CORPORATE GOVERNANCE REPORT

Volume 10 • Number 1 March 2015

In This Issue:

LexisNexis®

Risk Management in a Digital World: Addressing Cyber-Security Threats at the Board Level

Adam Kardash
Partner, Privacy and Data Management
Osler, Hoskin & Harcourt LLP

Shawn Irving
Partner, Litigation
Osler, Hoskin & Harcourt LLP

Carly Fidler
Associate, Litigation
Osler, Hoskin & Harcourt LLP

Carey O'Connor
Associate, Litigation
Osler, Hoskin & Harcourt LLP

The role of the board of directors has necessarily adapted to include an increased focus on risk management. In our digital world, cyber-attacks are now a pervasive risk, and the perceived lack of board oversight has garnered scrutiny by consumers, regulators, legislators, litigants, and the media.

News headlines in 2013 and 2014 underscore that the frequency and magnitude of cyber-attacks is greater than ever. Large scale cyber-attacks have left corporate victims scrambling to remedy their financial and reputational injury. Over the past number of months, a number of high-profile examples of security breaches—including state-sponsored attacks and unauthorized intrusions impacting millions of customers' credit card information and email addresses—have appeared on front pages in newspapers around the world. It is clear this issue affects both private and public companies. The cost to remedy a cyber-attack can easily run into the millions of dollars, not to mention the reputational cost and threat of litigation, which are far more difficult to quantify.

Corporate Governance Report

The **Corporate Governance Report** is published quarterly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

ISBN 0-433-45174-2 **ISSN 1718-2476**
ISBN 0-433-45172-6 (print & PDF)
ISBN 0-433-45173-4 (PDF)
ISSN 1718-2581 (PDF)

Subscription rates: $340.00 (print or PDF)
$425.00 (print & PDF)

Risk of Class Action Litigation from Cyber-Attacks

In Ontario, several class actions have been certified or partially certified, where the alleged wrong is premised on the collection and subsequent loss of customer information.

In *Evans v. Bank of Nova Scotia*,[1] a bank employee provided his customers' confidential information to his girlfriend, who used it to commit identity theft. The affected bank clients are now suing the employee and the bank.

In *Condon v. Canada*,[2] the Ministry of Human Resources and Skills Development Canada lost a hard drive that contained the names, birthdays, addresses, student loan balances, and SINs of 583,000 people. An action was commenced against the Ministry. Over the summer of 2014, the action was partially certified based on breach of contract and the tort of intrusion on seclusion.

These class proceedings are in early stages, and they serve as examples of the risk of collection of electronic customer information.

Risk of Data Being Held by Third Parties

In the emerging data environment, it is increasingly common for third parties to hold information about a company's clients and customers. In 2013, the Canadian Securities Administrators announced that it was launching an investigation into the Investment Industry Regulatory Organization of Canada ("IIROC") after one of its staff members lost a portable device containing information about investment dealer clients.

The confidential information pertained to IIROC member firms but was possessed by IIROC. The IIROC example illustrates that companies are not immune to risk if their customer data is possessed by a third party. Indeed, without adequate controls, providing information to a third party can increase the risk.

The Risk to Boards of Directors

Despite the high-profile examples of the costly impact of cyber-security breaches, surveys focusing on risk mitigation suggest that many boards are not actively addressing cyber-risk management, including

insisting upon and reviewing security program assessments and policies, reviewing budgets, delegating responsibilities for privacy and security, and being informed regularly of breaches and new risks. Not only does this leave a company exposed, but it also leaves a board exposed to potential shareholder activism.

Boards can minimize their chance of crisis and reduce corporate and director exposure by overseeing the risk management process and ensuring their companies have a clear response plan in the event of a cyber-attack. In a recent speech on the topic, Luis A. Aguilar, a Commissioner of the U.S. Securities and Exchange Commission ("SEC"), outlined that boards should, at a minimum, have a clear understanding of who has the primary responsibility for cyber-security risk oversight and ensuring the adequacy of the risk management practices. He also recommended the creation of a separate enterprise risk committee on the board, mandatory cyber-education, and regular reporting to the board. Boards should also consider obtaining cyber-insurance coverage. A company's response after a breach of security is just as important as a preventative plan. Boards should ensure that management has a deliberate response plan consistent with best practices for the industry and the goals of the company.

