fi all make mobile devices, and the networks to which they are connected, susceptible to being compromised.[9] This can lead to new potential security vulnerabilities and opportunities for malicious interference. Organizations therefore must assess their service delivery models, business environment and industry security standards, including a "threat list" and existing intrusion prevention controls, in order to develop a tailored cyber risk profile adapted to their unique situation. This will provide organizations with a clearer picture of the cyber threats they face and will enable them to make more informed risk management decisions and proactively anticipate and mitigate future attacks.

2. Have you identified your company's most significant assets?

Complete protection against malicious intrusions is unrealistic. Rather, a best practice is a risk-based approach which identifies and prioritizes the security of an organization's most critical assets from those threats that are most likely and most dangerous for the organization.[10] The information security program should begin with the identification of what types of information the company has and where it is stored. Companies should create, maintain and regularly update an accurate inventory of:

- Physical devices and systems
- Software platforms and applications
- Maps of network resources, connections and data flows
- Connections to company networks
- Prioritized list of resources, based on sensitivity and business value
- Logging capabilities and practices, assessed for adequacy, appropriate retention and secure maintenance[11]

The focus of the effort should be to evaluate and identify mission critical systems that could impact the reliable operation of the business and to prioritize remaining data and systems.[12] This should be conducted in conjunction with the organization's threat profile to allocate higher levels of protection to the most valuable assets.

3. Have you developed a robust breach incident response plan ... and do you review and rehearse it regularly?

The importance of having a robust response and crisis management plan in place and an incident response team, with clearly stated roles and responsibilities, cannot be overstated. The ability of an organization to immediately and effectively respond to a cyber attack can go a long way in containing, mitigating and remediating the damaging effects of a data breach. The emergency response team should comprise representatives from key departments within the organization whose input may be needed to successfully respond to the cyber breach and coordinate the internal investigation as well as the company's external communication efforts. Ideally this team includes:

- security and IT personnel tasked with first-response functions;
- representatives from risk management, communications/public relations, customer relations, operations and finance departments;
- a team leader for response coordination;
- the Chief Information Security Officer or other C-level executive with specialty expertise;
- senior management with decision-making authority; and
- internal and external counsel.[13]

Legal counsel plays a critical role and should be involved from the beginning stages of any investigation into a potential or confirmed cyber breach. Counsel's involvement may preserve the confidentiality of the investigation and provide strategic legal advice to the incident response team including any disclosure or notification obligations in connection with the data breach. Legal counsel should also review and coordinate all external communication, including any customer notification, press releases or media appearances. They can also assist in dealing with all relevant authorities including the police. This will become particularly relevant when the mandatory breach notification and record-keeping requirements enacted by the Digital Privacy Act[14] come into effect.[15]

4. Are you managing your corporate supply chain risk?

An organization's security is only as good as its weakest link. Outsourcing and supplier contracts can provide opportunities for perpetrators to hack into an organization's corporate systems through vendor connections or backdoor vulnerabilities built into components.[16] Therefore, identifying and addressing the cybersecurity risks associated with vendor and outsourcing arrangements is imperative. Vendor and partner agreements should establish the parties' responsibilities for safeguarding the relevant systems and data, provide for mandatory notification requirements in the event of a confirmed data breach as well as a suspected breach, allocate responsibility for incidents including adequate indemnification, and provide for security audit and verification requirements (including for downstream suppliers).[17] For significant business relationships, particularly those with access to customer information, a vendor management program may be an effective oversight and risk management tool. It is recommended that key contractual provisions be regularly reviewed and updated in order to maintain appropriate contractual safeguards.

Businesses should also be aware that cybersecurity-related risks may also arise in the course of merger and acquisition transactions. Assets that are being purchased from a third-party may have been compromised by a prior breach or subject to pending litigation. An assessment of the target's cybersecurity program should be part of any purchaser's due diligence.

