A New Realm:
Cyberspace, Cyber Liability and Cyber Liability Insurance

November 2017

Cox & Palmer is a member of the Risk Management Counsel of Canada

coxandpalmerlaw.com | @coxandpalmer
New Brunswick | Newfoundland & Labrador | Nova Scotia | Prince Edward Island

COX & PALMER
The difference is a great relationship

Table of Contents

Ryan Burgoyne
Partner | Fredericton
506.453.9647
rburgoyne@coxandpalmer.com

With valued contributions from
Veronica Medon.

Introduction

For any business today, the reality of day-to-day functioning and management involves mass-communication, networking, marketing, and the organization of important confidential information on secured computer networks. Digitalization of information and communication is becoming second-nature due to the efficiency and simplicity that computers provide, as well as their instantaneity. However, as the amount of important and confidential information being stored on computer networks continues to grow, so does the risk of becoming an appealing target for scammers, fraudsters and cybercriminals. This correlation makes it arguable that cyber liability insurance will soon become one of the most important forms of insurance on the market.

This paper aims to clarify the impact cyberspace and cyber-liability has, has had and will continue to have on businesses in this modern age. The continuing, and ever-growing risk of data and security breaches in the midst of more and more information being stored on computer networks illustrates the need to understand cyber-liability generally, and what exactly may be covered in a cyber liability insurance policy. For that reason, this paper begins by clarifying the risks and implications of data loss, cyber-attacks, viruses and other cyber threats. It then examines the growing relevance of cyber liability insurance, and ends with a summary of how cyber-liability has been addressed in the courtroom thus far.

Data Loss, Cyber Attacks, Viruses and other Cyber Threats

When the World Wide Web was introduced in the 1990s[1] the appeal of computers increased exponentially because of the number of tasks that became feasible with the click of a button, such as shopping and banking. As of July 1, 2016, it was estimated that over 3.4 billion people had the ability to access the internet at home on either a computer or mobile device.[2] The internet and computing have become ingrained in our daily life and it is becoming increasingly difficult to imagine or remember (depending on your age) a life without them.

Corresponding to the increase of computer users over the years, statistics relating to the cyber world demonstrate an increase in cybercrime and its impact on businesses. As a result, the demand for cyber liability insurance is growing and will continue to in the years to come. A 2017 cybersecurity report from Bennett Jones, confirmed the progression in targets of cybercriminals from individuals to multi-million dollar healthcare companies, legal services companies and governmental organizations.[3] Attacks on businesses within these industries are reported to lead to compromised information within minutes.[4] As for small and medium sized businesses, 3.5 new threats targeting them are released every second.[5] If these threats are successful, it can lead to theft of business information, loss of clients or data centre delay, and normally, a data breach signifies only the first step in a chain of criminal acts causing long-term legal issues for a business. The Ponemon Institute, a prominent privacy, data protection and information security policy research centre located in Michigan, estimated that the average cost to manage and mitigate a data breach at $3.62 million (USD) in 2017.[6] The staggering number of attacks and the expense associated with recovering from breaches points to the importance that cyber liability insurance is guaranteed to have in the years to come.

Generally, individual computer users are aware of the risks associated with using a computer and surfing the World Wide Web, taking the time to install virus protection and delete "phishy" emails with questionable website links attached. For businesses, there are risks far beyond the generally known variety in cyberspace, and the first

1 CED 2016 (online), *Science & Medicine*, "Computers and Society".
2 Internet Live Stats, "Internet Users", online <www.internetlivestats.com/internet-users/>.
3 Bennett Jones, "Cybersecurity: 2017 Report & 2016 Reflections" (2017), online <www.bennettjones.com> at 1 [*Cybersecurity 2017 Report*].
4 Lisa R. Lifshitz, "Is cyber-liability insurance the answer to data breaches?", *Canadian Lawyer* (April 27, 2015), online: <www.canadianlawyermag.com> [Lifshitz].
5 *Ibid*.
6 Ponemon Institute, "2017 Cost of Data Breach Study" (2017).

step in protecting a business' information assets is gaining knowledge of the risks that are present. Certain cyber-attacks which target businesses may have ever-lasting implications that are sometimes completely destructive. Understanding what is out there is crucial in order to properly secure a computer network, and in the event that security fails, to have a security policy in place that covers as many of the possible cyber contingencies associated with a particular business as possible.

