THE QUEBEC PERSPECTIVE IN CYBER RISKS

J.F Bilodeau, Partner, Robinson Sheppard Shapiro

I. INTRODUCTION

The Internet today is a worldwide web of connections allowing people to send and receive information. However, the idea was born in August 1969 when an experimental net (ARPAnet[121]) was created by DARPA[122] (Defense Advanced Research Projects Agency. The goal was to link four universities to exchange data. The founders would never have envisioned the incredible developments that would arise from their simple venture forty years later!

Today, millions if not billions of users, private citizens, public and private bodies are using the net on a daily basis to exchange massive amount of data. E-commerce entails the sale of goods and electronic payment by credit cards. Governments store huge amount of data on their citizens. The safety of the information stored is paramount and theft of such data can and did happen.

Are insurers aware of the risks related to the storage of information by their insured and the exposure to thefts or unauthorised disclosure of such information? Can insurers property make estimates of the risks and manage such coverage?

In the present paper, we will attempt to review the risk, the exposure and tools available to insureds and insurers against cyber risks.

II. WHAT ARE THE RISKS RELATED TO THE INTERNET USAGE?

The risks related to the safety of information on the internet may be categorized as theft of personal information and as exposure to viruses.

1) Theft of personal or confidential information

Personal, financial, health or government information is now widely available and this data is exposed to theft and unauthorised disclosure to third parties. Very often, the dissemination of information will give rise the identity theft.

[121] http :fr.wikipedia.org/wiki/arpanet
[122] http :fr.wikipedia.org/wiki/Defense_Advance_Reesearch_Agency

a) Financial information and identity theft

The theft of financial information is clearly foremost as it allows access to credit cards, debit cards, account numbers or investment folios. Once this basic information is obtained, further activities such as the creation of fictitious identities and more complex frauds can be initiated.

In order to protect the private information of the public, states have enacted laws to protect and restrict the disclosure of personal data. For example, California adopted in 2003 the *California Security Breach Information Act*[123] requiring persons of business doing business in the State and which holds personal data to disclose any breach in information safety to the persons whose data have been exposed.

In 2000, the Federal government sanctioned the *Personal Information Protection and Electronic Documents Act*[124]. The Act has been amended and now compels data holders to inform individuals of any safety breach concerning their information. The regulatory body created under the Act must also be informed of any security breach. This Act only applies to federal bodies or within the federal sphere of jurisdiction. Provinces have adopted their own statutes such as Alberta, British Columbia Quebec and others to regulate the provincial sphere of activities[125].

In Quebec, the *Act to Establish a Legal Framework for Information Technology*[126] was enacted in 2012 and is to the same effect. The Act also indicates how the information is to be protected or disclosed to third parties.

The Act also renders responsible, amongst other parties the data holder who fails to abide by the regulations or failed to prevent the unauthorized information disclosure.

B) Medical and Health Information

The patient information is undergoing computerization to allow access to authorities, medical personnel or various players. The data is also exposed to theft or disclosure. The protection of this private information is necessary and recognized by governments.[127]

In 1996, the United States adopted the *Health Insurance Portability and Accountability Act*[128] ("HIPAA"). HIPAA required health facilities to protect, control and prevent the unauthorised disclosure of confidential medical information[129]. Canada adopted in 2000, as indicated above

---

123 Bill 13861 (CA1386)

124 S.C. 2000, c. 5, and various bills amending the Act in the following years.

125 MEYRICK, M., ASHALL, J. and F. VARTANINAN, « Cyber Risks & Privacy Liability- Are you covered? », Sept. 2007, 8 Lexpert no. 10, 134-135

126 Q.S. c. C-1.1

127 HIMSS Privacy & Security Task Force, « Creating a Trusted Environment : Reducing the Threat of Medical Identity Theft", June 2012, aux pages 3 et suivantes; http://himss.files.cms-plus.com/HIMSSorg/content/files/CreatingaTrustedEnvironment_Reducing_the_Threat_of_Medical_Identity_TheftFINAL.pdf.

128 Pub. L. No. 104-191, 110 Stat. 1936 (1996)

129 HIMSS Privacy & Security Task Force, « Creating a Trusted Environment : Reducing the Threat of Medical Identity Theft", June 2012, à la page 6; http://himss.files.cms-

the *Personal Information and Electronic Documents Act* and most provinces adopted similar acts to also protect medical information.

According to a recent American study, the theft of medical identity allowed persons not otherwise covered to obtain medical care amounting to 30 billion dollars per year[130].

2) VIRUSES

Viruses affect and compromise electronic data without the knowledge of its owner. The term is used commonly and refers to programs such as

« malware », « adware » and « spyware» which do not have any reproduction capacity. Others such as « Trojan Horse » may execute functions within the computer.

What are the losses attributable to viruses affect software, hardware, programs, data, etc?

a) Loss of data and risk of property damage

Corporations and businesses communicate with other companies and clients via internat. The exchange of contaminated information may compromise data and result in damage. Viruses could be propagated via e-mails, web sited or even through the malicious act and of employee.

