

CORPORATE GOVERNANCE

Cyber Risks & Privacy Liability— Are You Covered?

BY MURN MEYRICK, JONATHAN ASHALL AND FERNAND VARTANIAN

Good risk management requires a look beyond D&O coverage when it comes to significant exposures to both the corporation and individuals in this new cyber world

If you haven't been hit by virus, spyware or data theft—be prepared. You may be next. In recent months, we have witnessed an increase in security breaches. In light of well-known corporate scandals such as Enron and Hollinger Inc., directors and officers have been scrutinizing their director and officer liability (D&O) coverage. However, good risk management requires a look beyond D&O coverage when it comes to significant exposures to both the corporation and individuals in this new cyber world.

Actions by legislators across North America continue to impact businesses and have further raised network security to a strategic business concern. Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to organizations in provinces other than Alberta, British Columbia and Quebec (where provincial privacy legislation applies). Organizations are required to protect all personal information in their custody or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, copying, modification or disposal of personal information. PIPEDA is currently under parliamentary review, where it will likely be amended to require organizations suffering security breaches to notify individuals whose information is at stake, credit agencies, and relevant government agencies or banks. (Such notifications have triggered class-action lawsuits in the US.)

Today's web-based technology and extensive public and private computer networks afford businesses and their customers more speed and convenience than ever before in terms of functions and transactions, but the benefits to both parties are fraught with new and complex risks. Businesses should consider their exposure to key e-business risks and identify insurance solutions to mitigate their potential exposures. Risks can arise from:

Privacy/identity theft—unauthorized access/use of credit card information: Identity theft involves the unauthorized

use of others' personal information in order to commit fraud. Individuals as well as businesses and professional service firms that use or store personal information (including outsourced service providers) are exposed. Data is most often stolen by employees, vendors or outside hackers and most commonly used to commit credit card, bank account and phone services fraud.

Malicious code: The rising incidence of malicious code—viruses, worms, Trojan horses—is causing network damage and crippling denial-of-service attacks. Network and website disruptions can result in large losses for businesses as they, and many of their customers, rely on the network (i.e., supply chain, fulfillment, logistics) and web (i.e., online sales for transactions).

Reliance on supply chain, logistics and other network operations: Network outages may result in the temporary shutdown of a business's critical operations, including supply chain, logistics, websites and credit card processing. If critical business and operational functions are outsourced to vendors, day-to-day control over operations may be lost despite contractual agreements.

Theft of proprietary competitive business data: Electronic theft of confidential data can wreak havoc on operations and a company's marketing edge.

Online media—breach of intellectual property rights: Content published on a website or electronic advertising may infringe upon third parties' trade-marks or copyrights or disparage a name or likeness.

Downstream liability: There can be a liability risk to third parties (e.g., vendors, distributors, suppliers, customers, business partners) for passing on malicious code

or facilitating an attack via a network.

Costs

Identity and security breaches can come with devastating costs. TJX has estimated costs associated with its computer data breach at US\$25 million and ongoing. Costs associated with privacy breaches fall into three main categories: direct damage costs, liability arising from third parties and costs associated with a company's privacy disclosure plan.

Direct Damage Costs

- decline in revenue related to the breach
- extra expenses to mitigate the loss
- costs to restore information assets (e.g., reconstructing client files)
- changes to the internal processes to ensure a preventative measure is in place to avoid reoccurrence.

Liability to Others

- contingent (downstream) business interruption (e.g., denial of service)
- compensation to affected clients from unauthorized access to personal information
- third-party subrogation costs (e.g., credit card issuers' charge-backs to the retailer for costs to reissue credit cards due to a network breach).

Response Plan to a Breach in Privacy

- public disclosure to clients including letters, publicity (newspapers) and face-to-face interaction
- regulatory costs and fines: interaction with regulators; local and national law enforcement authorities; auditors; Alberta's *Freedom of Information and Protection of Privacy Act (FOIP)* imposes fines of up to \$500,000 for the willful disclosure of employee information
- crisis management costs: establishing a call centre and website to handle inquiries; credit monitoring; special oversight committee; law firms and public relations professionals.

Traditional Insurance—Mind the Gap

In light of the financial, regulatory and reputational risks confronting businesses, it is imperative that organizations have sufficient insurance coverage in place. However, many questions remain regarding the adequacy of traditional insurance programs to address this risk. Most traditional insurance policies do not cover the risks that arise in today's cyber world.

Property insurance policy: Usually requires physical

damage to a tangible asset to trigger the coverage. This is problematic in a cyber breach, because data is not considered tangible property in most policies. Also, computer viruses and hacker attacks seldom damage systems physically. Finally, most property policies include computer virus exclusions, or provide for small sub-limits of coverage.

D&O insurance policy: Generally only covers directors and officers. Cyber breaches would more typically attract entity liability, and the entity, if covered at all, would only have securities loss coverage under the D&O policy. Problematic provisions would include the property damage and intentional acts exclusions.

General liability insurance policy: Difficult to trigger for a privacy breach. First, physical damage or bodily injury is not activated in a network security breach. Second, coverage for Advertising Injury and Personal Injury may not respond to intentional and/or criminal acts, like breach of confidential data due to a hacker or computer virus.

Crime insurance: Covers theft of money and securities, but does not cover the true costs arising from the theft of data, information and account numbers.

Professional liability/errors & omissions insurance policy: Typically excludes intentional acts. Often an event such as a security breach can not only harm a client, but also a client's customers. Many E&O policies do not respond to these types of events.

Cyber Risk Insurance—The Solution

Cyber risk insurance fills the gaps and exclusions in traditional coverages. It provides both first- and third-party protection for risks incurred by Internet and network operations. The kinds of loss covered by cyber risk insurance include business interruption/income loss, and expenses associated with security notification requirements and other public relations expenses. As in all areas of risk management, the solution lies in defining the business risks, understanding the exposures, and then tailoring a specific risk management and insurance program to meet the needs. ☺

Murn Meyrick is a lawyer and senior vice-president of the executive risks practice, Jonathan Ashall is senior vice-president and Canadian practice leader for executive risks practice, and Fernand Vartanian is chief compliance and privacy officer of Willis Canada Inc., a global insurance broker.