BEARDWINTER LLP
The Defender
Vol.12 | Issue 1
January, 2018

Cyber Hacking and Security:
Consequences For Canadian Companies And Insurers

Cary N. Schneider is a partner at Beard Winter LLP who specializes in commercial and insurance litigation matters including the growing area of cyber and privacy law. He is a member of the International Association of Privacy Professionals (IAPP) and is in the process of being certified as a Certified Information Privacy Professional/Canada (CIPP/C). He focuses on being effective and efficient in his law practice with the goal of achieving excellent results for his clients in a timely manner.

Your comments are appreciated and if there are any commercial or insurance related topics that you would be interested in reading about, please feel free to email us and we will certainly explore the possibility of writing an article. Contact: defender@beardwinter.com

Who Is Being Hacked?

The prevalence of cyber-predators unleashing new and comprehensive hacks that infiltrate a company's network grows seemingly unabated. Front page news stories reveal that reputable billion-dollar organizations have fallen victim to cyber-attacks and that our personal information may be in the hands of unsavoury characters. The question is not "if" a company will be subject to a cyber-attack but rather "when".

Headline news stories that capture the dramatic breaches include:

- Credit reporting company Equifax suffered a massive breach of 143 million personal data information;
- Bell Canada suffered a breach that affected 1.9 million customers;
- 815,000 Canadian users of Uber were exposed in a hack of data of 57 million users;
- Every single Yahoo account of over 3 billion users was compromised;
- Hackers stole 40 million credit and debit card information under the control of Target;

- On December 21, 2017, Nissan Canada Finance revealed that 1.13 million customers had their personal information stolen;
- Real names, home addresses, search history and credit card transaction records for clients of Ashley Madison;
- McDonald's Canada, Casino Rama, Canadian Tire, Shopper's Drug Mart, JP Morgan, Sony, Home Depot, and the list goes on.[i]

As a small to medium size business owner, this list of breaches might appear to be somewhat disturbing but not particularly relevant. What does a hacker have to gain to attack the owner of a local restaurant, medical treatment centre, retirement home, small accounting firm, investigation business, or sporting goods store? Unfortunately, the answer is that small to medium-sized companies are considered "low hanging fruit" targets for cyber-predators and often result in quick as well as easy rewards. Small and medium-size businesses (businesses with under 1000 employees) constitute 61% of all cyber-attacks[ii] and 60% of small companies are unable to sustain their business six months post such an attack.[iii] It is estimated in the USA that over a 12 month period of time in 2016-2017 that half of all small businesses have suffered a breach.[iv] Why are these small businesses being hacked? It is estimated that 87% do not feel that they are at risk and 1/3 do not have the tools in place to properly address cybersecurity.[v]

While as many hackers perpetrate their craft as a challenge to prove how intelligent they are, and others for ideological reasons, it is estimated that 73% of breaches are financially motivated.[vi] The four most common institutions attacked include financial, healthcare, public sector, and retail & accommodation.[vii] While 75% of breaches are perpetrated by outsiders it is perhaps even more concerning to note that 25% of breaches involve internal actors.[viii]

Profit For Cybercriminal And Cost To Business

The more sensitive the data that has been subject to a breach, the more significant the consequences to the individual hacked and to the company that was exposed. Private information such as credit card information, bank account data, health records, and social security information in the possession of criminal actors are being manipulated for financial gain. Such information will be utilized for the purposes of identity theft, monetary theft, and credit card fraud among other things.

Ransomware is one of the more popular and exponentially growing forms of attack used by cyber-predators. This is a type of malware that locks and denies access to victim computers, digital files and systems once encrypted. When a user learns their computer is locked, the perpetrator will demand payment to unlock files and allegedly allow consumers to regain access. Ransomware is often spread through email attachments and botnets. Once the virus is installed, a pop-up will advise the user that payment is required to obtain a 'private key', which if not paid, will result in the encrypted files being deleted. There is no guarantee against exploitation. The user is given approximately 24 to 72 hours to pay before the private key is destroyed and the files are lost forever. Payment of ransom is mostly by way of anonymous cryptocurrency (most often Bitcoin) and can range in the thousands of dollars depending on the size of the company.[ix] For example, it was recently revealed that Uber paid $100,000 in ransomware, the University of Calgary paid $20,000, and an undisclosed Canadian company paid $425,000 in July 2017 in order to restore its computer systems. Canada is a hotbed for ransomware as only three countries in the world have been hit more times than us (USA, Germany, and the UK are the others in order).[x]

What is even further concerning is that the cyber-predator need not be a criminal technological genius anymore. Cybercrime has become commoditized as customized ransomware, (or other forms of malware), is often available for purchase or even made available for free. As such, the business of cyber-crime has exploded as it has allowed individuals with little to no experience in coding to make a living extorting companies for profit.[xi] Hackers range from nation states, terrorist groups, organized crime, amateurs, journalists, disaffected current/ former employees, to just about anyone.

