CANADIAN UNDERWRITER.ca

Canada's Insurance and Risk Magazine

TABLE OF CONTENTS Mar 2015 - 0 comments

Moving Target

Cyber risk is evolving. Despite recent high-profile attacks meant to disparage, disrupt and produce fear, though, a true picture of cyber risk involves far more than intended events. Risk managers must, first, accept the breathtaking breadth of the risk and, second, be ready to absorb information that will help them to set an accurate sight on what is (and will continue to be) a moving target.

By: Angela Stelmakowich, Editor
2015-03-01

Hardly a week goes by without news of a new cyber risk, some breach that has prompted concern over both immediate response and nagging dread over what might be the ultimate impact. While these near-constant reminders serve to keep the issue top of mind - and rightly so - is this enhanced awareness translating into effective protection and response? Do organizations have a full enough view of the risk to underwrite and cover it?

The breadth and potential ramifications of cyber risk can be tough for anyone to firmly grasp in light of its rapid and slippery transformation. Ask those in Canada's property and casualty insurance space if cyber risk is established, emerging or evolving, and replies may vary on the first points, but likely not on the last.

"Cyber risk is different than most risks in the sense that it will never stop emerging and evolving," suggests Nate Spurrier, director of business development at IDT911. "Like technology itself, this will continue to evolve, as will our response and adaptation to this risk," says Sean Duggan, vice president and practice leader for Cleantech, Technology, Life Sciences, at HUB International HKMB.

"Cyber risks have been around for quite some time and exist in a dynamic environment of ever-changing technology, evolving threats and a legal environment that is in a constant state of flux," says Jeremiah Tonn, senior underwriter in Zurich Canada's Management Solutions Group.

And while more mundane breaches and security lapses may not be quite as sexy as attacks, they are equally important, warranting attention and care.

The leading cause of data breach "is from the loss of a laptop that is not encrypted, followed by hackers and then rogue (disgruntled) employees," reports Carol Kreiling, vice president at Swiss Re.

"Breaches can also occur from the inside - employees taking or sharing confidential information, accessing customer and client files when not authorized to do so, loading information onto laptops or USBs which are lost or stolen, confidential files being tossed into the garbage rather than being properly shredded and, of course, the photocopier where the data is not cleaned off the hard drive. The list goes on," says Betty Hornick, national commercial senior manager and team leader, Product Development & Functional Support, at Aviva Canada.

"As an organization's dependence on technology increases, so does its exposure to this issue. It's not solely financial loss that is a concern, but physical damage or bodily injury," says Jacqueline Detablan, vice president, Personal Lines, for AIG Canada.

CHANGE IN APPROACH

Kreiling suggests that the risk management approach may change depending on whether a risk is established, emerging or evolving. "If a risk is emerging, there may not be as much information to evaluate the risk as a risk manager would like," she points out.

"If it is emerging, then it is monitored for significance of risk and potential impact; if it is established, it is monitored and managed with all the company's other risks; if it is established and evolving, it requires constant monitoring and upgrading of the risk management approach, techniques, tools and policies and procedures to monitor and mitigate effectively," explains Ed Berko, senior vice president and chief risk officer for Economical Insurance.

The view of Tony Nicholls, chief architect at Insurance Technology Solutions Inc? "Everybody should be on guard all of the time, keeping their software patched and implementing best practices."

Duggan says "there's been a paradigm shift in the risk management approach to include intangible (digital) risk as part of the enterprise risk management plan. In many cases, the CIO (chief information officer) now has a seat at the risk management table and is actively involved in designing the business continuity plan."

In addition, many corporations are now bringing an IT or cyber expert into the C-suite, says Kreiling, but acknowledges that "designating a CRO (chief risk officer) and apportioning the necessary resources towards protecting a corporation against a cyber attack might be two different issues."

Being on the same page is key. "'Getting' the risk, and then having the preventative measures and systems in place and designing for that anticipated event, are different things," says Kadey B.J. Schultz, a partner at Hughes Amys LLP.

