DOLDENWALLACEFOLICK LLP
Insurance Law Expertise... It's our policy.

Insurance Journal

July 5, 2013

Volume 1, Issue 4
Editor Keoni Norgren

In this Issue…

By Paul Dawson

Cyber Insurance – Who Needs It? (And <u>What</u> Do They Need, Anyway?)

Answering the first question is easy: anyone who collects or stores data about their customers, employees, or other individuals. That includes virtually every business, institution or organization in Canada.

The second question is… a bit more complicated.

"Cyber" coverage used to be a relatively obscure line of specialty insurance, but no longer. Rapid changes in technology, the economy, and the law are forcing businesses to consider new and potentially devastating forms of risk relating to the loss or misuse of sensitive data. Insurers have responded by developing a wide range of "cyber" policies and endorsements to cover those risks.

The Perils of Data

All cyber risks arise from the use or misuse of information, but the form and scope of those risks vary widely, depending on the nature of the insured's business.

Types of Data

The cyber coverage an insured requires will be guided in part by the type of data that it collects.

The broadest category of data can be loosely defined as "Personal Identification Information" (PII). PII commonly includes contact information, such as name, address, phone number, etc., but can also include social insurance numbers, electronic passwords, or details about one's family members and relationships. "Personal Health Information" (PHI) is a partially-overlapping subset of PII, consisting of medical and health related information; it could include

treatment records, diagnoses, prescription drug usage, genetic information, etc. A second subset of PII is "Financial and Credit Information" (FCI), including banking and credit card information.

Insureds may collect some or all of these types of data, in varying degrees. A small retailer or non-profit organization might collect simple contact information about its customers or donors; an online vendor might also hold credit card information. PHI will typically be collected by medical professionals and institutions, but may also be held by insurers, educational institutions, and other public bodies. Banks, credit unions, rating agencies, and insurers all hold FCI. Employers will often hold all three types of data about their employees. Knowing what types of data an insured collects is important to insurers because it may help indicate the likelihood and potential severity of claims that might arise. One study of cyber insurance claims between 2009 and 2011 found that data breaches involving PHI made up only about 15% of claims; breaches involving FCI and other PII made up 40% and 42% of breaches, respectively.[1] Medical and financial information will typically be more sensitive than mere contact information, so breaches involving PHI and FCI may be more likely to lead to litigation, and be more costly to resolve: a 2013 study found that "per capita" costs, *i.e.*, total costs divided by number of records disclosed, were greatest in breaches affecting the healthcare ($233), financial service ($215), and pharmaceutical ($207) industries, and lowest in media services ($103), public services ($81), and retail businesses ($78).[2]

Third Party Liability Risks

The first broad category of cyber risks involve liability to third parties for the loss or mishandling of personal information. Claimants who allege their data has been lost or improperly used will

[1] Mark Greisiger, NetDiligence, "Cyber Liability & Data Breach Insurance Claims", October 2012.
[2] Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis", May 2013.

typically seek damages for breach of privacy, whether at common law (as in *Jones v. Tsige*, 2012 ONCA 32) or pursuant to a statutory cause of action, where such legislation exists. Such events can arise from improper review of personal information by an insured's employees, as in *Tsige*, or from the theft of personal data through malicious hacking, as in the notorious data breaches that afflicted the Sony Playstation Network in May, 2011. The Sony case is said to have spawned more than 50 class actions and other lawsuits against the company.

The costs of defending and resolving data breach cases can be substantial. One study found that the average settlement for data breach cases between 2009-2011 was $2.1 million, with defence costs averaging $582,000.[3] In *Tsige*, the claimant received damages of $20,000 for breach of privacy; such an award to each member of a class action could become very expensive indeed. However, in many cases it will be difficult for claimants to prove that they have suffered any actual loss, and such actions often settle for more modest amounts than originally claimed. For example, a class action in Ontario relating to the Sony Playstation Network breach, *Maksimovic v. Sony of Canada Ltd.*, claimed to represent one million class members, and sought $1 billion in damages – yet the proposed settlement created a fund of less than $1.5 million to satisfy all claims.[4] Not an insignificant sum, but not one that would likely trouble organizations of Sony's stature.

