CYBERSECURITY and DATA PROTECTION IN A GLOBAL INFORMATION ECONOMY—FINAL ESSAY

LEGAL MEMORANDA TO THE BOARD OF DIRECTORS OF E CORP – A MAJOR CANADIAN TELECOMMUNICATIONS COMPANY

DAVID HIRSCH DAVIS

STUDENT # 1005942820

The following is a legal memoranda to the attention of the Board of Directors (hereinafter referred to as "BOD") of Evil Corp. (hereinafter referred to as "E Corp"). This legal memoranda provides an overview of the legal obligations of the BOD when it comes to the oversight and management of cyber risk. The legal memoranda is divided into the following sections for ease of reference: **PART ONE** – Introduction and Overview of Cyber Risk; **PART TWO** – Review of Fiduciary Duty and the Duty to exercise Care, Diligence and Skill by members of the BOD; **PART THREE** – Importance of a Cybersecurity Plan; **PART FOUR** – Importance of Cybersecurity Insurance; **PART FIVE** – Conclusion and Summary of Cyber Risk Management.

PART ONE – INTRODUCTION AND OVERVIEW OF CYBER RISK

The third industrial revolution is essentially upon us. E Corp as well as its competitors and third party partners and suppliers are doing most if not all of their business ***on line.*** The online world includes, mobile phones, laptops, IoT (Internet of Things) used by every employee within and outside of E Corp mainframe. The opportunity for a cyber attack is ripe for large company's like E Corp who has thousands of employees in offices across Canada.

Hackers bread and butter is to attack a company'computer system or the third party they do business with by identifying their weakness and then attack by using malware or phishing software. The Western industrial world has seen numerous cyber attacks against well heeled corporations in the past 10 years. The frequency of such attacks has steadily increased in severity and effect as well as the amount of ransom paid to the hacker which has increased to upwards of $1 million or more.

An example is the ransomware attack against Target in the USA. In that incident it was a third-party supplier whose system was compromised as a result of malware that was installed in their

system. The hackers were then able to use the credentials it stole from the third-party supplier as a staging point into Target's internal network. This led the hackers into the heart of operations of Target. The learning experience here is: A) ensure that any agreements with third parties should necessitate knowledge of and consent of the use of cyber risk insurance policies and to know what hardware and software is being used by the third party provider and to ensure that there are as few possible entries into the computer systems of that provider from the outside as humanly as possible. B) to ensure that any portal created for a third party provider has built into it a robust encryption coding system to prevent hackers from easily gaining entrance into the mainframe of E Corp system.

There is also the possibility of a derivative action by one of the shareholders of E Corp wherein a Superior Court justice agrees that the BOD did not adequately prepare for a cybersecurity attack. Cyber attacks can result in huge financial losses, damage to the reputation of E Corp as well as other pecuniary and non-pecuniary damages that a Court could impose against E Corp. The officers of the company and members of their board could be held personally and collectively liable.

It is important for the BOD of E Corp to realize and understand that "*Information security involves people, processes, and technologies-getting all three in the right measure is the real art of a successful security program.*"[1]

PART TWO – REVIEW OF FIDUCIARY DUTY AND THE DUTY TO EXERCISE CARE, DILIGENCE AND SKILL BY MEMBERS OF THE BOD

The BOD has two duties that form part of their responsibility for the governance of E Corp: "a fiduciary duty to the corporation under s. 122(1)(*a*) (the fiduciary duty or duty of loyalty); and a

[1] Rebecca Weinstein, "*Cybersecurity: Getting Beyond Technical Compliance Gaps",* 19 N.Y.U. J. Legis. & Pub. Pol'y 913 (2016) at p. 917.

duty to exercise the care, diligence and skill of a reasonably prudent person in comparable circumstances under s. 122(1) (*b*) (the duty of care)."[2]

The SCC explained how the fiduciary duty is a broad and contextual concept with the following statement: "It is not confined to short-term profit or share value. Where the corporation is an ongoing concern, it looks to the long-term interests of the corporation. The content of this duty varies with the situation at hand. At a minimum, it requires the directors to ensure that the corporation meets its statutory obligations. But, depending on the context, there may also be other requirements. In any event, the fiduciary duty owed by directors is mandatory; directors must look to what is in the best interests of the corporation."[3] The Court also stated that directors "may look to the interests of, *inter alia*, shareholders, employees, creditors, consumers, governments and the environment to inform their decisions."[4]

There is some ambiguity regarding the nature and extent of such duties. The court did not provide guidance as to how to give effect to this concept, but the reference to "good corporate citizen" in the judgment suggests some degree of accountability to stakeholders. The BOD would be well advised to constantly re-evaluate its position vis-à-vis cybersecurity responsibility as such is in the best interests of the corporation and, at the same time, will be ensuring good value for its stock to its shareholders.

