Insurance
BUSINESS CANADA
WWW.INSURANCEBUSINESS.CA
ISSUE 7.04

SPECIAL REPORT

CYBER INSURANCE

Brokers' Key Questions Answered

Brokers' key cyber questions answered

Insurance Business Canada spoke to four experts in the cyber insurance space to get their perspective on emerging trends, crucial policy details and how to convince clients of the necessity of cyber coverage

FROM EQUIFAX to Marriott, from WannaCry to Petya, cyber attacks have been grabbing global headlines in recent years – but for many, they still feel like something that happens "somewhere else." In a landscape of Russians allegedly interfering with US elections or giant firms like Yahoo being brought to their knees by hackers, comparatively small Canadian businesses can seem such a long way from it all.

Until, that is, you realize that nobody is safe from what has become *the* crime of the 21st century.

Canada's new threat

Research by Accenture and the Ponemon Institute reveals that cyber attacks are costing Canadian companies millions – the annual cost of malware- and people-based attacks, such as social engineering and phishing, reached US$9.25 million in Canada in 2018. Meanwhile Scalar Decisions' annual cybersecurity study reported that 58.4% of Canadian firms had data exfiltrated during the previous year, and more than 25% of the organizations victimized lost personally identifiable information on customers or employees.

The attacks are only getting more frequent and more devastating, too. "One of the first trends right off the bat when it comes to

ransomware is that we're seeing a lot more claims, and the strains of ransomware are becoming more and more virulent, making them harder to remedy," says Tony Dolce, Chubb's cyber claims lead for North America. "The other significant trend we're seeing is that ransom demands are going up. A couple of years ago, a demand in the neighbourhood of $15,000 to $20,000, converted into cryptocurrency, were the norm. Then it climbed up into the $30,000 range, and over the course of the last year and a half, we've started seeing demands frequently in excess of $100,000. That's a very disturbing trend."

Not every business has $100,000 sitting in the bank to pay off a ransom demand, so the need for cyber insurance has never been more apparent. It's a message that may finally be getting through.

"Most organizations finally realize they have some degree of exposure and know they must do something about it," Brian Rosenbaum, Aon's national cyber leader in Canada, wrote in the organization's 2019 Cyber Security Risk Report. "For the better part of the last decade, a large number of Canadian organizations were either ignorant or in denial about their cyber risks. So, we have no doubt seen progress."

A survey from a Silicon Valley analytics firm revealed that cyber insurance take-up rates among Canadian companies are growing: Only 18% of companies had full-coverage cyber insurance in 2017, but 40% purchased it in 2018. On the other end of the spectrum, the proportion of Canadian businesses that reported not having any cyber insurance dropped from 36% in 2017 to 22% in 2018.

Clearly, the appetite for cyber insurance is there – but how do brokers make the most of it?

A hard sell

While businesses are becoming more educated on cyber threats, some retain the "it won't happen to me" mentality. Typically, they fall into the trap of thinking that if they don't collect personal data as part of their business, they won't be a target; or that if they have their own IT department in-house, they will be able to handle their exposure; or, simply, that they're not big enough to be hit.

The reality, of course, is that small businesses are under attack, and it's up to brokers to get that message across and convince them of the benefits of insurance. How to do that, however, is open for debate.

"We get a lot of objections from clients who say, 'We have the best IT systems in place; we don't actually need a cyber policy,' and you can get quite a hostile reaction from a CISO or somebody in the IT department that you're trying to sell a cyber policy to because it's effectively saying, 'The IT department isn't good enough, so here's a cyber policy to help mitigate some of your exposures,'" says Lindsey Nelson, international cyber team leader at CFC Underwriting. "It's really helpful to play on the human error element of cyber versus whether the IT systems are good or bad."

Meanwhile, James Arnold, principal of cybersecurity at KPMG, says it's about making cybersecurity as important as the overall value of the business, particularly when a merger or acquisition is in the works.

"Insurance brokerages and agencies, as well as sellers of any type of business, can help secure and enhance the value of their entities prior to a sale by ensuring their cybersecurity risks are properly addressed," he says. "A well-developed and -implemented cybersecurity program will help ensure there are no surprises during the deal period and after closing. It will also help put buyers at ease, knowing the target cybersecurity issues have been addressed."

