The Rise OF CYBER INSURANCE

A ransomware attack leaves a company with few options. One may be to resort to backup systems, if they exist. Another may be to simply pay the ransom. And then there's cyber insurance

BY PAUL MCLAUGHLIN • ILLUSTRATION BY GARY NEILL

WITHIN A PERIOD of about six weeks, from early May to late June 2017, two major cyber-attacks targeted businesses and government entities throughout the world.

The first became known as the WannaCry ransomware attack, which targeted computers running the Microsoft Windows operating system. Infected computers — estimated at some 230,000 in 150 countries — had their data encrypted, virtually paralyzing a victim's ability to function online. Among the targets was the United Kingdom's National Health Service, FedEx and Telefónica, a leading telecommunications giant in Spain. Canada was largely spared.

The attackers — allegedly a North Korean cyber-gang known as the Lazarus Group, according to *The Guardian* — demanded each victim, if they wanted to have their data unlocked, pay $300 per computer in bitcoin, a digital currency created in 2009 (that is almost impossible to trace).

A few days after the intrusion, however, a UK security researcher discovered a kill switch in the ransomware that effectively disabled WannaCry. CNBC estimated the hackers made only $50,000, a tiny amount considering the number of machines they had infiltrated.

A second high-profile onslaught occurred in late June. Known as Petya, it too crippled thousands of computers around the world, including those at Russia's largest oil producer, the pharmaceutical company Merck & Co. and Ukraine's international airport. Many of the targets were located in Ukraine, which blamed Russia for the attack. As with WannaCry, the hackers requested $300 per computer in bitcoin to release the encrypted data. Some experts, however, weren't sure raising money was the actual purpose of the attack. "A growing number of researchers believe the program was launched just to destroy data," the BBC reported.

VANESSA COITEUX
> STIKEMAN ELLIOTT LLP

> In the last two years, more and more companies are asking us about the process. They're asking about premiums and making assessments about how they're covered in their current insurance policies, what they need to cover and their risk profile.

ILLUSTRATION BY GARY NEILL

Although Canada, once again, was virtually unscathed by an international attack, it nevertheless "caught the attention of the boards of directors," says Matthew Liben, a partner in the Montréal office of Stikeman Elliott LLP. And there was no doubt that a similar response reverberated through the upper echelons of governments at all levels in the country.

Among the questions raised in the nation's C-suites was one that, until recently, had rarely been discussed: do we need cyber and ransomware insurance to help protect us if we become the next victim? "The issue is more of a *when*, not an *if*," says Ira Nishisato, a partner at Borden Ladner Gervais LLP. "Attacks on networks and systems are a daily occurrence for many organizations. They range from fairly low-level attacks to increasingly sophisticated ones that present potentially serious consequences. I think it's fair to say, clients in Canada are increasingly aware that no one is immune."

Faced with that chilling reality, an increasing number of Canadian organizations and governments are purchasing insurance to cover or mitigate losses caused by a breach. "Globally, [cyber insurance] has been increasing at double-digit rates," says Imran Ahmad, a partner at Miller Thomson LLP, who specializes in cybersecurity. "In Canada, it's been less than stellar in the recent past, but it has picked up significantly. We're having more and more clients ask about it because the coverage can be so critical to their business operations."

Canada is "still a nascent market, in my experience" for cyber insurance, says Dean Dolan, who focuses on information governance and privacy in the Toronto office of Baker & McKenzie LLP. "The vast majority of organizations do not [have it] and the insurance industry in Canada is having a tough time pricing it."

Although there is a greater awareness of the need for cyber insurance in the US — the number of attacks and the numerous class-action lawsuits resulting from breaches see to that — the market for such insurance "is not as mature as you might hope," says Brian Hengesbaugh, chair of Baker & McKenzie's Global IT/C Data Security Steering Committee in Chicago. "Over time it will become something that, as a board, you want to make sure you have, just in case. But I think it's still the early days."

The City of Mississauga has cyber and ransomware insurance, says City Solicitor Mary Ellen Bench, who is President of the International Municipal Lawyers Association. It also has a proactive approach to protecting the city's data, which includes everything from health-care information obtained from sporting permits to financial details provided by vendors and local businesses. Protecting against voter fraud is also a priority. "We've not had any significant breaches, but we've had a couple of different threats that our IT people have been quick to shut down fairly quickly."