At its core, a cyber-attack targeted at a company is defined as, "*an attempt to gain unauthorized access to compromise the confidentiality, integrity or availability of the company's information, communication systems, or networks*".[7] Attacks can occur outside of the company headed by hackers and cyber-spies, or they may come from inside a business at the hands of a "rogue" employee. The risk of human error is also very real within a business and must be accounted for in the context of cyberspace and cyber-liability. It is possible that an honest mistake, or negligence on the part of someone within a company, may have the same outcome as a cyber-attack although unintended.

With respect to intentional cyber-attacks, methods are vast and constantly evolving. An attack may involve hacking, the installation of a virus, phishing, or the use of malware, crimeware or ransomware.[8] Hacking occurs as a result of an individual breaching the security levels of a company's computer network. The action may be as simple as figuring out someone's password or as intricate as writing a custom program to break a different computer security software.[9] The installation of a virus, a small program or script, in a computer's software works in the same way as a biological virus that causes deterioration to the human body. A computer virus may lead to the creation, removal or misplacement of files, which affects a computer's memory and ability to function correctly, and overall negatively effecting the "health" of a computer.[10] Viruses can enter a computer's system by the simple click of a website link included in spam email. Phishing also involves spam email where fraudulent attempts are made to obtain personal information.[11] For example, sending emails out in the names of businesses or banks requesting payment information or a social insurance number is phishing. These emails appear highly sophisticated, and it was estimated that 23% of recipients of phishing emails open the messages with a further 11% going on to open the links and attached files.[12] Malware is short for "malicious software", and encompasses any and all software programs that are intended to damage a computer system, such as viruses, worms, trojan horses and spyware.[13] Crimeware and ransomware are sub-types of malicious software. Crimeware is designed to further enable illegal online activity,[14] while ransomware infiltrates a computer system and works to hold it or whatever information it possesses hostage until the ransom is paid.[15]

Gaining wrongful access by utilizing any of the aforementioned methods of a cyber-attack can lead to various results depending on the goal of the attack. The potential repercussions that a business may face in the midst or aftermath of a cyber-attack include: exploitation, cyber-espionage, web defacement, extortion, point-of-sale intrusions, insider misuse, local denial of services, loss of data integrity, privacy breaches, or theft of trade secrets, intellectual property or insider information.[16] Any one of these occurrences may result in the complete loss of or damage to electronic data, which will require extra time, resources and expense to recover or recreate the files. Generally, extra expenditures will be necessary to cover rental computers during the time needed to fix

7 *Cybersecurity 2017 Report*, *supra* note 5.
8 Marianne Bonner, "Dangers of Cyber Attacks", *The Balance* (July 20, 2016), online: <www.thebalance.com> [*Dangers of Cyber Attacks*].
9 Sharpened Productions, "Hacking", *Tech Terms Computer Dictionary* (2017), online: <https://techterms.com> [*Sharpened Productions*].
10 *Ibid* at "Virus".
11 *2015 Data Breach Report*, *supra* note 3 at 12.
12 *Ibid*.
13 *Sharpened Productions, supra* note 11 at "Malware".
14 *2015 Data Breach Report*, *supra* note 3 at 39 and 40.
15 *Cybersecurity 2017 Report, supra* note 5 at 13.
16 See generally: *Cybersecurity 2017 Report, supra* note 5; *2015 Data Breach Report, supra* note 3; *Dangers of Cyber Attacks, supra* note 10.

those affected, and to pay professionals to remedy the situation. A company may also be obligated to pay costs related to extortion and ransom demands. In turn, income will be lost as resources are switched from operating the business to repairing it. There are also costs associated with notifying those who have been affected, or are at the risk of being affected by a cyber-attack. Those affected may then commence actions under privacy laws against a company for not securing their networks properly which could lead to related legal costs and more time and energy spent cleaning up the aftermath of a cyber-attack.