Clearly, there are plenty of contrasting opinions out there on the best approach to market – and if brokers are to truly capitalize on this burgeoning space, it's vital that they get a clear understanding of what the product is and where it's heading. That's why *Insurance Business Canada* has put together a panel of experts to address five key questions that our research suggests brokers are lacking clarity on.

Armed with this insight from industry experts, we hope brokers can start to transform cyber insurance from the product everyone is talking about to the product everyone is buying.

Paul Lucas
Managing editor
Insurance Business Canada

MEET THE PANELISTS

Jacqueline Detablan
Vice-president, specialty
CNA CANADA

Jacqueline Detablan is CNA Canada's vice-president of specialty, a division that includes healthcare, professional liability and technology, as well as the commercial and financial institutions executive liability departments. She is a frequent speaker at industry conferences, focusing on professional liability, especially emerging cyber risks.

Michael Kalakauskas
Assistant VP and product manager, professional liability and cyber liability
TRISURA GUARANTEE INSURANCE COMPANY

As the national E&O and cyber product manager at Trisura, Michael Kalakauskas is responsible for product development, strategy, training, reinsurance placement, marketing and broker relationships in Canada. His product expertise includes miscellaneous and technology E&O, media liability, and cyber liability.

Darren Peters
Director, commercial insurance
THE WAWANESA MUTUAL INSURANCE COMPANY

Darren Peters brings 23 years of insights from both the insurer and the broker perspective. He began his career as a licensed insurance broker, ultimately holding the role of COO at an independent brokerage. After 13 years, he transitioned to the insurer side and has pursued extensive industry volunteer work, including serving as president of the Insurance Brokers Association of Manitoba.

Dan Lewis
Director of cyber liability and Canadian management liability practice leader
GALLAGHER

Dan Lewis advises corporate clients in the for-profit and non-profit sectors on liability exposure in the areas of D&O (private and publicly traded companies), E&O, cyber liability, employment practices, fiduciary liability, white-collar crime, kidnap/extortion, trade credit and transaction liability. Lewis has worked in the insurance market throughout Canada, the US, the UK and Bermuda since 1998.

What key market trends should brokers be aware of in the cyber insurance space in 2019?

Michael Kalakauskas: I would place key market trends into two different categories: cybersecurity trends and cyber coverage trends. Both categories should be front of mind for brokers, not only in 2019, but in the years to come as well, as they allow brokers to think of exposure, risk and insurance solutions simultaneously.

From a cybersecurity trend standpoint, the sheer volume of cyber attacks and compromised personal information on a worldwide level is at an all-time high and will only continue to grow with the expansion of things like company interconnectivity, the Internet of things, the use of cloud services, artificial intelligence and machine learning, automation, and small to medium-sized business vulnerability.

These trends are at the heart of cybersecurity and point to the need for all organizations to increase their security and awareness in protecting themselves against cyber attacks and data breaches. Cyber criminals and attackers are only getting more sophisticated, so as an industry, we need to keep up with, and respond to, emerging threats. Another important trend from a cybersecurity standpoint is the evolving landscape of international data privacy laws and government/regulatory body involvement.

From a cyber coverage standpoint, brokers need to be aware that third-party liability coverage for data breaches is only one piece of the overall cyber insurance puzzle. The trends from a coverage standpoint – and the biggest causes of current cyber claims, in Trisura's experience – are ransomware, social engineering and business interruption. Not all businesses carry large amounts of personal data that data breaches might target; however, all businesses are dependent on computers, cell phones and the internet, ultimately making them vulnerable to different types of cyber attacks.

The one thing all companies do hold is employee data, so all companies are exposed to a potential data breach. Our experience, though, is that the coverages I mentioned are the ones most sought after by small- to medium-sized businesses. It is easier to target small- and mid-sized companies, as they may not have adequate security measures and resources in place to protect themselves. Small companies must reassess their security position and ensure adequate measures and controls are implemented to safeguard against today's cyber attacks.

Jacqueline Detablan: There are several. For example, there has been an increase in the level of business-interruption-related claims activity after a cyber criminal strikes, and brokers cannot ignore ransomware/cyber extortion and the fact that no industry or size of operation is safe from this threat. Cyber crime is on the rise, as are the financial impacts on businesses that become victims of cyber attacks – Cybersecurity Ventures projects that the global cost of cyber crime will grow to $6 trillion by 2021.

In the current environment, cyber insurance has become a valuable risk transfer and risk mitigation tool for companies across the board. Even over the past year, there have been evolutions in the cyber insurance space, from continued expansions of coverage for business interruption and system failure resulting from cyber attacks to a heightened focus on silent cyber, according to experts at CNA Canada.