Other damage may be caused by a technician while repairing hardware such as computers or software. Ask your IT employees about their worst nightmares…

Another risk relates to work performed by employees, programmers at customers.

b) Business Interruption

Most of not all businesses or organizations rely on computerization of systems to handle all aspect of their activities: design, finance, human resources, sale and purchase and payables/receivable to only name a few. The contamination or destruction of data will result in business interruption for hours, days or weeks. You all know the scope and losses attributed to business interruption.

For instance the "Poison Ivy" virus would allow operators to control the infected computer. Companies victim of such viruses may not know the extent of their loss if unaware of the scope and breathe of the accessed data.[131]

---

plus.com/HIMSSorg/content/files/CreatingaTrustedEnvironment_Reducing_the_Threat_of_Medical_Identity_TheftFINAL.pdf.

130 Ponemon Institute Second Annual Survey on Medical Identity Theft, March 2011

131 Microsoft, Threat Report: Poison Ivy, October 2011, http://download.microsoft.com/ download/E/1/5/E1552019-2022-4D7D-A001-044D5AE9251D/MMPC%20Threat%20Report%20-%20Poison%20Ivy.pdf

In 2003, public services were affected by the « Slammer» worm. This virus released huge amount of data to paralyse systems. It would appear that the Washington State 911 emergency service was paralysed by such virus as well as nuclear power plants in Ohio[132].

c) Liability Issues

The cyber liability arising from human error or breach of system security increased exponentially with the use of internet.

In Quebec, the civil responsibility is governed by the following principle which is to the following effect: « Every person has a duty to abide by the rules of conduct which lie upon him, according to the circumstances, usage or law, so as not to cause injury to another. »[133]

In order to prove liability, a claimant must establish fault or negligence, the damage and a causal link between fault and damage.

Fault or negligence may be established in various ways: failure to abide by existing statutes or regulations such as the various private information protection acts[134]. Liability may also be found in contract and finally, it can be found as a result in the failure to act as a reasonable person under article 1457 Q.C.C. cited above.

In fact, the liability principles are not affected because the vehicle of damage is a computer. Individuals using computers must act and in accordance with good practices. Fault or negligence may be found in:

- The failure to recognize faults or systems defects or to correct such defects;
- The failure to instruct or supervise employees;
- The failure to use reasonable means to secure safeguard the electronic systems against intrusion;
- The failure of manufacturers to install or test systems against defects.[135]

In fact, the electronic systems should benefit from all the protection that a prudent IT manager can make available and install on the equipment in use[136].

The damage caused to electronic systems may result in claims such as:

- The costs related to repairs the systems;
- The business interruption;

---

132 NILOSEVIC, Nikola, "History of Malware", Computer Security, http://cryptome.org/2013/02/malware-history.pdf

133 Art. 1457 Q.C.C.. – The equivalent rule in contractual matter is found at article 1458 Q.C.C..

134 *Loi sur la protection des renseignements personnels dans le secteur privé*, chapitre P-39.1

135 VERMEYS, Nicolas, "Computer "Insecurity" and Viral Attacks: Liability Issues Regarding Unsafe Computer Systems Under Quebec Law", Lex Electronica, vol 9, no. 1, Hiver 2004; http://www.lex-electronica.org/articles/v9-1/vermeys.htm

136 BAWDEN, Brian R., "The Ten Commandments of Computerization ", CA Magazine, August 1993, pp. 32-38

- The loss of data.

In many instances, the difficulty to advance claims will relate to the establishment of the causal link between the negligence and the damage. For instance, can a weak anti-virus system be causal to damage from a virus that would have penetrated a standard system? In the case of a vulnerable system attacked by two viruses originating from different sources, who would be held liable? Article 1480 Q.C.C. may be of help in the latter situation:

1480 Q.C.C. Where several persons have jointly taken part in a wrongful act which has resulted in injury or have committed separate faults each of which may have caused the injury, and where it is impossible to determine, in either case, which of them actually caused it, they are solitarily liable for reparation thereof.

This provision is important in IT security because often, the persons transmitting viruses or infecting systems are doing so without knowledge and after having been infected themselves.

Finally, it would be appropriate for companies involved in the IT field to include in their contracts limitation/exclusion of liability clauses relating to electronic security and safety. Such exclusion of liability clause could also be found on web sites.[137]

III. INSURANCE COVERAGE

The insurance forms made available by insurers did not, for the longest time, include clauses on cyber-risk. The new attached CGI form issued by the Insurance Bureau of Canada (IBC) provides insureds are not covered for damages resulting arising from data losses. Other provisions have also been introduced by the IBC.