---

[2] *BCE Inc. v. 1976 Debentureholders* [2008] 3 SCR 560 (SCC) at para. 36; referring to the CBCA.
[3] Ibid., at para. 38
[4] Ibid., at para. 40

The BOD must be aware that the exercise of care, diligence and skill is subject to the *business judgment rule* (BJR). Directors will not be in breach provided they act prudently and on a reasonably-informed basis. The SCC has held that perfection is not demanded but look at the reasonableness of the business decision under the particular circumstances involved.[5]

The federal government may be introducing a new bill in Parliament that would codify elements of the *BCE* decision. If the bill is passed, the CBCA will expressly provide that, when acting with a view to the best interests of the corporation, one may consider the interests of shareholders, employees, retirees and pensioners, creditors, consumers, and governments; the environment; and the long-term interests of the corporation.

In light of the provisions in the CBCA and recent SCC decisions, it is prudent for the CEO and BOD to designate particular individuals to fill the roles of Chief Information Officer (CIO) and Chief Security Officer (CSO). The CIO would be in charge of all data information that is collected from customers of E Corp as well as all corporate data and information that forms part of E Corp. The CSO would be in charge of implementation of a cybersecurity plan of action and overseeing all aspects of an incident response to any type of breach.

It is further recommended that the BOD creates a subcommittee that is charged with the responsibility to stay informed of all legal changes to the CBCA as well as privacy legislation for each province and federally in relation to PIPEDA and the Digital Privacy Act. The subcommittee would maintain communication with the CIO and CSO but would be answerable to the BOD. It is integral that the CIO and CSO are answerable to the BOD. As a national company, E Corp must have committee members who possess experience in the IT field. Top level managers from each

[5] *Peoples Dept. Stores 1992 Inc.* [2004] SCJ NO. 64.

province would communicate with the subcommittee to ensure all cybersecurity and data management issues are dealt with expeditiously.

The BOD needs to ensure that access to capital assets of E Corp is not interrupted. It is therefore wise to address the interests of creditors.[6] Although there has not been a successful derivative action by shareholders for breach of duties to date, it is still important for the BOD to ensure shareholder interests are taken into account. It is apt to note the SCC decision in *Kosmopolous* wherein the Court held that shareholders have an insurable interest in the assets of a corporation.[7]

When it comes to the defence of due diligence of board of directors, it is not considered sufficient for a board member to rely on the expertise of a fellow board member when defending their own decision in light of controversial matters. Refer to the recent Superior Court of Quebec decision in *Autorite des Marches financiers v. Descheneaux*[8]. The E Corp directors would be prudent to ensure that most if not all of its members have some degree of knowledge on information technology and cybersecurity.

In a practical sense, cyber breach costs can incentivize the Board to become more proactive. [9] E Corp has a reputation to uphold, shareholders to please and employs thousands. An appropriate portion of its annual budget must be devoted to cybersecurity and data management. It would be unwise for E Corp to fall victim to the adage, "it's just a technical issue – it will resolve itself if we

[6] Imran Ahmad, *Cybersecurity in Canada: A Guide to Best Practices, Planning, and Management,* (Toronto, ON: Lexis Nexis Canada Inc., 2017), at p. 65.
[7] Ibid., at p. 66.
[8] June 9th, 2020 (2020) QCCS 1779 Justice Mongeon cited in an article written by Sophie Melchers, *Passive Reliance on Fellow Director is Insufficient for the Due Diligence Defence,* July 06, 2020 of Norton Rose Fulbright Canada LLP.
[9] Supra, see note 1 at p. 919.

are using the latest software." Such thinking is myopic and could be interpreted as a board of directors being in violation of its duty of care principles.