There is also a lot of discussion around the topic of cyber as a peril. Rather than covering all exposures related to cyber under a cyber policy, consideration needs to be given to treating cyber as a peril that needs to be addressed under multiple coverage lines.

Darren Peters: New cyber trends are emerging constantly. And while threats like ransomware attacks, phishing scams and banking trojans aren't new market trends, they are becoming more sophisticated and commonplace.

As an insurer that is 100% broker-distributed across Canada, it is our duty to instill in our brokers the confidence to conduct effective risk assessments with our mutual clients and recommend the appropriate first-

CNA

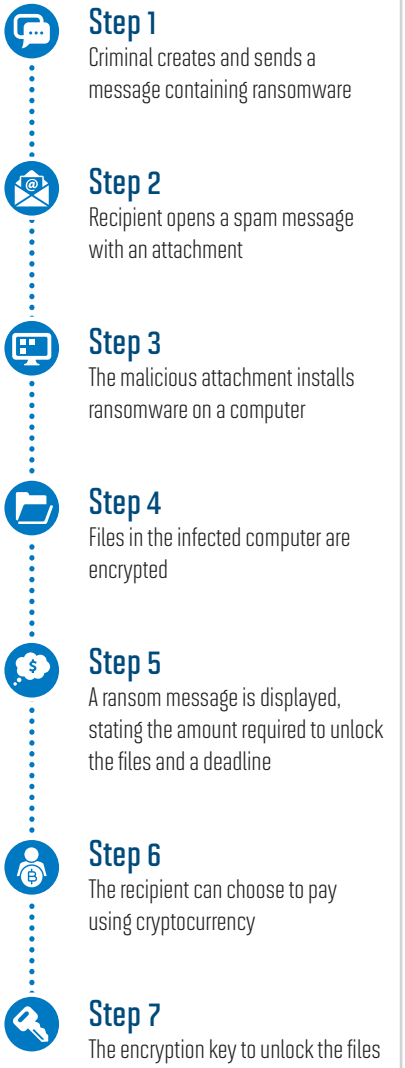
In today's technology-driven world, cyber threats represent a critical and growing risk.

There is no one size fits all approach.

Now available, pre-breach cyber risk services from CNA designed to help companies take an individual and holistic approach to cyber threats, aiding CNA cyber policyholders combat cyber losses with minimal controlled and predictable costs.

Learn more today: cnacanada.ca.

STAGES OF A TYPICAL RANSOMWARE EVENT



Source: National Cyber Threat Assessment 2018, Canadian Centre for Cybersecurity

and third-party coverages to address common and emerging vulnerabilities. In partnership with the Boiler Inspection and Insurance Company of Canada, one of the most innovative firms for cyber risk coverage, we are able to provide our brokers with outstanding education and training seminars.

We are mindful of how overwhelming it must be for clients to try to keep up. We encourage our brokers to take the lead on simplifying the process, educating clients on best practices to avoid attacks and ensuring the right coverage is in place.

Dan Lewis: Because the threat environment is constantly evolving, the insurance market is continuously trying to adapt. New insurance contract wordings may specifically address threats like cryptojacking, push payment fraud and system failure, or clarify their intent with respect to cyber warfare. In the past, these may not have been addressed. Some forms will even address full physical damage.

PIPEDA, the new federal law enacted in 2018, addresses mandatory breach reporting when there is a risk of significant harm. Also, there is no proof of economic damages required in order for plaintiffs to bring a claim. We will continue to see the tort of 'intrusion upon seclusion,' or privacy breach, commonly referenced in class-action litigation.

Which client groups should be the target markets for cyber insurance this year?

Jacqueline Detablan: Given the increase in ransomware events across all industries, it's impossible to identify a specific market. In fact, cyber crime as a whole impacts businesses of all sizes. Sixty per cent of small to medium-sized businesses will fail six months after a cyber attack.

Brokers should have conversations with their clients and educate them on the importance of cyber risk. If a client chooses not to buy, they need to be comfortable with the possible stress on their balance sheet, as well as how to respond to these events independently. Insurers have relationships with vendors who are experts in dealing with these situations.