The cost involved for a company to respond to a breach is much more significant than the ransom paid to get access to one's computer again. As per the Canadian Chamber of Commerce, the average cost to respond to a breach is $6.03 million, the average cost per record is $258, and the average number of records breached is 20,456.[xii] Based on these figures, if you are an owner of a small to medium-sized business who suffers a cyber breach of 4000 sensitive records, the cost to address this breach would be $1,032,000. Most businesses have not accounted for such an expense and would have a hard time paying for same.

The loss of business reputation for being subject to a privacy breach could be even more damaging. The realization of a client base that their private information has been compromised and that the company has not taken proper

steps to account for a possible breach before it occurred or taken proper steps thereafter to address the situation could be fatal to a business.

Cyber Insurance

One of the steps taken to mitigate the cost of a breach is the purchase of a cyber insurance policy before an incident occurs. Insurers and companies should be aware that the typical CGL (commercial general liability), E & O (errors and omissions), and D & O (directors and officers), policies provide limited to nil insurance coverages.

The popularity of cyber insurance policies has grown in direct proportion to the growth in cyber-attacks in that specific industry. After Target was attacked in 2013 retailers started to purchase coverage to protect their point of sale credit card processing devices. The breach of Sony in 2014 led to big tech firms taking notice and the 2017 global WannaCry ransomware threat increased public awareness of cyber-security.[xiii] It is suspected that the recent breach of Equifax will result in companies realizing that no one is safe from an attack. The global market for stand-alone cyber coverage is estimated to have grown to between US 2.5 billion and US 3.5 billion annually.[xiv]

Insurers and companies need to take a close review of cyber insurance policies as these are not the same standard *proforma* CGL policies that have existed for hundreds of years. Cyber policies are new and different from one another. In general, these policies cover for the cost of restoring data compromised from a breach, payment for cyber response teams (including legal), breach notification, indemnification to address reputation harm, and coverage as a result of a lawsuit from an affected third party. It is imperative to determine whether the breach occurred during the life of the policy and to what extent the policy has a retroactive date. Indeed, many breaches occur anywhere from days to years before they are discovered and this may impact whether there is insurance coverage at all.

Many policies provide insurance coverage for certain cyber events but are conditional on certain actions to be taken by the insured. For example, some coverages include payment for ransomware but have a confidentiality term that the insured will not disclose to the hacker that the policy of insurance will pay for the ransom. This makes sense as the insurance company does not want cyber-predators to target companies that are insured with the same insurer for future attacks. Another example is that cyber insurance policies typically require that the company has a proper cyber breach protocol set-in-place and can deny coverage if this was not followed.

Some policies do not cover the cost of investigating whether a breach has occurred but will indemnify for the rectification of that breach. Some policies set-out a designated response team that a company must use in the event of a breach and others that require the insurer to pre-approve who is chosen. There are detailed definitions of what is and is not covered that are not necessarily obvious.

Once a breach occurs parties are forced to act in an emergency situation and reading the fine print of a policy of insurance for the first time is typically not ideal. Companies need to be familiar as to what is covered under their policy before a breach occurs so that this can be used to help direct their actions where they are dealing with this situation proactively and not retroactively. A consultation with an expert in insurance law about the type of policy that would be applicable to this particular business, and map out how the coverage would apply in a breach situation in advance, is important.

Similarly, due to the relative newness and untested nature of the policies, insurance adjusters will also likely be dealing with unique claims for coverage and compensation. Everything is moving at lighting speed subsequent to the realization of a breach; including a request from the insured for an insurer to approve for the cost of a cyber-security company to repair the breach, notification to data subjects, and/or pay the ransom. These are immediate concerns that may impact the financial livelihood of a small to medium-sized company. Having an insurance lawyer/professional knowledgeable in advance as to the particular wording of the policy for immediate consultation would be crucial to address these situations.

Canadian Law

1. The Regulatory Framework And The Private Sector

Canadian law has evolved and is constantly changing in order to address the growing rise of cyber breaches. In fact, we are at the precipice of significant legal changes coming into effect within the next several months requiring federal mandatory breach notification in many situations that will undoubtedly increase the number of reported breaches and impact businesses. As more companies now are forced to disclose a breach, (which otherwise may have been kept secret), there will be an increase in regulatory oversight, legal consequences, financial repercussions, and likely a rise in purchases/claims related to cyber insurance policies.