Another key development is the move toward potentially enhanced disclosure requirements for cyber-security risks and practices. The Canadian Securities Administrators suggest that issuers should consider whether the cyber-security risks they face, any cyber-security incidents they may experience, and any controls they have in place to address these risks are matters that need to be disclosed in a prospectus or a continuous disclosure filing. The SEC has made similar suggestions for U.S. public issuers.

As cyber-attacks become more frequent and more sophisticated, the need for a proactive strategy has never been more important. Directors should make themselves aware of their company's policies for protection of confidential information, and work to ensure that their policies follow the best practices in the industry. Directors and officers should also ensure that there is adequate liability insurance coverage in the event of a cyber-attack.

[*Editor's note*: A version of this article first appeared on Osler, Hoskin & Harcourt's *Risk Management & Crisis Response* blog <www.riskandcrisismanagement.com>.]

---

1 [2014] O.J. No. 6014, 2014 ONSC 7249.
2 [2014] F.C.J. No. 297, 2014 FC 250.

Cyber-Security Corporate Governance: Three Essential Steps to Form a Cyber-Security SWAT Team

Duncan C. Card
Bermuda Managing Principal, Co-head Technology, Outsourcing and Procurement
Leading Canadian Technology, Outsourcing and E-Commerce Lawyer
Bennett Jones LLP

Last year, *Canadian Lawyer InHouse* magazine[1] posed the question, "Should in-house counsel be asking more questions about the strength of their company's cyber systems?" They cited the Association of Corporate Counsel 2012 survey that reported 28 per cent of their companies had experienced a cyber-security breach in the preceding 12 months and "data breaches and protection" as one of the top issues keeping them up at night.[2] In my view, the best answer to this question is that in-house counsel should be actively participating in providing cyber-security corporate governance leadership and risk management guidance, including legal and compliance advice.

Regardless of your industry or business sector—whether retail, transportation, financial services, manufacturing, energy, or otherwise—there are now daily (if not hourly) news reports of aggressive, targeted, and damaging cyber-attacks that cause significant financial, reputational, and commercial harm to the enterprise as affected, whether through data breaches, trade secret theft, or business disruption otherwise. Chances are the bigger or more visible your company is, the more international

your company is, or the closer your company is to our critical infrastructure, the more likely your company is a target for cyber-attack. For example, in March of this year, the Department of Homeland Security in the U.S. reported[3] the following statement by the Chairman of the California Energy Commission: "If you're a utility today, depending on your scale, you're under attack at this moment".[4] Similarly, Canada's the *Globe and Mail* newspaper recently reported that,

> North America's electricity grid is facing increasing risk of cyberattacks from criminals, terrorists and foreign states, and utilities have to devote growing resources to defend the system [….] In a report last year, cybersecurity firm Mandiant Corp.[5] exposed a multiyear, large-scale computer espionage threat [across many sectors] originating from a group in China with close ties to the People's Liberation Army [….] Robert Gordon, a special adviser to Public Safety Canada on cyber threats, identified three distinct risks that Ottawa is working with industry to combat: criminal, espionage and activism.[6]

Therefore, right now, before your company is hit by another cyber-attack (yes, another)—whether by hackers, agents of IP espionage, malware, activists launching a denial of service attack, or by a disgruntled employee—you need to proactively formulate the practices and resources that your organization requires in order to manage the response to such attacks. I believe it is possible to summarize the governance undertakings that are required to reasonably manage the risk of cyber-attack into a three-step process, all of which may lead to the assembly, organization, and training of a cyber-security response SWAT (Special Weapons and Tactics) Team comprised of managers (internal and/or external professionals) who will know exactly what to do, and who can be called into action on a moment's notice, in the event of a cyber-threat.