5. Are you effectively using cyber insurance?

Cyber insurance can be an important tool in a company's risk-management strategy, however it should not be treated as a complete solution. While cyber insurance can absorb some of the financial loss suffered due to a cyber incident, it may not effectively address the reputational damage and resulting decline in business following a security breach. First-party insurance typically covers damage to digital assets, business interruptions and, sometimes, reputational harm.[18] Third-party insurance, may cover liability and costs associated with forensic investigations, customer notification, credit monitoring, public relations, legal defence, compensation and regulatory fines.[19] However, insuring against all possible cyber threats can be cost

prohibitive, so companies need to identify the most significant assets which need to be secured, and quantify and insure the remaining risk. Cyber insurance can also vary across markets, and global organizations in particular should be aware of local differences in liability coverage. The United States, for instance, has a more mature cybersecurity insurance market in comparison to Europe, in part because of many US states' mandatory data breach notification legislation.[20] It is also essential to clearly understand the terms of any cyber insurance policy, since some policies may not provide adequate coverage in some areas, particularly for intellectual property asset theft, reputational damage and business setbacks.[21]

Conclusion

As business assets are increasingly taking digital form, companies need to be aware of the cyber threats associated with protecting them. As well, more businesses cannot function if the computer system is inaccessible or compromised. Cybersecurity is no longer solely an "IT problem". Effective risk management integrates multiple lines of defence and individuals from multiple departments into a company's data protection and security strategy. A comprehensive governance framework, setting out clear risk management roles and responsibilities, the company's values and objectives, internal controls and risk management strategy, is essential to effective enterprise-wide data security.[22] Increasingly cybersecurity risk management issues are making their way to the senior executive and board level, who should consider their responsibility and duty of care with regard to safeguarding the company's assets and share price.

Security breaches can result in significant damage to an organization in the form of reputational harm, theft of intellectual property assets and trade secrets, class action lawsuits, regulatory investigations and forensic, legal and PR expenses. In 2014, a steel mill in Germany was the victim of a spear phishing attack. The mill was unaware that its system has been hacked until it discovered it was unable to shut one of its blast furnaces down properly. The result was significant damage to the furnace.[23] Therefore companies should assess their capabilities in detecting, responding to, and mitigating the potential damage that results from cyber attacks.

by Joanna Vatavu, Peter E.J. Wells and Sharon E. Groom

[1] Letter from Hollywood Presbyterian Medical Center (17 February 2016).

[2] *Ibid*.

[3] *Ibid*.

[4] *Ibid*.

[5] For example, class action litigation was commenced in 2014, in Quebec and Ontario, following data breaches affecting Target and Home Depot. See, for example, *Zuckerman c. Target Corp*., 2015 QCCS 1285, 254

ACWS (3d) 562 and *Lozanski v. The Home Depot Inc.*, CV-14-51262400CP (Ont. Sup. Ct.). More recently, in August 2015, class proceedings were commenced in Ontario following the high profile cyber attack targeting the dating website Ashley Madison, Eliot Shore and Avid Life Media Inc. and Avid Dating Life Inc., CV-15-22622CP (Ont. Sup. Ct.).

[6] Deloitte & Touche, "Transforming Cybersecurity in the Financial Services Industry: New Approaches for an Evolving Threat Landscape" (2014). The report analyzed data from an annual investigative report on data security by Verizon Risk.

[7] *Ibid*.

[8] Canada, Office of the Privacy Commissioner of Canada, "Privacy and Cyber Security: Emphasizing Privacy Protection in Cyber Security Activities", (Gatineau: OPC, December 2014).

[9] *Ibid*.

[10] Investment Industry Regulatory Organization of Canada, "Cybersecurity Best Practices Guide: For IIROC Dealer Members", [nd].

[11] *Ibid*.

[12] *Ibid*.

[13] DLA Piper, "Breach Incident Response: An Emergency Preparedness Guide", [nd].

[14] *Digital Privacy Act*, SC 2015, c 32.

[15] Lyndsay A. Wasser et al, "Cybersecurity – The Legal Landscape in Canada", Cybersecurity Bulletin (January 2016).

[16] Jim Halpert, "Effective Cybersecurity: 8 Questions for You and Your Team" (24 March 2015), DLA Piper Insights / Publications.

[17] *Ibid*.

[18] Lucian Constantin, "5 Things You Need to Know About Cybersecurity Insurance", CIO (25 April 2014).

[19] *Ibid*.

[20] *Ibid*.

[21] *Ibid*.

[22] Investment Industry Regulatory Organization of Canada, "Cybersecurity Best Practices Guide: For IIROC Dealer Members" [nd].

[23] "Cyber Hack Attack" Canadian Chemical News, March/April 2016.

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.