Similarly, a 2011 class action against Durham Region Health in Ontario initially sought $40 million following a data breach, but settled upon the payment of $500,000 in costs plus the establishment of a process to handle claims from any class members who demonstrate they have suffered loss from the breach.[5] It is yet to be seen how many claims might ultimately be paid out, if any.

[3] Greisiger, above, October 2012.
[4] Notice of proposed settlement.
[5] *Rowlands v. Durham Region Health*, 2012 ONSC 3948.

First Party Losses

The second broad category of cyber risks insureds might face relate to the insured's own first-party losses, including those incurred to respond to regulators, to investigate a breach, and to restore the insured's business operations and reputation.

Coverage for the cost of responding to regulatory inquiries will likely become an increasingly important element of cyber insurance, particularly as legislation regarding privacy, electronic commerce, and data generally becomes more common. In our May 2013 newsletter, Shelley Armstrong described how Provincial and Federal privacy commissioners in Canada have a statutory mandate to investigate privacy issues, in response to complaints or on their own motion. In June, 2013, the Federal privacy commissioner's Report to Parliament describes her office's investigations into an insurer's use of credit ratings to set premiums; a bank's release of information to a wife about her husband; and even the unauthorized disclosure by one summer camp to another about a particular child – a total of 220 formal investigations. The Report also describes the commissioner's response to 33 voluntary reports of data breaches, and a "compliance audit" performed on a major Canadian retail chain.[6] Such investigations will become more common if Canada's 2010 anti-spam legislation is finally brought into effect,[7] or if federal privacy legislation is amended to include mandatory data breach notification, as is currently proposed.[8]

Investigations can also arise from other quarters. For example, the Securities Exchange Commission in the United States published guidelines in 2011 as to how registrants should disclose in their public filings details of cybersecurity risks affecting their businesses (including in some cases details of their cyber insurance coverage),

[6] Office of the Information and Privacy Commissioner, Annual Report to Parliament 2012.
[7] Bill C-28, commonly known as the "Anti-Spam Legislation", received Royal Assent on December 15, 2010, but is not yet in effect.
[8] Bill C-12, *An Act to Amend the Personal Information Protection and Electronic Documents Act.*
[9] SEC, "CF Disclosure Guidance Topic No. 2: Cybersecurity", October 13, 2011.
[10] Hunton & Williams LLP, "Disclosure of Cybersecurity Risks in SEC Filings on the Rise", March 13, 2013.
[11] University of Victoria, "Credit Monitoring Services."
[12] Greisiger, above, October 2012.

and specifying the information that must be released to the market concerning data breach events.[9] As it becomes increasingly common for registrants to disclose cyber risks,[10] those who provide inadequate disclosure may face increased scrutiny from the SEC (and from securities class action lawyers...).

When a data breach occurs, an insured may face immediate "crisis management" costs. These can include forensic analysis to investigate the breach and prevent future breaches; notifying affected parties about the breach; and the provision of services intended to reassure affected individuals, *e.g.*, by providing ongoing credit monitoring services. The University of Victoria in British Columbia offered to provide such services to 11,000 employees whose personal information was contained on a lost, unencrypted USB stick in January, 2012.[11] The cost of credit monitoring alone can amount into the millions of dollars, though the typical range is between $6,000 and $300,000 per data breach.[12]

The cost of resuming operations and restoring an insured's reputation may in some cases require the reconstruction of essential data that has been lost or become corrupted. Malicious "denial of service" attacks can even in some cases damage network hardware, requiring physical replacement or repair.