In the private sector, there are a number of statutes that require organizations to protect personal information within their possession or control. The most prominent, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), is federal legislation that applies to protection of personal information for federally-regulated organizations (such as banks and telecommunications businesses), as well as for all companies nationwide engaged in commercial activities. The exceptions to the latter are for provinces that have "substantially similar" legislation to PIPEDA (which constitutes Alberta, British Columbia, and Quebec). While as the federal and provincial legislation is mostly in sync, there are some significant differences such as Alberta already requiring breach reporting requirements. Institutions/businesses that deal with private health information of individuals are subject to various other requirements, different rules, and often subject to different regulators (ie: in Ontario the applicable statute is *PHIPA – Personal Health Information Protection Act*). Companies that operate in multiple provinces (and in the USA/abroad) and various disciplines must ensure that they are cognizant of the applicable legal requirements. Similarly, insurance adjusters who are responding to claimants with cyber insurance must also be aware as to the differences in the law when addressing such claims.

PIPEDA was recently amended to require that organizations notify the Office of the Privacy Commissioner of Canada ("OPC") if a cyber breach occurred that poses a "real risk of significant harm" to the affected individuals and keep a record of all breaches. It is expected that this amendment will come into effect in early 2018. There is teeth to this amendment as knowingly failing to report or record a breach will be an offence punishable by fines of up to $100,000.

Likely even costlier will be the obligation to address the breach and the damage to reputation once this is exposed to the public. Indeed, the applicable regulator may conduct an investigation of the company and recommend or even order a company to take action to address any flaws in the cybersecurity. As per the OPC's 2016-17 Annual Report, it is the intention of the federal regulator to take a more proactive role in investigating possible privacy violations and accordingly, this will subject companies to privacy information audits [xv]. Companies/Insurers will want to check their cyber insurance policies to determine to what extent the costs associated with dealing with the OPC and/or any fines are covered.

Companies that have suffered a breach or informed that they are subject to an audit by the OPC should contact external counsel right away for direction as to what to do and for protection of their business / legal interests. Communications between a client and their lawyer are protected by "solicitor-client privilege" and therefore confidential. Among other things, these communications can help direct a company as to whether the breach constitutes a "real risk of significant harm", what must be disclosed to the regulator, communication with the police, and what to do about affected clients. Rushing to disclose all cyber incidents to the regulator when it is not necessary can have significant implications for one's business just as unreasonably delaying to address a breach can too.

2. Third Parties Claims And Class Actions

In addition to the statutory and regulatory frameworks described above, there is an evolving body of case law in Canada that is developing in response to individual and class action claims related to privacy and data protection breaches. Insurers and clients need to closely review the existing insurance and cyber insurance policies to determine if coverage applies to third party claims and policy limits.

In Ontario, there is a right of compensation for an individual if his/her private personal information is disclosed even if that person has not suffered any financial or reputation harm. A statutory tort of invasion of privacy has been recognized in four provinces (British Columbia, Manitoba, Newfoundland and Saskatchewan), and has now been recognized as applicable in Ontario in the Court of Appeal decision of *Jones v. Tsige* (2012) ("*Jones*"). In *Jones*, the tort of "intrusion upon seclusion" requires two elements: (1) the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns and (2) a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish. It is important to note that no proof of economic loss is required as a pre-requisite for such a claim.

As of 2012, the Court of Appeal set the maximum value for such a tort to be $20,000 and for the claimant in this case the range was found to be $10,000. To be clear, this is a case where the claimant did not suffer any provable economic loss and the breach was limited to one person knowing the claimant's personal affairs. The public's consciousness of the significance and growing threat of breaches has grown exponentially over the past six years and one should not consider this upper range to necessarily be followed into the future.

Building upon the "intrusion upon seclusion" tort recognized above in Jones, the Superior Court decision in *Doe 464533 v N.D. (2016)* recognized for the first time the new privacy tort of "public disclosure of private facts." This case arose out of a "revenge porn" case in which a defendant posted a sexually explicit video of the plaintiff to a pornographic website. General damages were awarded in the amount of $50,000, aggravated damages in the amount of $25,000, and punitive damages for an additional $25,000 for a total judgment of $100,000. The defendant did not initially defend this claim, (was noted in default), and following an appeal, this original decision is being reconsidered. The state of the law is currently in flux but this decision highlights the fact that Courts are recognizing the importance of privacy rights, prepared to legitimize new causes of action, and willing to award substantial damages awards.

While as individual lawsuits for privacy breaches will likely increase as individuals' private information is disclosed, the bigger concern for organizations and insurers is the rise of class action lawsuits. In Canada, these class action lawsuits tend to fall under three broad categories: (1) employee errors; (2) employee "snooping" and other misconduct; and (3) data breaches. By way of example, these types of class actions include the following:

- Employee Errors: class action lawsuits filed in Ontario and British Columbia after a mailing was sent to approximately 40,000 individuals, which identified them as participants in a federal program for access to medical marijuana;
- Employee "Snooping" and other Misconduct: in Ontario, a class action was filed after a mortgage officer gave customers' confidential information to his girlfriend who then distributed it to persons who used it to commit identity theft and fraud;
- Data Breaches: various breaches of confidential personal information such as class actions against Target, Sony, Yahoo, Home Depot, Ashley Madison, Casino Rama and Equifax.