1) The property damage coverage

The notion of property damage needs to be reviewed before studying the cyber exclusion clauses. The insuring agreement in a CGI policy typically refers to « Property Damage » in the following fashion:

We will pay sums that the insured becomes legally obligated to pay as "compensatory damages" because of « bodily injury » or « property damage » to which this insurance applies. […]

[137] VERMEYS, Nicolas, "Computer "Insecurity" and Viral Attacks: Liability Issues Regarding Unsafe Computer Systems Under Quebec Law", Lex Electronica, vol 9, no. 1, Hiver 2004; http://www.lex-electronica.org/articles/v9-1/vermeys.htm

The notion of « property damage » is defined in the policy as:

25. « Property Damage » means :

a. Physical injury to tangible property, including all resulting loss of use or that property. All such loss of use shall be deemed to occur at the time of the physical injury that caused it; or

b. loss of use of tangible property that is not physically injured. All such use shall be deemed to occur at the time of the "occurrence" that caused it.

For the purpose of this insurance, electronic data is not tangible property.

As used in this definition, electronic data means information, facts or programs stored as or on , created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells date processing devices or any other media which are used with electronically controlled equipment.

This definition in the IBC form 2100 would clearly indicate that electronic data is not included in the definition of property damage and is not covered under the policy.

However, for prior policies that do not includ such a definition, courts had to determine if electronic data did constitute tangible property.

2) the electronic data exclusion

The electronic data exclusion found in the IBC form 2100 reads as follows:

2. Exclusions

This insurance does not apply to :

I. Electronic Data

« Compensatory damages » arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

The exclusion reveals that under the form, the insurer will not cover damages arising from loss of electronic data. There is no requirement to establish the cause of loss on the part of the insurer but only that the loss results from the loss of data.

Several judgments from British Columbia have examined the effect of the wording «arising out of»[138] and have found in favour of the insurer. The cases dealed with the « cause-related » issue

[138] ***Jordon v. CGU Insurance Co. of Canada,*** 2004 BCSC 402; ***Leahy v. Canadian Northern Shield Insurance Co,*** 2000 BCCA 408

reveal that the prior form was problematic as it required the insurer to prove a link between the loss and the cause. This issue would likely now be resolved with the new form.

However, our courts have not yet rendered any judgements on this issue at the present time.

3) COVERAGE FOR advertising and bodily injury

The CGL form provides coverage for personal and advertising injury liability. This coverage includes advertising injury and consequential bodily injury arising from oral or written publication, in any manner, of material that slanders or libels a person or organization or violate a person's right to privacy.

However, the IBC form contains two exclusions:

j. insures In Media and Internet Type Business

«Personal and advertising injury » committed by an insured whose business is:

(1) Advertising, broadcasting, publishing or telecasting;

(2) Designing or determining content of web-sites for others; or

(3) An internet search, access, content or service provider.

However, this exclusion does not apply to Paragraphs 21, a., b. and c. of « personal and advertising injury » under the Definition Section.

For the purpose of this exclusion, the placing of frames, borders or links, or advertising, for you or others anywhere on the Internet, is not by itself, considered the business of advertising, broadcasting, publishing or telecasting.

K. Electronic Chatrooms or bulletin Boards

« Personal and advertising injury » arising out of an electronic chatroom or bulletin board the insured hosts, owns, or over which the insured exercises control.

The terms « personal and advertising injury » have been defined as follows in the IBC form. We reproduce below the relevant definition sections:

21. « Personal and advertising injury » means injury, including consequential « bodily injury », arising out of one or more the following offenses:

d. Oral or written publication in any manner, or material that slanders or libels a person or organization or disparages a person's or organization's good, products or services;

e. Oral or written publication, in any manner, of material that violates a person's right of privacy;

f. The use of written publications, in any manner, of material that violates a person's right of privacy »

Insureds should be careful in understanding the wording of the standard CGL policy.

IV. CASE LAW

1) QUEBEC ET CANADIAN PROVINCES

There are no reported decisions in Quebec and few from other provinces on the loss of electronic data. However, several decisions have been rendered United States on this topic.

2) UNITED STATES

We do not wish to review the United States case law in the present paper but it suffices to say that Courts in the U.S. have rendered inconsistent and inclusive judgement on the issue whether electronic data constitute « physical injury to tangible property ». However, it would appear that a majority of cases suggest that electronic date is not tangible property and will not offer indemnification to policy holders.

V. OTHER INSURANCE PRODUCTS

We have seen that the new IBC CGL form does not cover the cyber risks. However, the older forms may afford a certain protection but the issue is not clear and litigation may be necessary to solve the dispute.

Insures may have to create new product to answer the needs of customers involved in e-commerce, data handling, software programming, installation and maintenance.

In order to offer relevant protection, insurers may have to revisit four categories of cyber risks:

- Losses resulting from unauthorized access to private information or data (ex. Target breach of security, I-Cloud and stored pictures);
- Damages for the transmission of virus;
- Loss for the web access denial to customers;
- Failure to notify customer of data access violation.

The liabilities for such incidents could be very costly and would require coverage but the challenge would be to assess the exposure and to determine premium.

VI. CONCLUSION

The significant increase of the worldwide web and the daily applications to all human endeavours exposes users to all kinds of liabilities. Presently, the available liability coverage and protection is minimal and would need to be revisited as business opportunities exit for insurers to explore acquire markets.

We believe new products should be developed to respond to the need of the internet users.