The effects of a cyber-attack are generally devastating for a business with respect to its operations, liability and reputation.[17] Therefore, it becomes necessary for a business to not only become adequately prepared in terms of security, but also to become adequately prepared in the event that security fails, and a breach does occur.

The Growing Relevance of Cyber Liability Insurance

Cyber liability insurance is a company's protection in the event that its security measures fail with respect to their computer network. Cyber-liability policies are specifically intended to cover claims that may not be covered by commercial general liability (CGL) policies,[18] particularly actions that arise from the exposure of protected electronic information as well as technological losses. The gap in CGL policies in relation to electronic data stems from the fact that electronic data may not be considered tangible property, and therefore, does not fall within the definition of "property damage".[19] Further, CGL policies typically include a specific electronic data exclusion clause.[20]

As it stands, the cyber liability insurance market is relatively new so there is no standard form of cyber-liability coverage.[21] This means that policies will vary in coverage, limits, and exclusions. Moreover, coverage that may be available at one point in time may not be available later, as the market evolves in an attempt to find the perfect balance in a cyber liability insurance policy. In this regard, cyber liability insurance policies are normally on a claims-made basis.[22] As for coverage, cyber-liability policies will generally cover third-party liability, including invasion of privacy claims, breach of fiduciary duty claims where there is a failure to protect a client's personal information, libel or slander, or the infringement of intellectual property rights.[23]

There are more than 30 pending privacy class actions triggered by data breaches in Canada.[24] The Superior Court of Quebec recently approved a class action on behalf of all Canadians that were affected when hackers breached the computer network of the U.S. based retail company, Target, in *Zuckerman v. Target Corporation*.[25] The breach affected 40 million credit and debit card holders, as well as 70 million people who had provided personal information to the company during the course of the breach, which occurred in late 2013. The Plaintiff's claimed damages for inconvenience, losses because of firewall or identity theft, loss and publication of personal information, as well as punitive damages. Having a policy in place that covers claims that may arise is important in light of the potential exposure to mass liability and pay-outs, and the heavy legal costs that will undoubtedly be incurred in order to settle an action such as the one arising in *Zuckerman*.

---

17 *Cybersecurity 2017 Report, supra* note 5 at 3.

18 Gregory Boop, "Cyber Liability Insurance – Coverage for Data Breaches", *The Balance* (April 24, 2017), online: <www.thebalance.com> [*Cyber Liability Insurance*].

19 *Ibid*.

20 *Ibid*.

21 Lifshitz, *supra* note 6.

22 *Cyber Liability Insurance, supra* note 20.

23 See: Lifshitz, *supra* note 6; *Cyber Liability Insurance, supra* note 20.
Also see a sample cyber liability insurance policy: Hiscox, "Cyber and data – Policy wording", online: <www.hiscox.co.uk/sites/uk/files/documents/2017-03/13388-cyber-and-data-policy-wording.pdf> [*Policy wording*].

24 Éloïse Gratton, "Superior Court of Quebec Authorizes Privacy Class Action in Zuckerman v. Target Corporation" February 3, 2017 online: www.eloisegratton.com/blog/2017/02/03.

25 2017 QCCS 110 [*Zuckerman*].

Cyber liability policies may include various first party coverages such as information asset loss and the associated costs of restoring data and the company's network.[26] Cybercrime costs which include extortion expenses or ransom costs may also be covered, and some policies even extend coverage to e-vandalism and the onward transmission of computer viruses. The loss of income a business experiences when dealing with a cyber event may be covered, along with third party losses of income due to a business' partial or complete shutdown during a cyber-attack.[27] Third party loss of income covered by a cyber liability insurance policy is specifically not included under business income or extra expense insurance in a CGL policy. Finally, these policies may be able to cover the costs of investigations following a breach of security, as well as assessment and notification costs for those people who have been affected by a breach. In some instances, a policy may even go so far as to cover the cost of a "crisis management" team consisting of public relations, legal and computer forensics consultants who help to minimize the damage of a cyber-attack.[28] The variety of coverage options available in a cyber-liability policy demonstrates that the policies in this area are not "one size fits all". Different businesses face different risks in the event of a cybersecurity breach, all dependent on the content of their information assets. The different options for coverage ensure that a business can obtain a policy that is particularly suited to them and their cybersecurity needs.

