GLOBAL BANKING &
Finance review
Issue 7

Desjardins Private Wealth Management

An inside look at Desjardins Private Wealth Management (DPWM), from its leader's point of view: Sylvain Thériault, Vice-President and General Director.

The Shifting Tides of Asian Trade

Dominic Broom, member of the International Chamber of Commerce (ICC) Banking Commission's Executive Committee, and Global Head of Trade Business Development at BNY Mellon

Investing in Angola

Interview with David Carvahlo, Head of Private Equity, Quantum Global Group

9 772396 717008 07

UK £50.00
USA $62.00
EUR €55.5
CAN $82.00
AED 227.50

Middle East | Americas | Europe | Africa | Asia

www.globalbankingandfinance.com

Not If, But When:

Five Questions You Should Ask When Seeking Cyber Insurance

"We are in a world now where, despite your best efforts, you must prepare and assume that you[r] [security systems] will be penetrated. It is not about if . . . , but when."
—Admiral Mike Rogers, Director, National Security Agency

Financial service businesses are living the "not if, but when" reality described by Admiral Rogers. Over 66% report having experienced a cyber-attack this past year. In fact, the risk has become so prominent that the New York State Assembly is considering legislation that would require those licensed under the state's Banking, Insurance or Financial Services law to implement, by February 2018, a particularized cybersecurity program "designed to protect the confidentiality, integrity and availability" of electronic information systems.

As financial institutions adjust to enhanced scrutiny from hackers and regulators alike, many have turned to cyber and crime insurance policies to address their risks. However, selecting the right coverage among relatively new and varied forms can be nearly as challenging as protecting against cyber risks in the first place. We have identified five questions to make selecting the right product a little easier and, once selected, coverage less uncertain.

1. What are your risks, including up-stream and down-stream risks?

A business cannot select the proper coverage until it understands its risks. But many in the financial sector do not know enough about the nature and breadth of their cyber exposure. According to one report, over 33% of financial service businesses do not know whether they have been attacked in the past year, and over 22% do not know whether attacks are increasing or decreasing as compared to previous years.

This lack of understanding could jeopardize coverage for later claims, since insurance applications require businesses to answer questions about existing and past cyber-related exposure, precautions and loss history. Courts have held that even unintentional misrepresentations or omissions of material information are sufficient to void the insurance contract.

Such lack of understanding could also be used to trigger exclusions. For example, insurers may argue that ignorance of risk and failure to address risk is tantamount to a circumstance that the insured should have reasonably foreseen would cause an event that could be the basis of a later claim – a common policy exclusion.

One way to improve understanding of business cyber exposure is to include critical personnel in the application and coverage selection process. Risk managers – who have the difficult task of being jacks of all trades for their employer – should consult with personnel in every essential department (e.g., human resources, information technology, and marketing) to obtain the benefit of those employees' deep knowledge of critical data, security measures, and hazards. This way, risk managers will have current, specific information about the business with which to seek and negotiate coverage.

Risk managers should also cautiously review service contracts, since exposure may be buried in the boilerplate language of common industry agreements. Once exposure is identified, do not assume the risk is necessarily covered because it is cyber-related, or assume that the risk would be covered because the insurer understands the nature of your business. As an example, the restaurant chain P.F. Chang's ran into that problem with its cyber insurance policy, which P.F. Chang's claim it purchased to cover payment card industry data security standard (PCI-DSS) assessments, among other risks. But P.F. Chang's could not prove its expectation in court, resulting in a denial of coverage (among other reasons). This case is a good reminder to demand specific policy language for specific risk, especially for passed-through exposures.

Risk managers should also consider how their businesses will be affected if third-party service providers are compromised. Such inquiry has become increasingly important as hackers discover new ways to disrupt business practices, as Netflix discovered in October 2016 when hackers used internet-connected cameras, baby monitors and home routers to effect a "denial of service" attack on the video streaming giant's cloud-based internet performance manager, Dyn. Similar attacks have affected those in the financial sector – including European, Russian and Asian banks – with increasing regularity. These types of attacks can be very costly for businesses: studies estimate from $22,000 for each minute a site is down to $40,000 an hour (with 15% reporting costs exceeding $100,000 per hour). These costs add up quickly, since most attacks continue more than six hours. Given potential extraordinary loss, businesses to analyze how they may be affected by attacks against those who they depend to perform critical business services. For example, how much business data or personally identifiable information (PII) is stored with a cloud provider? Will the proposed cyber coverage mitigate the business effects if that information is compromised?

2. What are the gaps in coverage between policies, or within cyber forms?

Many insurers have patched together their cyber policies over a number of years in order to respond to new threats. But the hodgepodge result sometimes causes critical gaps in coverage.