Although she agrees this kind of insurance can be "hard to price ... and can have a big deductible, I would not classify it as extremely expensive." In fact, says Greg Eskins, National Cyber Practice Leader in the Toronto office of Marsh, the international insurance firm, pricing is becoming

easier for insurers to determine. "I would say we have enough data on a typical privacy breach [from] thousands of breaches and hundreds of millions of records being compromised in the US" As for deductibles, "retention [the industry term for deductibles] for small firms can be as low as $1,000," he says. "For large firms, it may make sense to take retention of $5 million to $10 million."

Before a company or organization begins to explore purchasing cyber insurance (an umbrella term the industry uses to encompass all aspects of this type of insurance, including ransomware), it needs to determine whether it requires this coverage and, if so, what items on the "buffet," as Eskins calls it, are available.

Vanessa Coiteux, a partner in the Montréal office of Stikeman Elliott LLP, says that there's growing interest in this form of coverage. "In the last two years, more and more companies are asking us about the process. They're asking about premiums and making assessments about how they're covered in their current insurance policies, what they need to cover and their risk profile."

The buffet of options to consider can be extensive, including coverage for business interruption, and the costs related to data loss and restoration, forensic investigations and extortion demands, as seen in ransomware attacks. What, if any, coverage to buy can be difficult to assess.

"Among the questions clients raise with us as lawyers is what sort of scope of coverage they need and what limits they need," says Nishisato. "Is it enough to have $5, $10 or $50 million in coverage? That's hard to answer because it really depends. [However], these attacks are becoming larger in scale and are compromising more and more sensitive information."

Major data breaches, such as the one experienced by Target Corp. over the 2013 holiday season, resulted in staggering losses. Although the cost has been estimated at US$300 million, of which one-third was covered by insurance, "several industry analysts forecast that Target's breach-related losses will reach $1 billion," the New York law firm Patterson Belknap Webb & Tyler LLP wrote in its blog. "After disclosure of the breach in early 2014, Target's profit was cut in half — down 46 percent over the same period the year before."

While the relatively paltry demands made by the WannaCry and Petya hackers might make some organizations wonder if ransomware insurance (which is a separate policy) is required — "If you can pay $300 to get your information back, that's cheaper than calling a lawyer to ask them if you should pay," says Dolan — another perspective can be seen in the case of the South Korean web hosting company Nayana.

CHARLENE RIPLEY
> GOLDCORP INC.

> We had an attacker who basically sent us four extortion emails, each from a valid internal Goldcorp email. We think [the hacker] first attacked and infected our systems in 2015 and hung out and waited, which is typical, for an opportune time to attack.

In late June 2017, it was reported that Nayana paid hackers US$1 million in bitcoin to recover the data of approximately 3,400 customers. In the wake of that payment, several other South Korean companies became targets of Distributed Denial of Service (DDoS) attacks, in which the victimized company is flooded, and rendered inoperative, by incoming traffic from thousands of compromised computers

from different IP addresses. "If you're an e-commerce or other business completely dependent on your IT infrastructure, to have your systems completely shut down or paralyzed is catastrophic in many cases," says Ahmad.

Whether to pay a ransomware demand is, therefore, not an easy decision to make.

IMRAN AHMAD
> MILLER THOMSON LLP

> "I've seen it both ways. I have seen the honest criminal, if you wish. You pay the amount, they give you the key and they walk away. On the other hand, some ... will come back in a couple of months and ... try to exploit another vulnerability."

When the University of Calgary was attacked in June 2016 and its computer systems coopted, it decided to pay a $20,000 demand (the university had cyber insurance, including for ransomware). "Email was available to all faculty and staff users within five business days of the attack," Karen Jackson, General Counsel, said in an email interview. "There is no indication that any personal or other university data was released to the public. The university chose to pay ransom and obtain the decryption keys to protect key research and information that may have been lost as a result of the encryption of laptops, desktops and servers. We did not want to risk the loss of a research scholar's life's work as a result of the attack."