CNA Canada's latest cyber proposition reflects the changing risk environment. Technology adoption creates new exposures, and cyber criminals are becoming more sophisticated. Our new pre-breach services are designed to enhance our cyber solutions to help policyholders combat cyber losses with minimal controlled and predictable costs. The more prepared a business is to handle a cyber attack, the faster it can identify the problem and get back on its feet, which means fewer resources are used and they see less operational disruption.

Dan Lewis: If a corporation holds sensitive data, such as financial, education or healthcare data, they were likely among the first to adopt cyber coverage in Canada a few years ago. We are seeing much more take-up among companies that are more concerned about business interruption losses: industries such as manufacturing, infrastructure and energy/mining, where cyber coverage perhaps has not been as well understood in the past.

Canadian municipalities are another area where loss frequency has dramatically increased, especially when it comes to ransomware. In 2018 and 2019, we have seen a number of losses impacting smaller cities in Canada.

Finally, small and medium-sized enterprises, which traditionally felt somewhat immune to cyber attacks and had an "I'm not a target" mentality, have realized that their balance sheet likely cannot withstand even a low six-figure claim and that they likely cannot afford to have their network down for several days.

Darren Peters: Truly, all client groups are at risk. There was a time in which privacy concerns were the only argument for cyber coverage. Today, the adoption of technology in virtually every aspect of our lives – business and personal – is changing the way we think about cyber threats.

From a commercial perspective, we primarily write policies for small and medium-sized businesses, as well as agricultural clients, all of which are increasingly bearing the brunt of online predator groups. The threat of losing or compromising customer data is still very real; however, there are more consequences to consider.

If an online retailer were to be breached, for example, there could be considerable revenue lost from business interruption and long-term damage to its reputation. The same

WHEN CYBER CRIME STRIKES, WILL THEY BE COVERED?

The adoption of technology in virtually every aspect of our lives is changing the way we think about cyber threats.

Our suite of cyber risk solutions is designed to help your clients—personal and commercial alike—protect themselves in the face of our new realities.

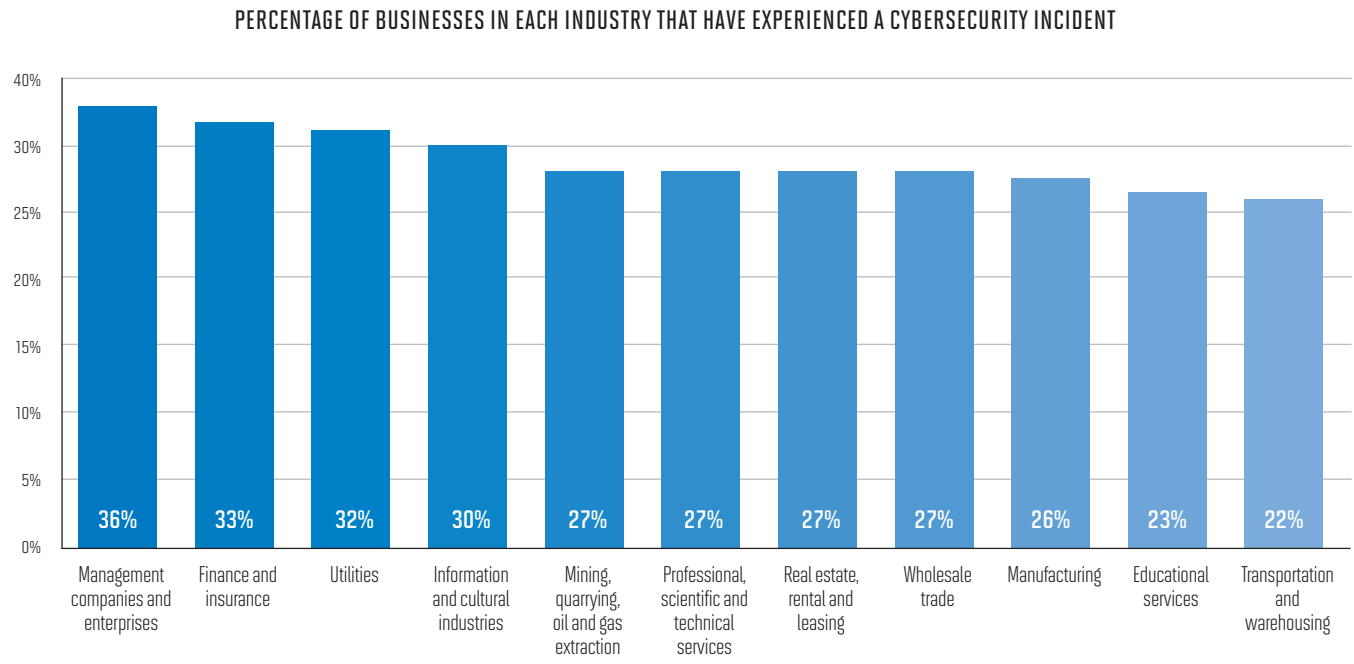
Contact your Wawanesa Business Development Representative for resources to prepare your clients for the exposures of today.