Notes Tonn, "It is very clear businesses that want to protect themselves from cyber risks must adopt a mindset of resilience, with steps in place to deal with cyber risks at all stages. Resilience means identifying the risks, establishing protective barriers, segmenting sensitive data, creating rapid detection mechanisms, and responding effectively - all with the goal of achieving a successful recovery."

COMMON TARGETS

In a cyber attack, Kreiling says there are generally three types of information that are most commonly stolen:

• Personally identifiable information (PII) - information that could be used on its own to identify, contact or locate a person, including name, date of birth or mother's maiden name;

• Protected health information (PHI) - information that concerns a person's physical or mental health; and

• Finally identifiable information (FII) - credit/debit card and banking information.

"There is now concern over the impact of cyber on systemic risk, and with cyber risk transcending to the Internet of Things as well as digital attacks leading to tangible damage in the physical world. This could be a game-changer," Duggan contends.

"Although we constantly see headlines about breaches and how most CEOs recognize the threat of being hacked is a significant one, very little if anything is being done about addressing the issue," argues Hornick.

A recent A.M. Best survey of property and casualty, life and health insurance firms found that 53% of respondents reported they do not buy any kind of cyber coverage, while 30% noted they purchased between US$1 million and US$5 million in limits.

In light of the changes now under way, Tonn advises customers to bear in mind a number of things:

• as more businesses become global, data centres may be located in different parts of the world;

• with expanding use of "the cloud" for IT operations and data storage, a presence may be established in foreign countries even when business is only conducted domestically;

• the reliability of foreign data centres can be challenging depending on the condition of the local infrastructure, local organized crime, and the economic and political stability of the region;

• cyber failures (unplanned IT and telecommunication outages) represent more than 50% of supply chain interruptions; and

• losses due to supply chain business interruption are significant and higher than businesses anticipate.

"Currently, cyber threats are focused on high-value targets: large firms, sensitive government information, and the computing 'cloud' where multiple companies can be attacked through a single point of entry," Berko notes. "Cyber security risk is not a matter of if; it is a matter of when and how bad."

Hornick notes that businesses and organizations must take preventive steps to protect valuable assets, such as business practices, personal data of employees and intellectual property.

HIGH-PROFILE VALUE

There are many ways to incorporate protections to guard against cyber risks - whatever form they take - but sources emphasize the need to be open to all fixes. "When we just focus on beefing up computer systems and network security protection, we're missing out, being blindsided to, a whole other set of risk factors that face an organization," argues Katie Andruchow, national cyber and privacy expert for Aon Risk Solutions.

"There's a whole host of risk management tactics that can go along with mitigating privacy risk that are separate from the IT department's responsibility in managing that network security breach aspect," Andruchow emphasizes.

"The internal threat is as large, if not larger, than the external threats," suggests Rick Roberts, president of RIMS, the risk management society.

Roberts says organizations are now very good at setting up firewalls and monitoring penetrations, but adds "it's very hard to control it internally when you need to give your people access to all the information they need to do their jobs. How do you protect it?"

Errors and omissions "are accounting for an increasingly large number of security breaches on an annual basis. That really comes down to the need for security awareness, effective policy, acceptable usage, etc., to try and combat those threats," says Kevvie Fowler, partner, Advisory Services, at KPMG Canada.

"Errors and omissions, if you look at it, it's growing in terms of the amount of cases. They're currently being reported in the industry as an area that a lot of organizations are seriously looking at. It is preventable," Fowler reports.

Even things as simple as use of thumb drives demand care, Roberts says. Only company-sponsored drives should be used to ensure there is some element of protection, he emphasizes. "Once you put a thumb drive into a company computer, who knows what can happen?"

There is also the challenge presented by people wanting to use personal devices in conjunction with company systems. "If there's no protections, you're really just leaving your company's computer systems wide open for some kind of Trojan horse to come in and infiltrate the system," Roberts cautions.

Questions need to be answered, says. Schultz. "What kind of internal systems have been articulated, implemented and are adhered to in a consistent way by membership of any company?" she asks.