In the modern era of the ever-present cyber threat, the courts may hold Board's accountable for ineffective cyber protection. However, the primary threat of such derivatives suits is not legal liability but, instead, the negative press and costs from defending such suits.[10]

PART THREE – IMPORTANCE OF A CYBERSECURITY PLAN

One can never guarantee the prevention of a cyber attack. It is highly recommended to the BOD that a list of "to do items" is created similar to the one discussed in the article *Cybersecurity Legal Task Force Vendor Contracting Project: Cybersecurity Checklist be created and followed.*[11]

The BOD must first conduct a thorough audit of all of the assets of E Corp in order to identify and determine strengths and weaknesses that are present in all facets of its operations.

a) Establishing a Cyber Incident Response Team (CIRT)

The CSO will have the responsibility to assemble a team of knowledgeable people with designated roles in the event of a breach. The cyber incident response team (CIRT) ought to include mid level and senior managers from its office's across Canada as well as IT experts to ensure that all aspects of E Corp is covered in the event of a breach. It is important that the BOD realize that even a minor breach must be met with a robust and effective response so that the hackers are not incentivized to orchestrate repeated attacks against E Corp.

[10] Ibid., at p. 922.
[11] Business Law Today, November, 2016 by the American Bar Association.

The CIRT will take the results of the audit discussed above and decide which assets of E Corp are most at risk and which assets are least at risk. Listing of all equipment being used by third party vendors and suppliers to E Corp ought to be included in such audit. The CIRT will also determine the appropriate threshold for when and who to notify in the event of a breach. The CIRT, which is under the direction and supervision of the CSO, will report to the BOD all of its findings.

The CIRT will also include outside legal counsel to manage the risk assessment. Engaging legal counsel may be effective in making all communications between counsel and a member of the CIRT part of solicitor-client privilege protection. However, such protection is not necessarily a guarantee. It will depend upon the nature of the communications and whether it is in contemplation of litigation.

It is recommended that the CSO will incorporate the NIST guidelines for incident response. The CSO should make cyber attack drills common place so that CIRT can stay ready.

The CSO should assign responsibilities in advance, identify key stakeholders – internal and external as well as create annual checklists since laws and policies can change.

b) Regular Schedule of Board Meetings and Proper Record Keeping

All BOD meetings need to be recorded with copious note taking by a designated person such as a Secretary. Appropriate record keeping could be crucial to assist and defend members of the BOD in the event of a serious breach which results in massive data loss. Any recommendations the CIRT sends to the BOD are recorded so that the BOD cannot be accused of being irresponsible and unresponsive.[12]

[12] Supra., see note 6 at page 70.

c) Mandatory Regulatory Reporting

The CSO and their team must ensure compliance with provincial regulators since E Corp has office's in every province across Canada. For instance, mandatory reporting is required to the Alberta privacy commissioner under their legislation but is unclear about how it's administered. BC and Quebec have similar legislation to bear in mind.

The new Digital Privacy Act came into legal force on June 15th, 2015 and the amendments to PIPEDA were passed and came into legal force on November 1st, 2018. They appear in s. 10.1 of PIPEDA. This Act is especially important for telecommunication companies like E Corp. The test to determine whether a report is made to the Office of the Privacy Commissioner (OPC) under PIPEDA is whether there exists a "real risk of significant harm" which can include financial loss.

d) Data Protection

It is crucial to be able to return to the data you had just before the attack. You can never know exactly whether the data was corrupted as a result of an attack.[13] Maintaining accurate information is critical to E Corp.

As a result of the regulatory changes, it has become absolutely critical to log all PII (personal identification information) of all of the customers of E Corp as well as all data that is stored on its servers. All PII and E Corp data should be saved in multiple places and encrypted for maximum protection.

[13] Derek E Bambauer, "Schrodinger's Cybersecurity," (2015) 48:3 UC Davis L Rev 791 at p.793-4.

d) Preservation of Evidence

E Corp must have a process in place that all evidence and information is preserved in the event of a breach. The BOD could open itself up to unnecessary legal action if key or relevant evidence is surreptiously destroyed by some unscrupulous employees. Furthermore, shareholders could launch a derivative class action if it is determined that E Corp had a culture of deceit such that profits took precedence over protection of shareholder's interests and its assets.

e) Human Resource Issues

It is also important to have all employees sign non disclosure agreements (NDA's) that prevents them from releasing any info to any person or media outlet outside of E Corp. The message needs to be under the control of E Corp. The CSO & CIO, under the supervision of the CEO, should make a proper public notification to protect its business and the interests of its shareholders.