Step One

First, make sure that the board of directors, the C-suite, and the managers of your company's IT and web-enabled infrastructure understand and appreciate the fast-paced world of cyber-insecurity, including all relevant threat sources, your organization's general vulnerability, and the potential business financial, reputational, and legal risks that your enterprise uniquely faces. As part of that exercise, all of the constituent subject matter experts in your organization should be identified and assigned to assist and contribute to that essential awareness exercise and in all of the undertakings that will follow. Experts in IT corporate governance, reputational and crisis management, cyber technology risks, advanced HR practices, and your company's unique legal and regulatory compliance duties should all play a vital role in understanding the nature and scope of cyber-security threats.

Step Two

There are two distinct aspects to the second step of preparedness.

First, enterprises should undertake a detailed review, assessment, and audit of their cyber-security history (either its direct experiences or by sector benchmarking), its vulnerability, and the risks and potential key business liabilities it may face—both commercial and regulatory (compliance) in nature. Every enterprise relies upon and uses the Internet and IT infrastructure very differently, and those different combinations of use and reliance will create a unique matrix of risk, potential liability, and defence posture. That is why a comprehensive assessment of how your enterprise is uniquely positioned (or not) to address cyber-threats is an essential aspect of security preparedness. As well, that assessment must include a comprehensive survey of your company's unique legal, regulatory, and compliance duties so that your cyber-incident action plan will be crafted to include all of your organization's required notification, reporting, and disclosure requirements.

Second, based upon your company's unique cyber-risk assessment, an overall cyber-security strategy must be formulated and implemented. That strategy review will likely consider the following:

- necessary technological and business process security improvements
- third-party security contributions and testing (including encryption service providers, ethical hacking services, *etc.*)
- a review of all relevant HR security programs
- your organization's online connections and practices with its key business partners, such as

suppliers, customers, and the service providers it depends upon to carry on business

- the need for cyber-risk insurance
- business continuity and contingency plans
- the formulation of cyber-security policies, procedures, and practices (including a cyber-incident action plan) that will address cyber-incident prevention, reporting, response, and harm mitigation.

Such corporate cyber-security policies usually include the following:

- information (awareness) systems to remain "threat current" (including warnings from trade associations and public sector security services such as police, public sector security alerts, and access to the full range of governmental support systems)[7]
- employee training programs
- IT security policies, possibly including data and IT access restrictions, segregated data, and SaaS or Cloud security stipulations
- supplier, customer, and e-commerce security practices
- management and employee resource allocation for ongoing security governance activities
- internal management policies, including the creation of a cyber-attack response and management SWAT Team.

Step Three

Based on your assessment of cyber-security vulnerability and risk, and in accordance with the directly resulting cyber-security policies and procedures that are formulated, your enterprise should proactively consider putting a specialized team of trained managers in place to both oversee the organization's cyber-security preparedness and response capabilities, as well as stand as the crisis management team in the event of a cyber-attack, including the following:

- to oversee the existing policies and procedures to ensure that they are properly implemented and that all related practices are constantly improved (as needed)
- to ensure that the company's preparedness is adequate (through testing and otherwise) and to have the management authority to correct any deficiencies
- to be trained, coordinated, and ready to immediately act on several fronts in the event of a cyber-threat in accordance with a detailed cyber-threat action plan

Basically, that focused management team may be thought of as a Cyber-Security SWAT Team.

Upon being first notified of a cyber-attack, the Cyber-Security SWAT Team will focus on the following choreographed efforts:

- identify/discover and diagnose the specific cyber-threat
- terminate the threat as quickly as possible
- assess its continuation (or abetment) and determine (if possible) the extent of any harm and unauthorized activity (impact assessment)
- act to mitigate or avoid potential harm
- work with third parties (police, regulators, telco, suppliers, distributors, *etc*.) to address all relevant stakeholder interests
- manage precipitating reputational issues, stakeholder communications, and public relations
- attend to all legal, regulatory, and compliance (including required or beneficial reporting, whether to insurers, regulators, or otherwise) activities while also preserving the enterprise's legal rights and defences in the face of any possible litigation or regulatory concerns

Typically, such Cyber-Security SWAT Teams would comprise (at least) the following key skill sets:

1. a crisis management leader to make (or shepherd) critical and urgently required business decisions
2. a highly trained IT manager with cyber-security technical expertise
3. a legal advisor to ensure compliance, to help assess sources of liability (including to identify any possible plaintiffs or classes of plaintiffs), and

to undertake any required legal action (immediate or otherwise)

4. a reputation management expert to address reputational risks and to attend to any public (stakeholder) relations, media relations, and even government relations matters that may arise, depending upon the nature of the cyber-attack.