"What is your security policy for remote access? For using laptops? For your personal iPhone or BlackBerry? What kind of security is implemented and education provided to your staff around using that equipment?" she continues.

"We need to be willing to engage in the mundane to really nail down what the risks are to protect ourselves from (cyber) risks going forward," she contends.

The general consensus seems to be that companies and organizations are not well-equipped - or, at least, not equipped well enough - at present to deal with all cyber-related risks.

Add to that the challenge of how varied preparedness is among industries, or even within the same industry.

"Sometimes it is a question of resources, priorities, sophistication of the infrastructure; sometimes it is a lack of awareness of how exposed the organization actually is," Detablan explains. "It is unlikely that a firm can protect itself completely from all cyber exposure. Even with the most secure network, there are additional exposures such as employees acting outside the scope of their mandates, which are hard to prevent."

As such, care must be taken to consider interconnectedness. Tonn advises the following be addressed when reviewing cyber exposure and internal controls:

• move beyond the IT department and embark on an enterprise risk management approach;

• map critical data by knowing what is most important, where it is, how it is protected, who touches it and where it travels;

• ensure all employees engage in ongoing cyber awareness training (a security awareness and training program is the lowest cost security measure with arguably the highest return on investment);

• formulate an incident response plan with internal and external teams and test it regularly so that everyone knows what to do when an incident occurs;

• extend beyond the four walls of the company by engaging with the organization's insurance carrier or broker's risk management team in an ongoing review of all business partner relationships, including how those vendors/partners approach their own exposures and controls, and how the vendor's supplier's approach fits into the company's overall resilience plan.

Berko further suggests "most companies are not looking broadly enough when assessing the risk and potential impact of a cyber security breach," including, for example, suppliers and business partners.

Companies "need to consider current and former outsourced service providers, consultants, contractors, key partners, employees, in addition to internal and external threats. They also need to consider the communication channels used by the company," he recommends.

"It's the small, very minimally secured entities that are then going to create more and more risk for their business partners," Schultz suggests.

Detablan's advice? "We think awareness around organizations as being only as strong as their weakest link is becoming clear, and many risk managers are trying to tackle this issue."

MUCH-NEEDED SUPPORT

Although there have been improvements, most sources suggest a lot more needs to be done with regard to companies supporting their risk managers so that they, in turn, can help to properly inform boards and C-suites of the risk.

"The issue is that business doesn't like to spend money on IT; just look at the amount of legacy solutions in the average business!" Nicholls argues.

Still, there are positives. "This is certainly on the C-suite radar screen, given the potential correlation between data breach events and downstream D&O (directors and officers) claims claiming breach of fiduciary duty for inadequate network security or levels of cyber insurance coverage," Duggan reports.

"Cyber risk is not a traditional risk management area of focus, and it requires a cross-functional working group of senior members of an organization to be effective," says Detablan. "This cross-functional group should include business senior management, as well as representatives from operations, IT, finance, legal and human resources," she adds.

"It is critical for business to build a culture of awareness at all levels from the board room to the mail room," agrees Tonn, adding that C-suites are seeing the importance of increased communication and bringing all key stakeholders to the table, including risk management, general counsel and supply chain teams.

Ivan Au, underwriter specialist-team leader, Technology Underwriting, at The Sovereign General Insurance Company, says there is often a cost-versus-benefit discussion that comes into play. "In recent years, there has been an increased use of network security consulting firms that audit and provide recommendations. However, these recommendations are not always followed through."

Fowler emphasizes the need for risk managers to provide an accurate message to company boards. "A lot of times, these risk managers try and water down the messaging. In some cases, they don't articulate the message in its entirety because they fear that it won't be absorbed correctly by the board," he reports.

"But it's very important that an accurate picture get sent to the board because, at the end of the day, the risk and liability lies with the board," he says.

Understanding the risk helps boards to be engaged, Fowler says."An engaged board will help put the organization in a defensible position," he maintains.

"Putting yourself in a defensible position is ensuring you're doing the right thing, but you can also demonstrate that you were doing the right thing when that breach did occur. And that can save the organization lawsuits and financial penalties associated with that," he adds.