Such gaps, if not resolved, may require other types of policies to pick up the slack, and vice versa. For example, crime policies are considered a necessary partner to cyber policies, because the former typically covers attacks involving stolen money as opposed to stolen data. But even crime policies may prove to be a deficient partner, as Apache Corporation recently found. The business wired $7 million in invoice payments to a fraudulent bank account that criminals claimed belonged to one of Apache's vendors. The scheme started with a phone call, confirmed by a fraudulent e-mail on vendor letterhead. The fake letter also included a false telephone number, which Apache personnel used to confirm the change request. The Fifth Circuit Court of Appeals held that loss was not a "direct result" of the e-mail, as required by the policy's "computer fraud" coverage, but rather caused by human error in failure to investigate the phony directions. The email, according to the court, was "merely incidental" to the money-transfer scheme. A well-crafted endorsement to the cyber or crime policy, or standalone comprehensive policy (both available through many insurers) may have avoided this outcome. Accordingly, businesses should ensure that seemingly broad cyber coverage is not unnecessarily truncated due to lack of imagination or failure to recognize the holes in the businesses' insurance packages.

Policyholders also may be able to fill gaps in coverage through existing forms. For example, last year, the Eighth Circuit Court of Appeals held that the State Bank of Bellingham was covered under a financial institution bond for losses arising from the fraudulent transfer of $485,000. An employee negligently facilitated the loss by leaving tokens in a bank computer – the physical part of the bank's multistep security process. With the tokens in place, hackers were able to access and transfer funds to a foreign bank account. The bank's insurer denied coverage under the bond based, in part, on an exclusion of employee-caused losses. The Court held that even if the employee's negligence had been essential to the loss, it was not the "overriding cause," as was the third-party criminal conduct. Thus, financial institutions should remember the possibility for cyber-related losses to be covered under policies that are not specific to cyberattacks or crime, though businesses should certainly not depend on these forms alone.

3. What triggers coverage?

Policies vary considerably with respect to what triggers coverage. Some policies trigger upon breach of a security system; others require an affirmative failure by the insured. The challenge of the latter category is that even the best defense may be insufficient to prevent a constantly improving and motivated cyber actor. Thus, there may be no real "failure" by the insured or of the insured's security system that would trigger coverage.

Also, if it is the breach – as opposed to insured's failure – that triggers coverage, the next question is whether the policy kicks in on discovery or occurrence of the breach. The trigger can be significant, since cyber breaches may go undiscovered for a long period of time. Nevertheless, a discovery-based trigger may make sense for some types of risks or may be non-negotiable with the insurer. Policyholders should note what triggers coverage and assess whether the trigger makes sense with respect to the particular insured risk.

Policies also differ in coverage for costs associated with alleged or suspected breaches. Such coverage can be helpful when the insured receives notice from a third-party (perhaps a vendor, or a government agency like the FBI) that an investigation discovered confidential business or personal information that appears to have come from the insured's network. In such circumstances, it is incumbent to investigate the alleged or suspected breach, but such investigations can be just as costly as investigations of confirmed breaches. Proper coverage will assist in the necessary forensic work which can ultimately help a business to address a security breach and patch security vulnerabilities.

4. Does the policy cover current cyber risks?

Cyber threats, which are ever-evolving, can outpace the black-and-white of policy language. For example, policies commonly cover ransoms paid in response to threats to release stolen data or to prevent system access, but not ransoms paid in response to successful attacks (for example, to return stolen data or to restore system access). The gap is explained by the fact that ransomware of the latter kind was not a prominent risk when the policy language was drafted. Failure to cover present threats could be disastrous for financial industry policyholders, against whom ransomware attacks have more than doubled in the past year. Studies report that more than 32% of financial firms say they have lost anywhere from $100,000 to $500,000 to ransom attacks, not including downtime losses.

Another common place where policies lag behind in is the definition of terms that describe the insured's technology or source of risk, like "Internet," "computer," "network," or "system." Those definitions should be broad enough to include common hardware (like laptops and cellphones), and electronic and cloud technologies. Some definitions of system may not capture wireless networks; others may not explicitly include cloud computing. A company's IT employees can be particularly helpful in reviewing definitions to make sure the descriptions are broad enough to cover the technology it directly and indirectly uses.

5. Do you have the right advocates?

Business leadership and managers – who understand the insured's daily activities – can be great advocates when selecting coverage. Likewise, it is essential to have a qualified broker who knows the market, the insurers and the available policies. But each of these parties may not be aware of the possible insufficiency of a

policy. Knowledge of the business is not equivalent to knowledge of litigation or coverage risks. Also, brokers may be so focused on the cost or the deal that the advisory role falls to the side.

Experienced coverage counsel can fill the advocacy void by analyzing policy language through the lens of potential litigation, advising the insured about coverage issues based on identified risks, and partnering with brokers to negotiate endorsements favorable to the insured's needs. Proper advocacy will, ideally, help insureds obtain coverage most responsive to the business needs and cyber threats of today's virtual landscape.

Since cyber losses are now a question of "when," not "if," policyholders should seek cyber coverage that responds with a similar level of certainty. While there are no guarantees due to the fickleness of language and the courts, businesses can get very close to coverage that responds to their risks and needs by tackling the five questions posed in this article.

Walter J. Andrews
LLP
Hunton & Williams

Walter Andrews is head of Hunton & Williams LLP's insurance litigation and recovery practice. Based in Miami and Washington, D.C., his practice focuses on complex insurance litigation, counseling and reinsurance arbitrations and expert witness testimony.

Jennifer E. White
LLP
Hunton & Williams

Jennifer White is an associate in the firm's Washington office. Her practice focuses on insurance coverage counseling and litigation, with an emphasis on cyber insurance matters.