wawanesa.com/cyber

Wawanesa Insurance

Financial Strength A.M. BEST A Excellent

TOP INDUSTRIES TARGETED BY CYBER CRIMINALS



Source: Statistics Canada, 2017

threat exists in manufacturing – a sector that may not have been previously concerned about cyber risks – thanks to the level of technology used throughout facilities' operations.

In our personal lives, most of us conduct routine banking, shopping and online research activities, and we take security for granted. Cyber criminals know this and are targeting us in ways that appear more professional and authentic every day. The disadvantage for individuals – and small businesses, for that matter – is that they simply don't have the resources at their fingertips to correct a breach, and recovery can be an exceptionally long and expensive process.

Michael Kalakauskas: All client groups! All businesses – small, medium or large – have cyber exposures, and each company should be having conversations with their insurance broker about adequate cyber insurance coverage and risk transfer options.

That said, I would prioritize some of the industries that have not previously bought cyber insurance on a widespread basis. Industries including finance, banking, healthcare, retail and hospitality – all well known for holding and using personal information – have already been exposed to cyber insurance and the risk of data breaches; however, industries like construction, transportation and manufacturing, as well as smaller professional offices, are slowly being exposed to the importance of cybersecurity and need more awareness in this space.

At Trisura, we are trying to increase the exposure of cyber insurance with all our small- to medium-sized business clients, regardless of industry type. As mentioned, it is easier to target small- and mid-sized companies, as they may not have adequate security measures and resources in place to protect themselves. Trisura has a large surety book that comprises clients of all sizes in the construction industry – for example, builders, developers and contractors – and with them being more reliant on technology and computers, it is imperative we offer cyber solutions as part of their overall insurance and surety bonding package.

Likewise, we insure many small- to medium-sized professional offices for E&O and directors & officers liability and are currently trying to target them for cyber coverage as part of their insurance portfolio.

How can brokers overcome the "it won't happen to me" mentality held by many smaller businesses in reference to cyber attacks?

Darren Peters: Cyber attacks are still just a concept to many individuals and businesses – something you'd see in a movie, for example, or more of a concern for large corporations. The "it won't happen to me" mentality tends to dissolve when threats become relatable. Frankly, our brokers are equipped with many of their own claims examples to share with clients to illustrate just how vulnerable the entire population is.

In addition to sharing real-life examples, our broker partners can continue to provide education and increased awareness to our mutual clients digitally, through social media, blogs and podcasts, as well as through traditional channels like education sessions. In collaboration with the Boiler Inspection and Insurance Company, we are able to provide co-branded resources for our broker partners to support their conversations with insureds.

In my opinion, nothing is more effective than facts and statistics to educate clients and convince them that "it won't happen to me" should really be, "When it happens to me, will I be covered?"

Michael Kalakauskas: All businesses, regardless of size and industry type, have cyber exposure. Regardless of whether they hold or store their customers' or suppliers' personal data or corporate information, they have data on all of their employees that is at risk. Furthermore, all companies are reliant on computers, cell phones and the internet, and therefore would be susceptible to loss in the event of a cyber attack like ransomware, a hack, data loss, payment diversion or phishing, malware, and software or hardware failure.

Cyber attacks are indiscriminate. Even if it's not from an attacker, one of the biggest forms of cyber exposure is the error of an employee clicking the wrong link, sending an email to the wrong person or leaving an unencrypted laptop or cell phone at a public place. Cyber exposure could come from anywhere, and if it were to happen, it could give rise to significant financial loss.

My rule of thumb is to advise businesses that cyber attacks are not a matter of 'if' but more of 'when' – and whether the company is able to withstand the financial impact of such an attack or loss. If the company is not equipped to sustain such an attack, or the business would like some additional protection, then cyber insurance is a key to their risk management process, no matter the size of their business.