Andruchow suggests that teaming up with suitable partners is a great way to speed up the in-house knowledge base of an organization.

"A way that organizations can gain expertise and the assistance that they need when there's so much flux and vulnerability in this space is partnering with third-party service providers who specialize in the risk management of certain areas," she advises. "With a strong contractual agreement with those service providers and really integrating them into your company's incident response plans, business continuity plans and your management process, I think there's a way you can outsource that expertise, but still keep that knowledge within your organization."

PINPOINTING COST

High-profile cyber events serve the function of creating "an enhanced awareness of cyber risk and the responses to data breach events, including claims precedents from losses," Duggan suggests.

"Once a company or organization has a basic awareness of the risk, then the risk manager can peel back the layers of the cyber risk 'onion' and begin to understand the potential losses and damages," notes Kreiling.

As it stands, Hornick does not believe organizations have a good understanding of the true implications of the financial cost in the event of a breach. "The financial impact could be potentially huge," she says, depending the size of the corporation, the extent of the breach and where the corporation does business.

"A lot of organizations have actually made the news in relation to security breaches not relating to a failure within their organization, but within one of their third parties," Fowler says, adding that third-party risk is critically important from a cyber security standpoint.

"Any organization, when they look at cyber security, number one, they identify the assets that they have, then they identify the kind of safeguards they want to put in place to ensure they protect those assets," he explains.

"A lot of times, they stop there and they don't look at these controls that the third party has to ensure the same of level of protection is provided by that third party that they would provide internally within their organization," he says.

"Many companies are focused on the risk to customer data and fail to appreciate the full impact to their own businesses, both direct first-party costs, as well as potential liability to third parties," Duggan says. "Whether it's brand damage and reputational harm, business interruption, intellectual property/corporate confidential or employee information, all companies have a degree of exposure," he emphasizes.

"Some aspects of cyber risks are more quantifiable than others. Hard costs such as regulatory expenses/privacy notification costs, credit monitoring and business interruption are easier to estimate using a data breach calculator, but how do you put a price on downstream risks such as brand and reputational damage, drop in share price, compromised intellectual property or lost customers?"

Most of today's loss dollars arise from first-party privacy breach costs, including notification costs, breach coaches, credit monitoring costs and call centre costs, Tonn reports, but notes there are others, including business interruption (income) loss, liability lawsuits, administrative actions from regulatory agencies, and derivative shareholder suits for the mismanagement of cyber risks.

But pinning down which coverage may be needed, and which risks could be excluded, continues to be challenging.

Berko notes that protecting an organization would be difficult to achieve in light of the rapidly evolving nature of cyber risk. "Mitigation of the impact is a more reasonable and achievable goal."

Andruchow reports that in the last year, Lloyd's of London has come out with a special code for cyber insurance products so it can properly manage the risk it is taking on its books.

In addition, there have also been exclusions come out in policy wordings.

"Insurance companies are realizing that there can be an interconnectedness of exposure between bodily injury, property damage and some of the different insurance policies out there," she says.

"As the technology that organizations rely upon grows and changes, insurance offerings will need to evolve as well," Detablan points out.

"When it comes to general liability and property protection, those are thought up on an annual basis or when there's some sort of event that spurs taking a look at it," such as the purchase of new equipment or merger and acquisition activity, Andruchow points out.

"But the developments in the cyber space are so frequent right now that the risk management needs to have more touch than just an annual basis, or just a quarterly basis, even," she recommends.

As it stands, Berko says that he thinks cyber risk and potential losses are not yet sufficiently understood to properly underwrite the risk. "Since the risk is established, but still evolving, it will require additional time and events to better understand the types of risks and their potential impact in cost, business interruption and reputation," he says.

"From an insurance standpoint, this is a very complex issue and there is not a lot of experience in underwriting the product," says Steve Kaukinen, president and chief executive officer of Insurance Technology Solutions. "However, an insurance product with reasonable limits and, preferably, tied to some kind of risk management/technology assessment would give underwriters more knowledge about the risk and potential losses. For sure there is a real opportunity for these products," Kaukinen adds.