The decision to pay is "a simple cost-benefit analysis," says Dolan. "In one of our cases, the client did a little digging and found that for virtually all of the [compromised] information they had backups, so they didn't pay. In another case, the client needed the files released quickly and couldn't establish whether the files were backed up, so they did pay."

Victim companies also need to consider whether the hackers, like many blackmailers, will release their data. "I've seen it both ways," says Ahmad. "I have seen the honest criminal, if you wish. You pay the amount, they give you the key and they walk away. On the other hand, some will take the money and give you the key. But the flip is they will come back in a couple of months and, more often than not, try to exploit another vulnerability."

Prevention is an obvious critical step to take in reducing the potential harm an attack can cause. "As someone who manages our IT, I can say we pay for top quality antivirus protection," says Danny Schwartz, a partner at Lax O'Sullivan Lisus Gottlieb LLP. "We pay to have our machines locked down if [an attack] was to happen, so the damage would be limited. And all our data is backed up. No system is foolproof, but what you want are multiple redundancies."

Schwartz adds: "To use a low-tech analogy, at Christmas time, the burglars case houses to see whose lights are on and which homes are dark. You want yours on."

He also recommends that firms prevent visitors from logging on to the firm's network. "Back in the day, we'd give them the password to our Wi-Fi. You can't do that anymore. For years, we have had a completely segregated network for guests."

The City of Mississauga has installed its own fibre optic lines for some of its most vulnerable services, says Bench, rather than using a telecom provider or having them cloud-based. "I believe Toronto does this for some services, too," says Bench.

Determining risk is another key consideration for an organization. One way to assess vulnerability is to conduct what is often referred to as a "white-hat" exercise (also known as a red-team investigation), in which outside experts are retained to explore whether they can breach the client's defence systems. The City of Mississauga, as an example, followed this route. "We're seeing more and more of it," says Ahmad, but it's still not where it should be."

Hengesbaugh says that, in the US, it's mostly online clients who are conducting these kinds of white-hat exercises. "I think people who have done it have had some kind of success but I don't think it's entered the mainstream yet." That could soon change. The demand is sufficient enough that some educational institutions, such as Humber College in Toronto, are now offering a Certified Ethical Hacker certificate program.

It's imperative, of course, to ensure that the ethical hackers, as well as any third parties that an organization conducts business with, are completely trustworthy. Unfortunately, that doesn't always happen. "It's increasingly concerning that some organizations fail to consider whether the third parties are, themselves, cyber-secure," says Nishisato, who has seen clients hurt because this didn't occur. "Issues frequently arise where there's been a data breach of the third-party service provider, and it tries to manage it on its own and doesn't disclose [the breach] to its customers." He recommends having a right-to-audit clause in third-party agreements and invoking it as required.

It stands to reason that the more cybersecurity protocols an organization puts into place, the better it will be able to respond to any breaches that occur. It will also result in lower cyber insurance premiums. In a December 2016 article, NetworkWorld.com noted that, "Last year, U.S. insurers earned $1B in cyber premiums. You can minimize your premiums by showing your insurance company you're actively mitigating cyber risks, which is a win-win: lower your risk and secure a more cost-effective insurance plan."

Not only that, it will reduce the numerous costs associated with investigating and responding to a breach. "There are many reports that say if you invest early on you will be saving two to three times after a breach," says Nishisato. "Do the calculus. Nine times out of ten, if not ten of ten, it makes more sense to spend a bit of time and resources on the risk-management side. It will help mitigate tons of your damages."

Although not every firm has the resources to spend a lot of money on prevention, just preparing a simple document, which

includes an incident response plan and a list of who to contact if a breach occurs, can be incredibly helpful, says Charlene Ripley, EVP and General Counsel at the prominent Vancouver-based mining company Goldcorp Inc., which experienced a data breach in 2016. "You don't have the luxury of time. If we had [our team of experts] ready to go, we would have saved precious time at the outset."

Another way to establish effective preventative methods is one that might not be apparent to most organizations: the exchange of information. One of the challenges insurers and insureds face is that "there's not a ton of information-sharing yet," says Eskins.