Cyber-security is now an essential aspect of corporate governance, business risk management, and legal (regulatory) compliance, and a Cyber-Security SWAT Team might serve as an excellent catalyst for top-down governance oversight and management of that increasing enterprise threat.

---

1 Jennifer Brown, "Managing Cyber Risk", *Canadian Lawyer Inhouse* 8, no. 3 (June 2013), 36.

2 *Ibid*., p. 36.

3 Homeland Security News Wire, "Making the Grid Smarter Makes It More Vulnerable to Hackers" (March 25, 2014), <http://www.homelandsecuritynewswire.com/dr20140325-making-the-grid-smarter-makes-it-more-vulnerable-to-hackers>.

4 Per Robert Weisenmiller, Chairman CEC, at page 1.

5 Mandiant Intelligence Center Report, APT1: Exposing One of China's Cyber Espionage Units, <http://intelreport.mandiant.com/>.

6 Shawn McCarthy, "Utilities Face Growing Risk of Cyberattack", *Globe and Mail* (May 7, 2014), B5, <http://www.theglobeandmail.com/report-on-business/expanding-electricity-grid-poses-cyberthreat-for-utilities/article18536720/>.

7 *See* Communications Security Establishment Canada's list of IT and Cyber-Security publications, such as the COTS Security Guidance, CSEC's Top 35 Cyber Threat Mitigation Measures, *etc.*; the Canadian Cyber Incident Response Centre (CCIRC), operated by Public Safety Canada; and many other accessible resources.

Cyber-Security Governance and D&O Liability

Charles Morgan
Partner
McCarthy Tétrault LLP

Sean Griffin
Partner
McCarthy Tétrault LLP

Introduction

The assessment of a corporation's cyber-risks is part of a board of directors' general risk oversight responsibilities. Since lawsuits, including class actions, are often commenced soon after a data breach, directors and officers should now consider that the board's oversight of cyber-risks may also be closely and thoroughly scrutinized in future litigation and regulatory investigations.

On October 20, 2014, a New Jersey court dismissed a shareholder derivative suit that sought damages notably from the directors and officers of Wyndham Worldwide Corp. ("WWC") for several data breaches.[1] This decision is the first decision issued in the U.S. in a shareholder derivative claim arising out of data breaches. The decision is important and instructive for board members, since it provides examples of approaches to cyber-risk oversight, which directors and officers may implement to help shield them from liability in the context of data breaches.

The Relevant Facts and the Claim

In the course of its business, WWC collects the personal and financial information of clients, including payment card account numbers, expiration dates, and security codes. Between 2008 and 2010, WWC suffered several data breaches that resulted in the theft of credit card information of more than a half million of its clients. In April 2010, the Federal Trade Commission began investigating the data breaches and commenced legal action against WWC for its security practices.

In November 2012, a shareholder sent a letter to WWC's board, requesting that WWC commence a lawsuit against the members of the board. The shareholder alleged that the directors and officers were liable to WWC for breach of fiduciary duty. The board's audit committee mandated external lawyers to assess the shareholder's demand. Counsel investigated the allegations and concluded that they were not founded. WWC therefore decided not to commence any proceedings against the board members.

In June 2013, shareholder Dennis Palkon ("Palkon") provided WWC with another letter reiterating the demand. This second demand was also dismissed as unfounded, based on the investigation that had been done previously. Palkon then commenced a derivative action on behalf of WWC against the board members for breach of the fiduciary duties of care and loyalty, corporate waste, and unjust enrichment. It was alleged that the directors and officers were responsible for the following:

- failing to oversee and implement the proper internal controls to protect the personal and financial information of clients
- allowing WWC to conceal the data breaches from investors and clients
- failing to conduct a reasonable investigation
- negligently refusing to commence proceedings against the board members

On October 20, 2014, Justice Stanley R. Chesler dismissed Palkon's derivative action with prejudice, based on the finding that WWC had done a reasonable investigation into the data breaches, following the initial demand to commence proceedings against the board members. Therefore, the decision not to commence proceedings was protected by the business judgment rule.