"Currently, as a main street insurer, the products being offered by most carriers today deal with measurable exposures. Limits provided are usually low and if higher limits are required, there is a charge for that increase," Hornick says.

"Do we know if the premiums being charged are adequate? No, not yet. We do not have enough experience or data. This will evolve with time and as the portfolio of this business grows," she says.

Some sources suggest that cyber risk should be seen as an opportunity with regard to product development.

Earlier this year, Willis Group Holdings plc announced its reinsurance division released a modelling tool intended to let insurance carriers quantify the exposure of their portfolio to data breaches.

"Our model help provide greater objectivity and will allow insurers to underwrite this risk with more confidence and to, therefore, write more and/or higher limits," says Mark Synott, executive vice president of Willis Re.

At Marsh, it launched a catastrophic cyber policy for large companies that offers limits of more than $300 million in coverage above a $100 million self-insured retention.

Au, however, sees issues forming. "The problem is a lot of insurers are jumping on the bandwagon without a good understanding of the risk/reward, and it puts downward pressure on pricing and gives that impression to both insureds and brokers that it is often a 'throw in' cover or an enhancement," he argues.

To his mind, the right approach is two-fold: a breach endorsement that provides basic cyber coverage for existing business, and a full-fledged standalone policy that caters to accounts that have real-world risk.

"The key with cyber risk is to layer your protection to minimize your loss. A basic first layer could be usage policies and training, a second could be things like firewalls, network intrusion detection, internal and external protection, a third could be insurance," he says.

Hornick notes that "Aviva, on most of its commercial policies, provides privacy breach expense coverage as a frill on its insurance policy." A small limit is offered and insureds can purchase higher limits if they wish, she reports.

The U.S. Insurance Market Report 2015, released by Marsh in February, notes that in the energy sector, standard policies, including property and general liability, contain exclusions for bodily injury, property damage and business interruption resulting from a cyber attack."But evolving cyber insurance can fill many of these gaps, providing direct loss and liability protection for technology risks. Emerging cyber insurance solutions designed for the energy industry are also written to specifically address this risk," the report adds.

"I am almost sure demand for cyber insurance products will eventually outpace the availability. Companies are going to have to assess any risk points and current practices to mitigate as much as possible," Kaukinen comments.

"A good portion of underwriting the risk is also explaining to the broker (and insured) what could happen and how coverage responds," Au says. "It is not like general liability or property, where there has often been a predefined rate that is credited or debited based on risk profile. There are no preset rates in cyber. It largely has to do with an underwriter's understanding of the risk, and the savviness of the broker to make the proper recommendations," he says.

"Risk managers should also appreciate the high degree of variability among cyber insurance products and policies in the marketplace to ensure that when they purchase coverage, it is addressing their core risks," Duggan advises.

"There is a lot of cyber coverage capacity out there, but it is non-commodity capacity," he points out.

"Like any peril, insurers will not be able to eliminate the threat or exposure," Hornick says. "However, they will be able to ensure that a risk manager has options to transfer the financial exposure to a third party, thus mitigating the exposure to their company," she says.

"Cyber risk mitigation needs to be built into an organization's fundamental solution architecture," Nicholls argues. "Insurance products are certainly part of the overall solution, but the business should be focused on eliminating the risk through good design first."

LOOKING FORWARD

Roberts says he believes recent events have really helped focus people on being able to develop plans around business resiliency.

"Many risk managers have the awareness and understanding of measures that must be in place to address the risk," says Kreiling. "But the worrisome aspect of cyber security is that simply putting measures in place does not eliminate the risk. For every step a risk manager takes in cyber security, the bad guys are working around the clock to stay one step ahead," she cautions.

"The understanding of cyber risks is a continuous process. Underwriters must stay current on the latest technologies to be able to assess and predict new exposures," Tonn says. "Better understanding will also come with time as more claims are experienced and, therefore, more data can be collected to help improve predictive modelling," he adds.