With coverage comes specific exclusions that businesses seeking to obtain a cyber-liability policy will need to be weary of. In some instances, the very events that were noted earlier as being covered will be excluded. Generally, coverage is barred in relation to a claim involving a dishonest or criminal act by anyone insured under the policy or a cyber-attack that was performed by a director or partner of the business. Any claims involving reckless conduct, credit monitoring costs, non-specific investigations, or claims brought by a related party are often barred from coverage.[29] In some instances, cyber insurance policies impose strict and substantial obligations on businesses requesting coverage with the underlying goal that cybersecurity risks be well-protected against when the policy is engaged. This is the insurer's way of spreading the responsibility between itself and the insured and mitigating risk before it becomes required to cover any loss. For instance, to be eligible for a cyber liability insurance policy in most cases, security technology and other security mechanisms and responses must already be in place.[30] Security technology may include the presence of a firewall, the presence of virus scans, assignment of a responsible person in the event of a cyber-attack, a data back-up and storage mechanism, and the adoption of a security policy. Failure to keep security technology, mechanisms and responses up-to-date after a cyber-liability policy is obtained could result in a bar to recovery.[31] A policy may require the training of staff members with respect to safe ways to use the company's network or that risk-reporting regimes be in place in order to be eligible for continued coverage under the policy.[32] Ultimately, the insurer does not want cyber-liability coverage to be the only fallback plan for a business in relation to its information assets.

As this section highlights, a business using any sort of electronic storage for its information assets will want to be prepared two-fold: by having proper security technology in place to help minimize the risk of a successful cyber-attack, and by having a cyber liability insurance policy in place to rely on in the event that the security technology fails. It becomes clear that having only one of the two elements in the realm of cyberspace and cyber-liability leaves a company vulnerable and exposed in one way or another with mass payouts and loss should the vulnerability be exposed. Together, cybersecurity and cyber liability insurance provides the best chance for a business to survive a cyber-attack and its consequences. Overall, the insurance industry in general is always changing and adjusting to the needs of particular times and circumstances. With respect to cyber-liability and cyber liability insurance in particular, the industry is set for an increase in the need and demand for coverage in order to respond to the ever-growing amount of sensitive information stored on computer networks,

26 Lifshitz, *supra* note 6; *Cyber Liability Insurance, supra* note 20.
27 *Ibid*.
28 *Ibid*.
29 *Policy wording, supra* note 26.
30 Lifshitz, *supra* note 6.
31 *Ibid*.
32 *Ibid*.

and corresponding risk with such storage. Although cyber liability insurance is novel with no standard form of coverage, the argument is strong that development in this area is imminent as the impact that cyberspace and cyber-liability has on businesses becomes clearer.

Regulation of The Cyber World

It is worthy to note the legislative movement towards mandatory data breach reporting as evidenced by the *Digital Privacy Act, supra*, which was assented to on June 18, 2015. Mandatory data breach reporting will serve as a means of mitigating cybersecurity risks. Section 10, in particular, will drastically change data breach reporting obligations once in force, because it requires all organizations dealing with personal information to report to the Privacy Commissioner any security breaches that create a "*real risk of significant harm*"[33], as well as to the individual whose information has been compromised.[34] Pending government crafted regulations, section 10 will become effective and provide clarity for businesses regarding the legal requirements placed upon them during a data breach. Until then, businesses faced with data breaches which exposed the personal information of individuals have no guidance in terms of the responsibilities and obligations owed to those affected. These requirements will give rise to legal obligations that a business will face in the midst of a data breach increasing exposure to liability if the requirements are not met. Mandatory reporting will also lead to an increase in the public's knowledge of businesses dealing with a security breach as well as an increase in the public's awareness of the implications a data breach may have. Cyber liability insurance will serve as a means of protection when requirements are not met and when people affected by a breach become aware of its implications to their personal privacy.