One organization that chose a different strategy is Goldcorp. When it was breached, its response was a model of what other victims might consider employing. "We had an attacker who basically sent us four extortion emails, each from a valid internal Goldcorp email," says Ripley. "We think [the hacker] first attacked and infected our systems in 2015 and hung out and waited, which is typical, for an opportune time to attack."

In a document that was posted to a public site, the hacker provided sample data and a link to a full torrent download, which measured 14.8 GB when uncompressed. The data included information such as employee performance and compensation rates, bank account details and employee passport scans.

Goldcorp's management team decided it would not negotiate with the hackers and refused to pay any ransom (Goldcorp declined to comment on whether it had cyber insurance). Soon after, a large amount of data was posted on a public website, but "we were able to get it down," says Ripley. "It took two weeks of effort, using all the experts we hired, and we basically got them excavated out of our system."

What Goldcorp did next was extremely proactive. Motivated by the knowledge that others in the mining industry had been targeted by hackers, in June 2016, Goldcorp held a mining cybersecurity roundtable with about a hundred members of the mining industry and other related sectors in Vancouver. "It was a forum for us to share information to combat these types of crimes by sharing what you know," she says. A year later, six of Canada's 10 mining companies formed the Mining and Metals Information Sharing and Analysis Centre to further enhance the exchange of information on this rapidly evolving topic.

Divulging information on attacks that expose a company's vulnerabilities is not always appealing to many C-suite executives, but new legislation in Canada will likely force organizations to do just that. In June 2015, the federal government passed the *Digital Privacy Act*, which will require entities that have experienced security breaches to notify anyone whose information has been compromised. By summer 2017, some of the specifics of the legislation had yet to be ironed out. "The devil will be in the details," says Ahmad, "and we don't know yet exactly what all the requirements will be." Alberta, however, already has legislation in place governing disclosure.

It seems certain a new era in reporting breaches will come to Canada, and organizations will face hefty fines if they fail to comply. "Small and medium-sized corporate clients are often more influenced by legislative changes," says Eskins. "The large ones are typically not swayed by legislation. They tend to do what makes business sense no matter what."

With attacks a daily occurrence throughout the world, cyber insurance seems like an almost mandatory requirement for most firms and many government departments. Anyone thinking the problem might go away should heed the words of Baker & McKenzie's Dean Dolan: "We're all screwed, I think, because it's going to be a really rough few years ahead. It's going to get worse before it gets better."

IN HOUSE INSIGHT

CYBERSECURITY CHECK LIST

Ransomware and denial-of-service attacks are on the rise. Here's how to prepare for the inevitable

RANSOMWARE IS THE FASTEST GROWING malware threat, according to a recent report by the US Federal Bureau of Investigation. "On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015." Such daunting statistics indicate the need to do as much as possible to protect against such attacks. There are many important steps that in-house counsel can take to shore up their defences, including:

"First of all, prepare a risk profile," says Vanessa Coiteux at Stikeman Elliott LLP. Doing so is important "to determine your weaknesses." In addition, the risk profile should include an incident response plan.

Utilize dedicated cybersecurity resources, says Ira Nishisato of Borden Ladner Gervais. "Threats are constantly evolving and organizations of a certain size really need dedicated cybersecurity resources and not simply someone in the IT department who has a dozen other things to worry about every day."

Establish a cybersecurity response team before an event happens, says Baker & McKenzie's Brian Hengesbaugh. "Have your forensic specialists and external counsel on board and [where applicable] call centres and credit monitoring [in place]. [The process] can also show where PR and legal, for example, might not see things the same way."

Run tabletop exercises, says Miller Thomson's Imran Ahmad. "Those meetings help identify any issues and uncertainties in your organization."

Know in advance where to obtain bitcoins, in case you decide to pay a ransom, says Marsh's Greg Eskins. "Do you have a bitcoin account? A bitcoin broker? Can we get, say, $50,000 of bitcoin in a relatively short time, usually 24 to 72 hours?"

No matter how sophisticated your defences, it just takes one employee to click on a phishing email and the hackers can get in, says Danny Schwartz of Lax O'Sullivan Lisus Gottlieb. "Employee training is critical. Make sure to include phones when protecting your systems. Now there are lots of viruses on phones."