ONTARIO BAR ASSOCIATION
A Branch of the Canadian Bar Association

iTECH NEWS

November 2012 Information Technology and Electronic Commerce Section

Information Technology & E-Commerce: Insuring Against Cyberspace and Other Network Risks

Prepared by Matthew Wanford and Al Cheng

The following is a summary of some of the salient points from the Information Technology & E-Commerce: Insuring Against Cyberspace and Other Network Risks program, held at the OBA on November 14, 2012, presented by Michael Petersen, Marsh Inc., and David R. Mackenzie, Blaney McMurtry LLP, chaired by Matthew Wanford, Osler, Hoskin & Harcourt LLP, and Salim Dharssi, Gilberts LLP.

The New Reality of Risk – Cyber Risk

Increasing Cyber Risks:

In his presentation Michael Petersen of Marsh emphasized that in today's interconnected world, data and technology are increasingly becoming sources of operational risk for any company that handles, collects or stores information, or simply uses a computer network. Privacy risks and data breaches are primary concerns, with the reality quickly becoming not whether a company will be hacked, but when. A data breach can be very costly and can happen due to a cyber attack or human error (for example, leaving an unencrypted USB key containing confidential information on a public bus). The key statistic in determining the potential value of a breach is the number of records that will be compromised. Simply put, the greater the number of records at risk, the greater the potential damages and costs of remediating the breach and protecting those at risk, for example, through the provision of initial notification, call centre support and credit record monitoring. It is also important to note that legal and forensic expenses incurred in responding to regulatory action following a breach can be substantial even where there is no actual harm or even the risk of harm (and therefore no civil action afterwards).

The Inadequacy of Traditional Insurance Policies:

Michael also emphasized that traditional insurance policies do not always adequately protect a company against exposures to cyber threats. For instance:

- Property policies are inadequate because they require a direct physical loss, and courts have also consistently held that data is not property;
- Crime insurance policies are intended to cover money, securities and tangible property only – they are not designed to cover theft of data (with the exception of a financial institution bond); However, some carriers will offer coverage for the value of data or stolen computer systems' resources excess/DIC of a crime policy;
- General Liability policies are likewise inadequate because they often do not cover damage to electronic data, criminal or intentional acts of the insured or employees – at the end of the day, there must be some bodily injury or property damage;
- Errors & Omissions policies are tied to "professional services" and often require that there be some act of negligence to trigger coverage;

- Directors and Officers Liability insurance is intended to protect a company's balance sheet in the event a director or officer of the company commits a wrongful act; the policy is not meant to respond to cyber risks;
- Employment practices liability insurance only protects against errors and omissions in the management and administration of human resources – akin to an HR malpractice policy;

Only Kidnap and Ransom policies can provide coverage, but even then only via a separate "cyber-extortion" endorsement.

Network Security / Privacy Insurance:

Compared to the traditional insurance policies listed above, most network security and privacy insurance policies more adequately protect against cyber threats by providing coverage for:

- Privacy liability arising from any harm suffered by others due to the disclosure of confidential information;
- Network security liability arising from any harm suffered by others as a result of the failure of an insured's network security, including any failure of an insured's computer systems' security to prevent or mitigate a computer attack that: destroys, corrupts or deletes data, applications or software; steals resources (e.g. bandwidth); interrupts the operations of the computer system; and/or creates operational expense;
- Costs of investigating a cyber extortion and the amount of the extortion demand itself (ransom and crisis consultant expenses are usually limited);
- Legal expenses to defend against regulatory actions;
- Costs of complying with breach notification laws and regulations;
- Lost revenue and extra expenses incurred during a period of business interruption caused by a cyber attack (usually includes a $100,000 sublimit covering lost business income attacks on a subcontractor or cloud service provider's network security);
- The cost to replace, recreate or restore the lost data, software or applications;
- The cost to determine that such assets cannot be replaced, recreated or restored;
- Forensic costs (sub-limited); and
- The value of the data or stolen computer systems' resources.

Because different insurance carriers offer policies with different coverage endorsements and exclusions, and because the insurance needs (for example, limits, deductibles, etc. required) of different companies will vary depending on the exposures particular to their business, it is recommended that companies obtain advice from a licensed insurance broker when purchasing coverage.

Cloud Computing:

Cloud computing refers to the delivery of hosted computer services over the internet. Michael noted that concerns with cloud computing services generally involve security breaches and service outages, and suggested that companies should seek contractual indemnification from outsourcers whenever possible. It may be possible for a client to be included as an additional insured under an outsourcer's cyber insurance network security and privacy insurance policy, but this is very rare. Most cloud service providers will not extend their insurance coverage to cover third parties because they do not know what kind (and the value) of data that is being stored on their service.