Businesses should become familiar with the requirements noted in section 10 of the *Digital Privacy Act, supra* respecting 'Breaches of Security Safeguards' in order to get ahead of these regulatory changes. The class action certified in *Zuckerman, supra* included authorization of a common question regarding the alleged failure of Target to notify class members of the breach, even though the petitioner had not included this allegation within his claim for damages. Although not yet mandatory, it is clear that the need to report a security breach is of the utmost importance, and section 10 is instructive. The necessity of reporting a breach to the Privacy Commissioner and individuals who have been affected by the breach, as mentioned earlier, occurs when there is a "real risk of significant harm". Section 10 defines "significant harm" as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.[35] The sensitivity of the personal information exposed in the breach and the probability that the information has been or will be misused are factors that influence the "real risk" of significant harm.[36] Companies will likely want to err on the side of caution when reporting data breaches and are required to report a breach as soon as possible. This is an effort to limit the damage to the individuals affected, and is also serves to protect a company and lessen the exposure to damages for a data breach as covered earlier. Following this reasoning, the notification given to the Privacy Commissioner and individuals must contain enough information to allow the reader to understand the implications of the data breach and to take steps to reduce the risk of harm resulting from the breach.[37]

As of now, legislation in New Brunswick only mandates notification of data breaches in the private sector, specifically in relation to health-related data, under the *Personal Health Information Privacy and Access Act*.[38] Alberta is the only Canadian province where data breach notifications are required beyond breaches of health-related data given that Alberta's *Personal Information Protection Act*[39] applies to all personal information held by private organizations.

33 *Digital Privacy Act, supra* note 18 at s 10.1(1).
34 *Ibid* at s 10.1(3).
35 *Ibid* at s 10.1(7).
36 *Ibid* at s 10.1(8).
37 *Ibid* at s 10.1(4).
38 SNB 2009, c P-7.05 at ss 2, 3, 49 [*PHIPAA*].
39 SA 2003, c P-6.5 at ss 3 and 4.

The notification requirements under the *Personal Health Information Privacy and Access Act, supra* are similar to those that will soon become effective under the *Digital Privacy Act, supra*, in that, at the first reasonable opportunity following the exposure of personal health information, the individual affected and the Privacy Commissioner must be notified.[40] If there is a reasonable belief that the exposed personal health information will not have an adverse impact on the provision of health care or other benefits to the individual to whom the information relates; have an adverse impact on the mental, physical, economic or social well-being of the individual to whom the information relates; or, lead to the identification of the individual to whom the information relates, there is no need to report under the *Personal Health Information Privacy and Access Act*.[41] Unique to the *Personal Health Information Privacy and Access Act* is the ability of the custodian of an individual's personal health information to disclose this information without consent in particular instances, such as furthering the individual's healthcare, informing family members as to the status of the individual, and for furthering the education of those in the healthcare industry.[42] In this respect, the ability to justify disclosure without the individual's consent is different than under the *Digital Privacy Act, supra*. Despite this, the Government of New Brunswick recently announced proposed amendments to the *Personal Health Information Privacy and Access Act* that will clarify accountability for safeguarding personal health information and strengthen the safeguards relating to the release of personal health information.[43] From this, it is easy to see how keeping an up-to-date regulatory scheme goes hand-in-hand with a custodian's ability to best deal with safeguarding information and reacting to any data breaches. Just as the health industry has a scheme in place for healthcare custodians to safeguard personal health information, the *Digital Privacy Act, supra*, has been long-needed to help with other industries that regularly deal with personal information.