The investigation that led to this decision demonstrated that prior to the data breaches, WWC had cyber-security policies and internal controls in place. These had been discussed numerous times at the board level. After the data breaches, more than 10 board meetings took place where WWC's security policies, internal controls and security enhancements were discussed. The audit committee also held more than 15 meetings in the context of its investigation of the data breaches to review the policies, procedures, and internal controls related to cyber-security. WWC's board had therefore based its decision not to commence proceedings against the board members on a thorough investigation of their conduct prior to and after the data breaches.

This decision by Chesler J. to dismiss the action underlines the importance of direct board involvement in addressing cyber-security, both before and after a data breach occurs.

Conclusion

In light of the decision rendered in the *WWC* case, the following are examples of steps that could now be considered by management and board in identifying and assessing the corporation's cyber-security risks:[2]

- Adopting written cyber-security policies, procedures, and internal controls:
  - The incident plans and protocols should consider whether and how cyber-attacks should be disclosed to customers, to investors, regulators, law enforcement, *etc*.
  - An incident response team should be identified and clear responsibilities given to each member.
- Implementing methods to detect the occurrence of a cyber-security event.

In addition, the following steps could also be considered:

- Management and board members could discuss the appointment of a chief information officer or a chief information security officer with the expertise to meet regularly with and advise the board.
- Consideration could be given to appointing a board member with cyber-security expertise and experience (or the board should seek out an expert who can provide presentation(s) to the board in this regard).
- The board should review annual budgets for privacy and IT security programs.
- The board should receive regular reports on breaches and cyber risks.

The board should have a clear understanding of who in management has primary responsibility for cyber-security risk oversight and for ensuring the adequacy of the company's cyber-risk management practices.

---

1 *Palkon v. Holmes et al.*, Civil Action No.: 14-CV-01234 (SRC), which can be found at <http://law.justia.com/cases/federal/district-courts/new-jersey/njdce/2:2014cv01234/300630/49/>.

2 These recommendations are notably inspired by the following two documents:

- *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus* presentation by Luis A. Aguilar, *Commissioner*, Securities and Exchange Commission (June 10, 2014), <http://www.sec.gov/News/Speech/Detail/Speech/1370542057946>.
- *Framework for Improving Critical Infrastructure Cybersecurity* by National Institute of Standards and Technology, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

Help—We've Been Hacked!

Cyber-Risk Insurance and Related Legal Issues

Belinda A. Bain
Partner
Gowling Lafleur Henderson LLP

Mark Coombes
Summer Law Student
Gowling Lafleur Henderson LLP

A nightmare scenario for any business: You've been hacked. The hackers have gained access to countless client records, including credit card and other financial data. The damage to business reputation and the expense of dealing with the breach could be crippling. How best can businesses insure themselves against this and other cyber-risks, and what are the legal issues involved?

Types of Cyber-Risks

Cyber-risks faced by businesses today take many different forms. In addition to hardware and/or software failure, or the loss of portable devices such as laptops or smart phones, companies face increasingly sophisticated attacks from hackers. Any of these events could disable access to company websites, corrupt databases, or result in the theft of large volumes of confidential customer information. Hackers may attempt to commit fraud with the stolen data or extort companies anxious to restore access to electronic resources. Hacking attempts, even if only partially successful, could result in the installation of viruses or Trojan horses that cause further damage to company systems or the theft of more data. Company employees or agents may inadvertently or purposefully defame competitors on company websites, blogs, or social networking sites like Facebook and Twitter. The list goes on.

Despite these risks, many businesses do not yet possess coverage for electronic and cyber-risks. Only 31 per cent of respondents in a 2013 study by the Ponemon Institute indicated that their organizations had some form of cyber-insurance coverage, though 57 per cent of those without coverage indicated that their organization had some plan to purchase coverage in the future.