Dan Lewis: There are four main areas that we focus on when speaking to smaller organizations. Our discussion usually begins with a refresher on the duties of directors and officers under the Canada Business Corporations Act [CBCA]. This is key because ultimately the directors and officers are responsible for safeguarding the data they collect, and they are charged with safeguarding the corporate balance sheet. Additionally, we link the organization's ethical responsibility to act in the best interest of all of the corporation's stakeholders, not just shareholders. This includes employees, customers and the general public. We also focus on the connection to service providers that insurance provides: breach coaching, PR, forensics, etc. This is invaluable, as SMEs would likely not have those relationships in place.

We as brokers can provide concrete examples of where SMEs have had tangible Canadian cyber claims – ransomware, social engineering fraud, rogue employee claims, accidental employee data issues – and the downstream impact of not having insurance in place. Finally, we note that the 2018 NetDiligence Cyber Claims Report found that small businesses with revenues of less than $50 million are targeted 49% of the time by hackers.

Jacqueline Detablan: Given the number of incidents in the media, I am hopeful that we have moved beyond this mindset. According to the 2019 Verizon Data Breach Investigations Report, 43% of breaches involved small business victims. While Statistics Canada reported that 58% of businesses undertook activities to identify cybersecurity risks and only 5% of Canadian businesses reported not having any cybersecurity measures in place, there continue to be major vulnerabilities within companies' four walls that expose them to cyber attacks. The human element, for one, plays a central role in increasing a company's cyber risk. I would encourage brokers to speak openly about the exposures without using traditional scare tactics.

What are the key differences between cyber as a stand-alone product and as an add-on? In which situations should brokers consider one option the better choice for clients?

Jacqueline Detablan: This is a tough question, given that not all add-on extensions are created the same, and sometimes these can create a false sense of security.

Brokers should review the limits of these bolt-on endorsements, as well as the various aspects of coverage included. Loss drivers today are focused on the first-party side of the coverage, particularly business interruption and cyber extortion. If the add-on does not contain these items, a full policy may be worth

PESSIMISTIC ABOUT CYBER PROGRESS

54% of IT professionals believe their organization's cybersecurity posture will either stay the same or decline

58% believe cybersecurity staffing problems will worsen

46% predict artificial intelligence will not reduce the need for experts in cybersecurity

Source: 2018 Study on Global Megatrends in Cybersecurity, Ponemon Institute

exploring. In addition, costs associated with even a relatively small cyber event can add up quickly. A modest sublimit won't go far.

Dan Lewis: The first-party extension on a general liability policy has been a good introduction for many clients in past years. It at least gave brokers a springboard to discuss the difference between the add-on and a full cyber policy.

Most add-ons only provide a sliver of first-party cover, such as notification costs, but may not respond to other first-party costs. They likely have no coverage for PCI fines/penalties, cryptojacking, social engineering, business interruption, contingent BI, system failure, ransomware payments, media liability and full data re-creation. They may offer a $50,000 to $100,000 sublimit, which may be eroded quickly. The 2018 Ponemon study pegged the average Canadian claim at nearly $6 million. Finally, most of these add-ons are a first-party coverage only, versus first- and third-party.

The key for brokers is to make sure that their clients clearly understand what they're buying. Weighing the pros and cons of coverage versus cost, and explaining what is available, is an important education step.

Darren Peters: Three key considerations are the limits of insurance, retroactive coverage and corrective action plan costs. Depending on what type of data one stores, the limit of insurance offered by any add-on coverage should be closely examined. Often, the limits are lower and can be incrementally increased. Stand-alone cyber offerings can be more flexible and allow clients to purchase much higher limits than are available with add-on cyber coverage.

With cyber claims, data breaches often go undiscovered for long periods of time. Some stand-alone options offer full, or at least partial, coverage for events that may have occurred even before the inception date of a traditional property & casualty policy. This is something we strongly recommend our broker partners address when consulting with clients.