Cyber-Liability in the Courtroom

Although cyber-liability is a new concept with a limited history in Canadian court rooms, developments in the common law in relation to privacy laws illustrate a trend towards finding civil liability for privacy breaches. For example, *Jones v. Tsige*[44] a decision in Ontario, recognized the tort of "intrusion upon seclusion". In this case a man's girlfriend used her position as a bank employee to access the man's ex-wife's bank account over several years. After becoming aware of the breach the ex-wife sued.

The Court recognized four scenarios which could result in an invasion of privacy: intrusion upon the plaintiff's seclusion or solitude or into his or her private affairs; public disclosure of embarrassing private facts about the plaintiff; publicity which places the plaintiff in a false light in the public eye; and appropriation for the defendant's advantage of the plaintiff's name or likeness.[45] In its aftermath, when a person found liable to another under the tort of invasion of privacy is a custodian's employee, the company by extension could face liability for the security breach, or for failure to adequately protect the personal information of its clients and customers.

The Ontario Supreme Court expanded the scope of claims under the intrusion upon seclusion tort in *Jane Doe 464533 v. ND,*[46] recognizing that public disclosure of embarrassing facts gives rise to a valid claim under the tort. The Plaintiff and Defendant were young adults that had been in a romantic relationship. The Defendant convinced the Plaintiff to send him a sexually explicit video of herself after assuring her that he would not show the video. The Defendant then posted the video on an internet pornography website and shared it with

40 *PHIPAA, supra* note 42 at s 49(1)(c).
41 *Ibid* at s 49(2).
42 See generally: *PHIPAA, supra* note 41 at ss 27, 37-45.
43 New Brunswick, Department of Health, *Amendments introduced to the Personal Health Information Privacy and Access Act*, (Fredericton) 28 March 2017.
44 2012 ONCA 32.
45 William Prosser, Law of Torts, 4th ed (West Publishing Company, 1971) at 808-12 as cited at para 18 of *Jones v. Tsige*, *supra*.
46 2016 ONSC 54.

several of the Plaintiff's acquaintances. The Defendant did not defend the action and in the default judgment ruling Justice Stinson described the test for unauthorized public disclosure of private facts as:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the of the act publication would (a) be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.

Upon learning of the default judgment, the Defendant brought a motion to set aside the finding of liability and the assessment of damages, which was successful. Until such time as there is a re-trial or another action alleging the tort of unauthorized public disclosure of private facts the precedential value of *Jane Doe 464533 v. ND* remains uncertain. However, it does show a willingness in Canadian courts to find liability for privacy breaches. It is worth noting that British Columbia[47], Manitoba[48], Newfoundland[49] and Saskatchewan[50] have passed legislation recognizing the tort of invasion of privacy.

In *Michael Evans and Crystal Evans v. The Bank of Nova Scotia and Richard Wilson*,[51] the possibility of a company being held vicariously liable became a reality when a class action was allowed to proceed against The Bank of Nova Scotia as a result of the actions of the bank's employee. Currently, the class action is still making its way through the court system.

The first Canadian decision relating to cyber insurance coverage occurred recently in *The Brick Warehouse LP v. Chubb Insurance Company of Canada*,[52] where the Alberta Court of Queen's Bench held that a commercial crime policy did not cover the loss which resulted from social engineering fraud. Commercial crime policies cover losses that are not covered under CGL policies and that result from crime, generally providing coverage for employee theft, robbery, extortion and computer fraud. In this particular case, the commercial crime policy covered "Funds Transfer Fraud", which covers loss where a third-party performs a fraudulent bank transfer. In August 2010, a fraudster acting like a new employee at Toshiba called The Brick's accounts payable department to obtain payment information, while another impersonator emailed a Brick employee to update Toshiba's banking information, requesting that future payments be made to the new bank account. The phishing attempt was successful because both employees complied with the requests and provided the necessary information and made the requested changes. The Brick ultimately suffered a net loss of over $200,000 after making payments to what they thought was a Toshiba account. The company submitted a claim to Chubb Insurance for "Funds Transfer Fraud" coverage. The clause was worded as follows:

> *Funds transfer fraud means the fraudulent written, electronic, telegraphic, cable, teletype, or telephone instructions issued to a financial institution directing such institution to transfer, pay or deliver money or securities from any account maintained by an insured at such institution without an insured's knowledge or consent.*

The terms 'knowledge' and 'consent' were not defined in the policy, and so, the Court applied their "plain, ordinary and popular"[53] meaning. In so doing, the Court found that The Brick failed to demonstrate that the transfer instructions were given to its bank without its knowledge or consent in light of the fact that the instructions were given directly by an employee of The Brick, not a third-party fraudster. For this reason, the clause was inapplicable in the circumstances and Chubb Insurance was not required to provide coverage to The Brick for its loss.

---

47 *Privacy Act*, RSBC 1996, c 373.
48 *The Privacy Act*, CCSM c P125.
49 *Privacy Act*, RSNL 1990, c P-22.
50 *The Privacy Act*, RSS 1978, c P-24.
51 2014 ONSC 7249.
52 2017 ABQB 413.
53 *Ibid* at para 23.

The Court referred to a decision by the U.S. District Court for the Central District of California, *Taylor and Lieberman v. Federal Insurance Company*,[54] where a similar fact situation had played out. The U.S. District Court had also found that a similarly worded clause was inapplicable since the insured's employee knew of the transfers, even if he did not know they were fraudulent. This decision makes it clear that coverage under a crime policy for "Funds Transfer Fraud" will only apply where the third party implements the fraudulent transfer without the knowledge or authorization of the insured company's employees. It will not be enough to trigger coverage where an insured's employee has been deceived, and used as an in-between, for a fraudster's illegal activity. The lesson to be learned from this case is to be aware of the discrete wording of clauses, otherwise a company may be exposed to a loss that it believed it had protection against.

Choosing Appropriate Cyber Liability Insurance Policies

Given that cyber liability insurance policies are just taking off in the Canadian insurance market, there is uncertainty in the terms and depth of coverage contained in them. As such, it is extremely important to ensure that a policy being purchased is thoroughly reviewed and covers all possible cyberattack contingencies that a particular business or company may face. Two recent cases out of the U.S. serve as cautionary tales that cyber liability insurance policy purchases require a great deal of expertise and care. Legal counsel or a broker qualified and familiar with data loss and cyber-liability should be retained to help identify the exact scope of coverage a policy provides, and in turn, should provide assistance to ensure the policy is tailored to cover everything as per the needs of the company, client, customer, etc.

P.F. Chang's China Bistro, Inc. v. Federal Insurance Company[55] dealt with the scope of coverage offered to P.F. Chang's China Bistro under a cyber risk and commercial insurance policy that had been purchased from Federal Insurance Company. The policy covered, "direct liability, and consequential loss resulting from cybersecurity breaches" and had been advertised as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology dependent world." With the need to perform a mass amount of credit card transactions each day, P.F. Chang's China Bistro contracted with Bank of America Merchant Services to process the transactions. Bank of America Merchant Services in turn contracted with MasterCard to process the same transactions. In their agreement, MasterCard required Bank of America Merchant Services to pay certain fees in the event of a data breach. In the event the fees arose, Bank of America Merchant Services required payment of them from P.F. Chang's China Bistro.

A breach occurred in June, 2014, when hackers exposed the credit card information of over 60,000 P.F. Chang's China Bistro customers. Federal Insurance Company reimbursed P.F. Chang's China Bistro for more than $1.7 million; however, it refused to cover $2 million in fees that MasterCard was seeking from P.F. Chang's China Bistro through Bank of America Merchant Services. The Court looked to the approach taken when interpreting CGL policies since, "*cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same.*"[56]

The policy excluded coverage for "any liability assumed by any insured under a contract or agreement". As P.F. Chang's China Bistro had contracted to indemnify American Merchant Services against MasterCard there was no coverage under the policy. In so holding, the Court also rejected P.F. Chang's China Bistro's argument that they had an objectively reasonable expectation that Federal Insurance Company would cover any potential fees incurred by a third party. Moreover, the Court stressed that the parties were sophisticated and that the policy and its provisions had been subject to a bargaining period where coverage of all extra fees or third party fees could have been obtained by P.F. Chang's China Bistro.