Insurance Issues: A Look Back in Time

Significant changes with respect to insurance available to cover cyber-risks took place in the late 1990s and early 2000s, as the volume of electronic data collected and stored by businesses worldwide increased dramatically and the number and extent of cyber-losses began to grow. Questions arose as to whether cyber-related loses ought to fall within the scope of traditional Commercial General Liability ("CGL") policies.

In particular, U.S. courts began to consider the issue of whether electronic data fell within the definition of tangible property in the context of commercial liability insurance. While some state courts in this early period found that electronic data was tangible property for the purposes of insurance coverage, other courts were unwilling to extend coverage on this basis. In 2001, in *State Auto Property and Casualty Insurance Company v. Midwest Computers & More*,[1] in the course of deciding whether an insurer was required to defend and indemnify a policyholder where the policyholder

faced a suit over negligently performed computer service work, which resulted in the loss of its customer's data, the court held that "computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property".

In conformance with this trend in jurisprudence, in 2001, the standard CGL form published by the Insurance Standards Office in the United States was revised to exclude "electronic data" from the definition of "property damage". In Canada, a similar exclusion was introduced in the Insurance Bureau of Canada's standard CGL form starting in 2005.

The resulting gap in coverage gave rise to an obvious need for a new insurance product, designed to address emerging cyber-risks.

What Insurance Coverage Is Available to Cover Cyber-Risks?

Many insurers now offer comprehensive cyber-risk policies, providing both first- and third-party coverages. Perils covered under cyber-policies include expenses incurred as a direct result of the breach, such as legal, investigation, and public relations expenses, as well as indirect costs such as business interruption and loss of goodwill. Third-party coverages available include losses suffered by customers as a result of the theft and use of their personal financial data. Insurers also offer value-added services, such as network security testing, designed to help companies avoid and mitigate the effects of a data breach, and crisis management services.

Legal Issues

Notwithstanding the electronic data exclusion discussed above, litigation continues with respect to whether and to what extent cyber-losses may be covered under CGL policies.

For example, in *Zurich American Insurance Company v. Sony Corporation of America et al.*,[2] Sony sought coverage under a CGL policy in connection with an on-line breach leading to theft of customer personal information. Rather than seeking to recover under the Bodily Injury and Property Damage coverages, Sony instead argued that the breach of its systems by hackers, which resulted in the information of millions of its users being compromised, constituted a disclosure of information so to trigger coverage under the Personal and Advertising Injury Liability coverages in the CGL policy, as publication of material "in any manner". Sony's CGL policy included coverage for "oral or written publication, in any manner, of material that violates a person's right of privacy".

Sony's insurers argued that the policy did not afford coverage because (1) "publication" required an intentional act on the part of the insured, and (2) "in any manner" referred to the medium of publication rather than the source of publication. The court agreed with the insurers and held that Sony was not entitled to coverage; though the hacking incident did result in a "publication" of the user data, the general liability policy required that publication come as a result of Sony's intentional act. The court ruled on a motion for summary judgment that Sony was not covered under its CGL policy for the breach of Sony's PlayStation Network and other online systems. As a result, Sony's insurers did not owe a duty to defend in class action lawsuits arising out of the breach.

Though the case is likely to be appealed, the decision may well be indicative that future attempts may be made to find coverage for cyber-related losses under CGL policies.

Conclusion

Cyber-risk insurance products and the legal issues surrounding them are in an emerging and developmental phase. However, as the number and extent of cyber-losses is steadily increasing, and regulatory disclosure and reporting obligations are evolving, it is critically important that businesses take steps to insure and protect themselves against cyber-losses.

---

1 147 F. Supp. (2d) 1113 (WD Okla 2001).