Conclusion: What Should Companies And Insurers Do?

Companies that are increasingly relying on technology to power their operations should take heed from the famous words articulated by Spiderman following the development of his super-powers: "with great power comes great responsibility". The use of technology by a business to gather personal information from their customers helps immeasurably with sales, targeted advertising, and efficiency. However, the growing dependence on the effectiveness of technology does come at a cost when things go wrong. Companies recognize the benefit of using technology to increase profitability and streamline operations, but often are somewhat lax or lacking the proper knowledge about putting forth the proper procedures, tools, and personnel in place to protect against breaches. At a cyber-security conference that I recently attended an executive from a major Canadian company that had been breached was asked how much money is spent on cyber-security; the answer was very informative "before or after the breach?".

Companies are increasingly recognizing the risk of a breach and taking action to protect themselves. Indeed, taking action proactively to address cyber-security before a

breach occurs results in substantial cost savings compared to if a company waits until after detecting that they have been hacked.[xvi] In advance of a cyber-incident, companies should have in place a data breach management team, develop policies, and have effective procedures to address cybersecurity concerns. The basic cybersecurity framework tends to break the steps involved into five stages including: (1) identifying the valuable privacy assets, (2) protecting the privacy information, (3) detecting any compromised account or device, (4) responding to the problem and, (5) recovering, restoring, or otherwise fixing the compromised assets. [xvii] A proper proactive plan in place would include multi-player consultation with management, technical, legal, and consideration of the interplay of insurance. With respect to cyber insurance, there are multiple types of different policies, and various key elements, that require careful consideration.

For insurance professionals, adjusting cyber insurance claims is challenging, and without much precedent. The cost to repair and address a breach can be hugely expensive and may impact the financial sustainability of a company / insured. Decisions made as to whether to extend insurance coverage for all / some of the claim, or deny outright any indemnification whatsoever, are often not clear. Insurers are often working with imperfect information, without precedent, and in tight timeframes. The threat of a lawsuit for coverage and potentially bad faith is always a factor in the forefront of an insurer's mindset.

Companies and insurers both need to be cognizant of third-party claims, investigations by regulators, and class action lawsuits. The actions of a company to take pro-active steps in advance of a breach and respond in a timely/effective manner after discovering a breach are mitigating factors that influence legal liability. Furthermore, these are factors that may impact insurance coverage.

The gathering of data for the purpose of running a profitable and efficient business has a price. The physical protection of one's office space by way of security passes, guards, alarms, and locked doors are no longer enough. Thieves no longer need a gun to steal from a business – a computer will do just fine. The protection of a company's private data in organizations of all sizes needs to be recognized as a vital element to running a business. Insurance is one key element to be considered to help mitigate the cost of a breach but both companies and insurers need to closely review the policy language and particulars of claims. While as the cost of cyber-security and legal consultation is not an expense that anyone prefers to incur, the risk of not being prepared to respond to the inevitable hack of private data can have dire consequences.

(Endnotes)

i. IT World Canada, December 22, 2017, and Wikipedia List of Data Breaches

ii. Verizon 2017 Data Breach Investigations Report

iii. GEM Strategy Management March 24, 2017

iv. CNBC, Congress addresses cyberwar on small business: 14 million hacked over last 12 months, April 5, 2017

v. CNBC, Congress addresses cyberwar on small business: 14 million hacked over last 12 months April 5, 2017

vi. Verizon 2017 Data Breach Investigations Report

vii. Verizon 2017 Data Breach Investigations Report

viii. Verizon 2017 Data Breach Investigations Report

ix. Government of Canada, Canada Anti-Fraud Centre: Ransomware Scam June 2, 2016

x. Global News: Ransomware On The Rise in Canada April 17, 2016

xi. Security News, By The Numbers: The Price of Ransomware, July 11, 2016

xii. The Canadian Chamber of Commerce, Cyber Security in Canada, April 2017

xiii. IT World Canada: Cyber Insurance a growing industry now necessary for business, June 19, 2017

xiv. Insurance-Canada.ca Cyber Insurance: A Growth Opportunity With Unique Risks, October 2, 2017

xv. Office of the Privacy Commissioner 2016-17 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*

xvi. IT World Canada, Average data breach could still cost a Canadian organization millions: Report, June 20, 2017

xvii. Cybersecurity For Beginners, Raef Meeuwise, 2017

Contact us at: defender@beardwinter.com