54 2:14-cv-03608, unreported, 2017.
55 No 15-cv-1322 (SMM), 2016 WL 3055111 (D. Ariz. May 31, 2016).
56 *Ibid* at para 8.

Columbia Casualty Company v. Cottage Health Systems[57] arises out of a data breach which resulted in the release of healthcare information of approximately 32,500 patients. Following the breach, Cottage Health Systems faced a class action lawsuit on behalf of the patients impacted. The class action settled for $4.1 million. At the time of the data breach, Cottage Health Systems held a cyber insurance policy against data breach claims with Columbia Casualty Company. Columbia Casualty Company funded the settlement pursuant to a reservation of rights and commenced its own action to recover the settlement funds from Cottage Health Systems.

Columbia Casualty Company relied on an exclusion which barred coverage for any data breach claims that occurred due to *"failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance and all related information submitted to the Insurer in conjunction with such application."*[58] The circumstances of the data breach involved a mistake, an innocent one, at the hands of a third-party vendor who was hired by Cottage Health Systems to store all of the company's electronic records. Instead of setting the online files with private-only access, they were left on a public setting allowing anyone access to them for approximately two months. Columbia Casualty Company alleged that this type of breach was not covered under the policy since Cottage Health Systems failed to continuously maintain and follow minimum required practices of cybersecurity.

The Court ultimately dismissed the complaint and ordered the parties to adhere to the alternative dispute resolution terms in the policy to settle the matter; however, the case is an example of the need to follow the security systems required by an insurance policy. In this respect a business wishing to purchase a cyber-liability policy must be clear on the obligations imposed on them by the policy, and the specific exclusions and condition precedents to coverage. Meanwhile, *P.F. Chang's China Bistro, Inc., supra* demonstrates that the approach to cyber-liability policies will be similar to that of the approach to CGL policies. More importantly, commercially sophisticated companies will be held to a high degree of competence when negotiating coverage and will not be able to rely on different expectations simply because cyber-liability policies are new. It remains the responsibility of a company obtaining cyber liability coverage to be informed and aware of exactly what the policy it is purchasing covers, eliminating the possibility for ignorance or error to circumvent situations where the policy fails them.

Conclusion

The use of computers and their networks to store data is essential to many companies in this modern age, and their use is only going to increase as innovators work to maximize network capacity. As the amount of information stored on computer networks continues to increase so will cybercrime. As noted, cybercrime is already on the rise and its constant evolution makes data loss and exposure a very real problem for businesses. Even outside the context of cybercrime, there is the possibility of human error that may lead to a data breach. All in all, data breaches will become more regular, and soon, privacy claims will be more prevalent in Canadian courts as people begin to understand their reach and implications.

The purpose of the preceding information works to highlight the importance of not only implementing proper security mechanisms to protect a company's information assets, but also preparing for the possibility that security mechanisms will fail. A company will want to protect itself appropriately before a data breach, and cyber liability insurance is the most appropriate way to do so. Cyber liability insurance will cover costs that arise in the midst of, and following, a data breach, and allow a company to continue on successfully following the

57 No 2:15-cv-03432 (C.D. Cal.) (2015).
58 *Ibid* at para 40.

breach. In the same way that an automobile is equipped with countless safety features, but is not driven without automobile insurance, or a home is equipped with fire detectors, but fire coverage is included in a homeowner's policy regardless, there is no logical reason why a company dealing with information assets would protect those assets from a potential breach, but would not be prepared in the event that protections fail. In this regard, the issue of cyber liability is set to take off – it is only a matter of being adequately prepared with a cyber liability insurance policy when it does.

COX & PALMER

The difference is a great relationship

coxandpalmerlaw.com | @coxandpalmer