IT Recommendations:

It is recommended that E Corp implements computer defences to help keep data secure and safe such as authentication through credentials and cryptography, logging changes via journaling file systems, robust backup and recovery procedures, and verification of data through checksums.[14] Storing the checksum independent from the information itself to achieve end-to-end integrity (ensuring that the data is not altered after the check) and Secure Sockets Layer ("SSL") encryption typically protects sensitive Web-based exchanges of information, such as those that take place

[14] Ibid., at p. 796

during an e-commerce transaction.[15] It is also important that an off-site backup strategy is implemented as well as data being saved in the cloud and at different locations across Canada. [16]

PART FOUR – IMPORTANCE OF CYBERSECURITY INSURANCE

The use of mobile devices by employees of E Corp can increase the risk of a cyber attack. As a result a comprehensive cyber risk insurance policy must be implemented. First party insurance will cover expenses that E Corp will incur in the event of a breach.[17] The following is an example list of such expenses: Notification costs; Forensic Investigative Costs; Business Interruption; Crisis Management Expenses; Data Restoration; Cyber Extortion; Regulatory Proceedings Coverage, Publicists, outside legal counsel as well as ransoms that may have to be paid to the hacker(s) to secure the release of seized data.

E Corp must be aware of any agreements that their suppliers and other third parties have implemented that may make E Corp susceptible to a cyber attack. Identification of all third party suppliers and whether they too have insurance in place is also critical. Must ensure that any hacks to the third party is not going to affect the systems at E Corp or any other technological aspect of the company. As a result, indemnity clauses are typical in insurance policy contracts to protect E Corp from any possible breach violations committed by third parties.

Supply chain cybersecurity.[18] It is hard to manage the supply chain as there are too many pieces of a computer that are made by different third party entities. Risk Segmentation: having a risk

---

[15] Ibid., at p. 814-15 and 819.
[16] Ibid., at p. 843.
[17] Greg Markell, President & CEO of Ridge Canada, Slide Deck delivered to GPLLM Cyber class on May 8th, 2020, at slide 9.
[18] Maureen Wallace, *Mitigating Cyber Risk in IT Supply Chains*, (2016) 6 Global Bus. L. Rev. 4 at p. 7 – Discussion of Hardware, firmware and embedded systems which form part of supply chain in IT where certain cyber risks lie.

profile in a contractual relationship between different suppliers as they have this common connection between them. E Corp needs to fully understand what is the nature of the information to be processed or stored? Will a supplier give access to another supplier downstream? If so, define the protocols around that information sharing.[19]

The E Corp Board will be concerned about costs in cyber insurance. However, consider this quote: "Currently, due to the complex nature of cyber insurance and the time and effort that goes into ensuring calculations are correct and appropriate, the costs for these insurance policies are high. In time as the certainty levels rise, this will become far less of an issue and accessibility will be on a higher level."[20]

The BOD cannot forget that they must maintain the minimum level of security of its own volition. Breach expenses may not be covered by insurance such as not having proper "firewalls" in place [21] or the careless mishandling of sensitive information by employees and malicious acts by employees or theft of trade secrets or intellectual property.[22] Coverage can also be denied if a laptop with highly sensitive data goes missing or is lost on public transit. E Corp could be blamed for having no policies in place to account for removal of mobile devices from its physical premises.

PART FIVE – CONCLUSION AND SUMMARY OF CYBER RISK MANAGEMENT

It is impossible to be 100% secure against any cyber attack. But it is also clear that doing nothing is much worse. This legal memoranda has recommended some basic steps that E Corp can undertake such as assigning key roles to various managers and mid level officers, creation of a

[19] Supra, see note 6 at p. 58.
[20] *Cyber Liability Insurance,* (2018) 5 Ct Uncourt 32 at p. 33
[21] Nishi Dennis, "*The Ins and Outs of Cybersecurity Insurance et al.",* (June 05, 2019) Wall Street Journal (Online): NY, NY at p. 2.
[22] Ibid.

subcommittee to stay abreast of latest legal and policy changes as well as a Cyber Incident Response Team and having robust insurance coverage to protect E Corp from closure due to a hack. Proper reporting to government regulators and acting in the best interests of its stakeholders will allow the BOD to benefit from the business judgment rule (BJR).

In the event of a breach, the board must be ready to implement the policies and procedures to deal with the cyber attack. Perfection is not the key but rather whether the BOD followed a reasonable approach to assessing risks and discharging its duty to take care and due diligence in protecting the data of E Corp and its customers.

In conclusion, the BOD needs to have: sufficient policies & procedures in place; investigate the breach, and have that investigation reviewed by an audit committee. Education and training of particular staff to deal with protection of data and technology at E Corp. is an ongoing effort which helps to ensure that full compliance and defence against cyber attacks are in place. The corporate budget should and ought to include all of the recommendations contained in this legal memoranda.