Retailers can also face significant data breach expenses from a different quarter – penalties imposed by agreements with credit and debit card transaction processors. For example, footwear retailer Aldo Group Inc. was assessed penalties of nearly $5 million (USD) by Mastercard following a 2010 data breach. Aldo sought reimbursement from its directors and officers liability insurer. In May, 2013, the Quebec Superior Court concluded that the penalties arose from contractual obligations Aldo chose to assume, i.e., to protect

[13] *Aldo Group Inc. c. Chubb Insurance Co. of Canada*, 2013 QCCS 2006.
[14] Betterley, above, May 2013.
[15] Godes, above, March 2012.
[16] Craig Harris, "Cyber Surge", *Canadian Underwriter*, June 2012.
[17] David Mackenzie, "Data Risk, Privacy Breach and Insurance Coverage", Insurance Brokers Association of BC, *BC Broker*, June 2013.

confidential information, not from any alleged "Wrongful Act" under the policy in question, and were thus caught by a "Contractual Liability Exclusion" clause in the policy.[13]

Types of Coverage

As shown above, cyber risks are extremely diverse. They can involve different types of data; affect small, medium, and large enterprises in every economic sector; and produce third- and first-person losses of many varieties. The extent and potential scale of these risks depends heavily on an insured's individual context. No surprise, then, that the insurance industry offers a wide range of insurance products to address those risks.

Stand-alone Cyber Insurance Policies

Many insurers have developed free-standing cyber insurance policies, rather than offer endorsements that may sometimes sit awkwardly with existing forms of coverage. They are more typically purchased by large commercial entities, and especially those with significant on-line or technology-related activities.[14] Cyber insurance policies vary widely in form, even in their most essential elements (*e.g.*, duty to defend vs. reimbursement, claims-made vs. occurrence, insuring triggers, notice requirements, etc.).[15]

However, stand-alone policies are relatively new in Canada, and have not yet been widely adopted. Specialized cyber liability experience is relatively rare among underwriters and brokers in Canada, and the paucity of claims history can make it difficult for underwriters to determine appropriate premiums.[16] In the short term, insurers are more likely to offer cyber insurance incrementally, by offering endorsements to traditional, non-cyber forms of insurance.[17]

[18] Sony is currently locked in coverage litigation with its CGL insurer in the United States as to whether claims arising from the Playstation Network data breaches are covered.
[19] For example, *Netscape Communications Corp. v. Federal Ins. Co.*, 343 F. App'x 271 (U.S.C.A., 9th Cir. 2009); *Zurich American Ins. Co. v. Fieldstone Mortgage Co.*, 2007 U.S. Dist. LEXIS 81570.
[20] *Eyeblaster, Inc. v. Federal Ins. Co.*, 613 F.3d 797 (8th Cir. 2010).
[21] Scott Godes, ABA 2012 Insurance Coverage Litigation CLE Seminar, "Insurance for Cyber Risks: Coverage Under CGL and "Cyber" Policies", March, 2012.

Cyber Endorsements to Commercial General Liability Policies

CGL policies are commonly acquired by commercial and non-profit entities of all sizes, and in every sector. Hoping to appeal in particular to small to medium enterprises (SMEs) who might otherwise not consider purchasing cyber coverage, many insurers have designed cyber insurance endorsements that can be added onto an existing CGL policy.

Such endorsements are necessary because the scope of cyber coverage available under CGL policies is often unclear.[18] CGL policies typically only cover losses suffered by third parties arising from "physical injury" or "property damage". Many CGL policies contain explicit exclusions for damage to "intangible property" such as electronic data.