2 Index No. 651982/2011 (NY Sup Ct, Feb. 21 2014).

Major Cyber-Breaches Reveal Potential Cyber Insurance Coverage Gaps

Joseph Verdesca
Partner
Corporate Department
Weil, Gotshal & Manges LLP

Paul Ferrillo
Counsel
Litigation Department
Weil, Gotshal & Manges LLP

Gabriel Gershowitz
Associate
Corporate Department and Insurance Practice
Weil, Gotshal & Manges LLP

News reports abound of cyber-attacks and cyber-security breaches. The damage resulting from such breaches can include loss or disclosure of confidential customer and employee data and mission-critical intellectual property, destruction of business property, reputational injury, regulatory actions, fines and investigations, class action litigation, and loss of business, enterprise value, and market capitalization.

A comprehensive response to this growing threat must include a review of the degree to which the risks of cyber-attack or breach are covered by insurance.[1] Particular attention should be paid to the following three contexts in which we have seen significant gaps in coverage of late:

- Cyber-Exclusions in Directors' & Officers' Liability Insurance
- War and Terrorism Exclusions in Cyber-Insurance
- Coverage of Physical Loss Resulting from Cyber-Attacks

Cyber-Exclusions in Directors' and Officers' Liability (D&O) Insurance

A cyber-incident involving a company may have significant implications for its directors and officers. This is particularly true where the company has publicly traded equity or debt securities, as such a cyber-incident can adversely affect the holders of the company's securities, or where the company occupies a prominent or sensitive position from a governmental or regulatory perspective. For example, the degree to which a company's directors and management have complied with their fiduciary duties, taken appropriate precautions against cyber-related risks, and adequately disclosed such risks and related precautions may well be called into question in shareholder or creditor litigation or during a regulatory inquiry or investigation.

In seeking to mitigate the impact of cyber-related claims against a company's directors and officers (for example, where the company's share price drops following the disclosure of a cyber-related incident, and shareholder derivative claims are brought), one might first turn to the company's D&O insurance policy. However, we have seen several instances of existing policies (and proposed renewals of D&O insurance policies) containing exclusions of coverage for cyber-related matters, including for "cyber security breach" and "data breach". The existence of such exclusions could[2] eliminate D&O insurance coverage for a particular cyber-incident, thus leaving the company with only its cyber-insurance coverage limits (if and to the extent it has them) to address the costs and liabilities suffered by the company directly, as well as the costs and liabilities incurred in the defense and settlement of any related shareholder complaint.

We encourage you to review carefully with your insurance and legal advisors the terms of your existing D&O insurance policy to ascertain whether the foregoing exclusion applies to your coverage.

War and Terrorism Exclusions in Cyber-Insurance

Insurance policies routinely exclude coverage for losses resulting from acts of war or terrorism. Recent cyber-related incidents, particularly those involving or allegedly involving governmental or quasi-governmental actors or terrorist groups, raise questions of whether such incidents would fall within the scope of such exclusions. The globe-spanning nature and armchair execution of cyber-threats, together with reports that certain cyber-attacks have been conducted by or on behalf of governmental actors, distinguish the risks covered by cyber-insurance from risks covered by other forms of insurance. A company purchasing cyber-insurance expects

coverage in the event of a cyber-incident, irrespective of the identity of the perpetrator (including persons acting for or on behalf of other countries) and the reason for the cyber-incident (including perpetrating acts of "cyber terror").

Cyber-risks and cyber-insurance are still evolving. In evaluating or purchasing cyber-coverage, special attention must be given to exclusions for "terrorism", "war",[3] "government action", and other terms having similar import. The presence of these types of precise formulations of such exclusions could eliminate coverage for a cyber-incident merely by virtue of who perpetrated the act, for what reason the act was perpetrated, and/or how the act or a person, group, or country allegedly involved in the act is characterized by a politician, governmental agency, or regulator. We urge you to keep this in mind and discuss with your insurance and legal advisors when assessing protection afforded by existing cyber-insurance coverage or in negotiating new or renewal coverage.[4]

Coverage of Physical Loss Resulting from Cyber-Attacks

Exclusions for cyber-related matters are found in many commercial general liability ("CGL") insurance policies today, and such exclusions are being routinely included in CGL insurance renewals. Depending upon the formulation of such exclusions, the remainder of the policy language and the ongoing development of case law in this arena, coverage for losses from bodily injury, physical damage, pollution, or similar matters may not be available if arising from a cyber-related incident. Similarly, typical cyber-insurance policies often expressly exclude coverage for such losses.[5] Examples of such losses could include damage to persons or property (including pollution) resulting from a cyber-based attack on oil, gas, electrical, and other infrastructure control systems,[6] personal injury resulting from a cyber-based shutdown of healthcare or emergency responder systems, and destruction of computer hardware (including servers) and other assets through a cyber-based attack.