Insuring Against Cyberspace and Other Network Risks

First and Third Party Coverage Issues:

In his presentation on first and third party coverage issues, David R. Mackenzie, of Blaney McMurtry LLP, provided a detailed assessment of some of the related United States case law in this area due to the lack of relevant Canadian case law, as follows.

In *Retail Ventures Inc.* v. *National Union Fire* (6th Cir. Aug. 23, 2012) WL 3608432, a policyholder was able to get third party coverage on their Commercial General Liability ("CGL") insurance policy. In summary, Retail Ventures, a shoe retailer, was hit by a cyber attack that was carried out by both external hackers and some employees. Close to 1.4 million people had their credit card information stolen as a result. Retail Ventures was liable to both VISA and MasterCard and probably had no cyber insurance coverage. The insurer, National Union Fire, argued that the losses actually hit VISA and MasterCard and did not "directly" impact Retail Ventures. The Court however, held that "direct" did not mean a cause immediately preceding a loss – just the dominant cause, and ordered the insurer to pay out under its policy.

In *Eyeblaster, Inc.* v. *Federal Insurance Co.* (8th Cir. July 23, 2010) 613 F.3d 797, Eyeblaster provided online marketing solutions to advertising agencies and advertisers. The plaintiff alleged that Eyeblaster's program caused him to download spyware, which caused his computer to freeze frequently. Eyeblaster did not have cyber insurance coverage. The Court held that because the type of loss that was sought in the case was physical, for example, the plaintiff alleged that he could no longer use his computer (a physical property) – coverage under the CGL policy was triggered.

Zurich American Insurance Company v. *Sony Corporation of America* is a high profile case that is pending in New York and stems from the hack which Sony suffered to its Playstation Network in 2011. Personal information and credit card information belonging to millions of users were stolen. It is likely that Sony has cyber insurance coverage; however, it is possible that the tower of insurance in this case is inadequate and therefore Sony is hoping to obtain coverage under its CGL policy. In order to trigger coverage under the CGL policy however, the harm would have to constitute personal injury, which includes any oral or written publication of material that violates a person's right of privacy. Therefore, the question which the courts will have to address is whether hacking or stealing constitutes a publication or release.

Privacy and the new tort of "Intrusion Upon Seclusion":

In the Canadian context, David also presented on the potential for a connection arising from the Ontario Court of Appeal decision in *Jones* v. *Tsige*, 2012 ONCA 32, which created a new tort of "Intrusion Upon Seclusion", and the forthcoming Anti-Spam Legislation ("CASL"), by analogy to arguments that are being presented under United States case law. In *Jones*, the defendant had used information shared by her lover (an employee at Bank of Montreal) to access the online banking information of her lover's ex-wife. Because there was no pre-existing tort to address the harm in this situation, the court created a new one, but limited the penalty to a maximum of $20,000. Although this amount may not seem very large, the magnitude of an aggregate penalty may be impacted by CASL.

Under CASL, David explained that individuals may have a private right of action against companies who are found to breach the prohibitions in the legislation. David argued that it is not inconceivable that class action lawyers will argue, as part of a claim that the plaintiff class has had suffered 'intrusion upon their seclusion', although it remains, based on the facts of the particular case, as to how the invasion would be highly offensive to a reasonable person, which is part of the test.

In the United States the question of whether a communication may intrude upon a person's privacy has been considered. In *Owners Ins. Co.* v. *European Auto Works, Inc.* (8th Cir. Sept. 17, 2012) WL 4052406, the Court held that the receipt of a non-compliant email or fax constitutes a violation of a person's right to privacy, as the

act disrupted their peace and quiet. However, it is also uncertain whether anti-spam penalties constitute compensatory damages and are therefore covered under insurance policies. In *Standard Mutual* v. *Lay*, (2012 IL App (4th) 110527), Standard Mutual successfully argued that its actual loss ($0.05) was much less than the penalty imposed and was therefore not compensatory. The case is now before the Illinois Supreme Court. Either way, as penalties under CASL can be up to $10 million for corporations and $1 million for individuals, this is not an argument that should be taken lightly.

Finally, it is important to note that insurers will likely seek to protect themselves from anti-spam liability. One way they may do this is by clarifying in their insurance policies that, for example, a fax advertisement, being a form of commercial electronic message, is not a publication.

Matthew Wanford & Al Cheng (Articling Student-at-Law), Osler, Hoskin & Harcourt LLP