However, some policies cover "personal injury" claims, which may include cyber risks such as on-line defamation or breach of intellectual property rights. Unauthorized access to private information has been held to be a form of "personal injury" in several American cases.[19] Another case found that "loss of use" of a computer allegedly infected by malware negligently distributed by the insured was a form of physical loss, triggering a duty to defend under a CGL policy.[20] One author has suggested that credit monitoring services should be covered under CGL policies, analogizing to medical monitoring sometimes offered to individuals who claim that exposure to a harmful condition might lead to future health problems.[21]

One of the advantages to offering cyber insurance by endorsement to existing CGL policies is that CGL policies are already modular in form. Insureds can purchase additional coverage for particular risks affecting their businesses, such as auto or marine coverage.

[22] Rick Betterley, "Cyber Endorsements for Traditional Insurance Policies", International Risk Management Institute, The Risk Report (Vol. XXXV, No. 9), May 2013.

Many commercial policies also offer integrated property, errors & omissions, fidelity, business interruption, or other types of insurance that can be adapted by analogy to cover cyber risks. Insureds might therefore purchase cyber coverage for third party losses alone, or also for its own first-party losses, depending on the nature of the insured's business and risk exposure.[22]

Cyber Endorsements to E&O/D&O Liability Policies

Other insurers offer cyber insurance endorsements for errors and omissions or directors and officers liability policies. These policies may are in some respects more flexible than CGL policies – they usually cover losses arising from "wrongful acts", which can be defined widely enough to include purely economic losses or other forms of intangible injury. As noted above, publicly-traded companies may face increasing obligations to disclose cyber risks in their corporate filings; D&O policies already cover claims arising from other types of misrepresentations in such filings.

Because E&O and D&O insurance is more commonly purchased by professional services firms and larger or more sophisticated corporations, the cyber coverage they require may in many cases be broader than that offered in CGL policies held by SMEs. For example, entities with E&O or D&O coverage are more likely to require coverage for the costs of responding to regulatory investigations.

The Right Coverage?

As the market for cyber insurance products continues to evolve, the challenge for insureds and underwriters alike will be to match the right coverage to the right risks, at the right price.

Insureds should determine the types of cyber risks they face, considering the types of data they collect, and how they use and store that data.

The extent to which their existing insurance arrangements cover – or might not cover – those risks, and whether a stand-alone cyber insurance policy or a cyber endorsement to an existing policy would be preferable. They should consider whether they need coverage for third-party liability, first-person losses, or both, and whether they might also need access to the technical support, risk management, and crisis management services offered under some cyber insurance programs. In all cases, insureds should consider carefully whether the insuring clauses, policy limits (including sub-limits and deductibles), and exclusion clauses contained in competing cyber insurance products will best serve their needs.

For their part, underwriters will want to carefully assess the risks presented by each insured's operations, taking into particular account the types of claims most typically associated with the data and industry sector involved. Cyber insurance products will likely need to be carefully tailored to the legislative regime in each jurisdiction, *e.g.*, in jurisdictions that require insureds to notify their customers or clients about data breaches, or that have instituted robust regulatory mechanisms to investigate privacy complaints. Pricing will likely remain difficult until a more extensive claims history can be established; the provision of risk management services, particularly to SMEs, may prove particularly helpful in controlling defence and indemnity costs.

Editor

Keoni Norgren, Tel: 604-891-5253 E-mail: knorgren@dolden.com

Please contact the editor if you would like others in your organization to receive this publication.

Contributing Authors

Paul Dawson, Tel: 604-891-0378 E-mail: pdawson @dolden.com

Vancouver, BC

Tenth Floor - 888 Dunsmuir Street
Vancouver, B.C.
Canada / V6C 3K4

Telephone: (604) 689-3222
Fax: (604) 689-3777
E-mail: info@dolden.com

Toronto, ON

200-366 Bay Street
Toronto, Ont.
Canada / M5H 4B2

Telephone: (416) 360-8331
Fax: (416) 360-0146
E-mail: info@dolden.com

Kelowna, BC

308-3330 Richter Street
Kelowna, B.C.
Canada / V1W 4V5

Telephone: (250) 980-5580
Fax: (250) 980-5589

E-mail: info@dolden.com