As a result, unless its insurance program has been carefully constructed and modified as necessary as developments in the cyber arena emerge, a company may find itself without any insurance coverage for potentially material liability arising from cyber-related incidents, merely by virtue of the type of damage caused by such incident. One recent commentator noted, "[a]lthough the upstream, midstream and downstream energy markets are well-insured, many of these insurance policies contain exclusions for damages arising out of cyber attacks, malevolent viruses or malware. The end result is an ocean of insurance coverage, but barely a drop that would cover catastrophic damages arising from a cyber attack".[7]

In this age of cyber-crime and cyber-terrorism (and continued evolution of cyber-insurance and cyber-related exceptions from non-cyber-insurance policies), insureds would be well advised to review with their insurance and legal advisors their property and casualty and cyber-insurance policies to see whether and how they would respond to physical loss in the face of any of a number of potential cyber-related incidents.

[*Editor's note*: A version of this article was originally published as a client alert by Weil, Gotshal & Manges LLP on January 28, 2015. It is reprinted with permission of the authors.]

---

1 For a discussion of how insurance may be useful in mitigating cyber-related risk, *please see* Paul Ferrillo, "Cyber Security, Cyber Governance, and Cyber Insurance" (November 13, 2014) <http://blogs.law.harvard.edu/corpgov/2014/11/13/cyber-security-cyber-governance-and-cyber-insurance/>.

2 A careful, case-by-case review of the precise policy wording is necessary to determine coverage availability.

3 For example, an "Acts of War" exclusion may provide that "This policy shall not cover the defense of any matter, or any loss, injury, damage, costs, expenses or other amounts […] arising out of, based upon or attributable to any strike, lockout, disturbance or similar labor action, war, invasion, military action (whether war is declared or not), political disturbance, civil commotion, riot, martial law civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events; whether or not any other cause or event contributed concurrently or in any sequence to any resulting loss, injury, damage, costs, expenses or other amounts".

4 We note that express coverage of "cyber terrorism" is available from some insurers but caution that the precise formulation of such coverage and how such wording

interacts with the remainder of the policy requires careful review in order to avoid potential coverage surprises.

[5] Certain cyber-insurance policies are designed to provide cover for such losses in the case of a cyber-related incident excess of any coverage provided by a CGL policy. See, *e.g.*, "Cyber Edge PC" available at <http://www.aig.com/cyberedge-pc_3171_595334.html>.

[6] Admiral Rogers, head of the United States Cyber Command, has been quoted as saying "[w]e have seen instances where we're observing intrusions into industrial control systems [….] What we think we are seeing is reconnaissance by many of those actors in an attempt to ensure they understand our systems, so that they can then, if they choose, exploit the vulnerability within those control systems [….] There shouldn't be any doubt in our minds that there are nation states and groups out there that have the capability to […] shut down or stall our ability to operate our basic infrastructure, whether it is generating power across this nation, or moving water and fuel". *See* Peter Behr, "Cyberattackers Have Penetrated U.S. Infrastructure Systems—NSA Chief", E&E Publishing LLC, <http://www.eenews.net/stories/1060009391>.

[7] *See* "Cyberattack Insurance Challenges Confront Energy Sector," *Law 360*, <http://www.law360.com/articles/591022/cyberattack-insurance-challenges-confront-energy-sector>.

INVITATION TO OUR READERS

Have you written an article that you think would be appropriate for *Corporate Governance Report*?

Do you have any ideas or suggestions for topics you would like to see featured in future issues of *Corporate Governance Report*?

If any of the above applies to you, please feel free to submit your articles, ideas, and suggestions to <cgr@lexisnexis.ca>.

We look forward to hearing from you.