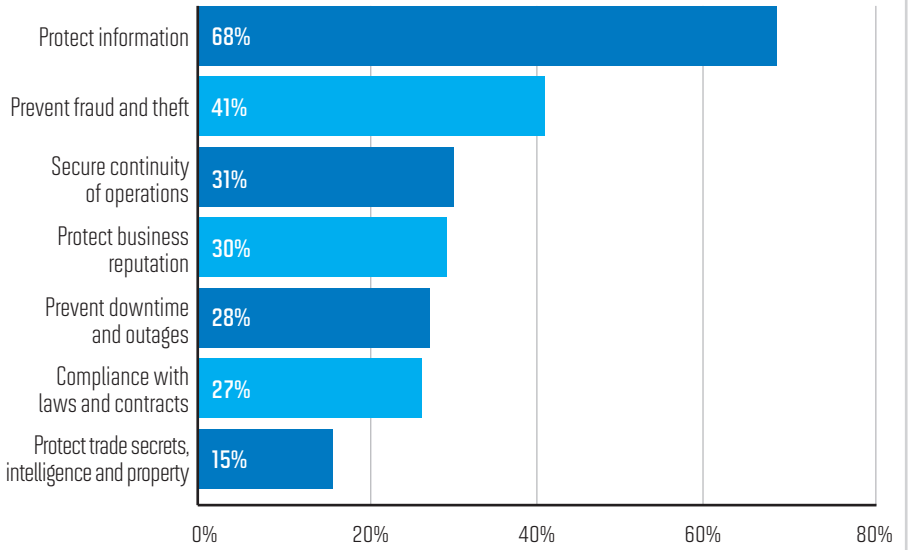
Depending on what businesses our clients are in, or how they use their personal computers, it is important to help them understand what the regulatory requirements would be if they experienced a data breach or cyber event. At times, regulators will mandate compliance protocols and/or audits, which drives up recovery costs.

Other factors to consider are bodily injury because of a cyber breach, post-event remediation, notification costs, as well as business interruption costs that often result from these types of claims. In most cases, a stand-alone or add-on cyber policy can be put into place at any time, not just at renewal.

Michael Kalakauskas: The key difference between a stand-alone cyber product and an add-on by endorsement is the quality of the coverage and of the claims service. With a stand-alone cyber policy, you are getting a dedicated product – and limits – with specific and broad coverage and, most likely, access to a comprehensive cyber response team that can help navigate any claim or cyber incident. Most add-on cyber endorsements cover such a limited amount, and language tends to be very restrictive. Furthermore, add-ons usually contain such a small limit of liability, or the limit itself is shared with the main policy limit.

My hope is that add-ons become less and less used in the industry and that all clients – again, regardless of size and operation – purchase a stand-alone cyber policy to properly cover themselves. Another advantage of a stand-alone policy is that it is most likely being managed by a dedicated and experienced cyber underwriter. A true cyber underwriter can not only help with exposure and risk identification, but can also tailor the cyber policy and coverage to the specific needs of the client. Most add-ons are offered by underwriters in the professional liability or casualty space, and they may not have any expertise in the field whatsoever.

WHAT MOTIVATES COMPANIES TO SPEND MONEY ON CYBERSECURITY?



Source: Statistics Canada

What are the vital elements of a good cyber insurance policy, and which elements are particularly important for different clients?

Dan Lewis: The primary reason you buy insurance is that you want claims to be paid. So, partnering with an insurer that has experience in handling Canadian cyber claims is key,

Want something real?

Real people. Real relationships. Real expertise.

Find out more about our specialty insurance, warranty and surety solutions.

Visit www.trisura.com

TRISURA®
a step above

Trisura Guarantee Insurance Company is a Canadian owned and operated Property and Casualty insurance company specializing in niche insurance and surety products. We are a proud supporter of the Insurance Brokers Association of Canada.

MOST COMMON CYBER INSURANCE EXCLUSIONS

Intentional or deliberate acts

Illegal activities

Privacy liability

Outdated anti-virus software

Certain types of websites (adult entertainment, gambling and sales of firearms or weaponry)

Source: Insurr.com/ca

including strong relationships with Canadian-based service providers such as breach coaches, IT, etc. You don't want a carrier to sit on their hands for days in a ransomware scenario, wondering whether elements of the claim might not be covered. Speed of response is important as well. How long is the waiting period for the business interruption coverage to trigger?

The coverage, of course, is important, and the most valuable coverage sections to an individual client differ depending on their business. For instance, a retailer may value PCI coverage. An oil company may be most interested in physical damage cover. An auto parts supplier may value business interruption cover that can extend to the full supply chain. A law firm may value crisis management services, reputational cover and robust data re-creation coverage.

Michael Kalakauskas: Overall, good cyber insurance provides coverage for both an insured's first-party and third-party losses associated with a network security breach, or the loss, theft or unauthorized disclosure of personal information or confidential corporation information. The coverage should include expenses related to breach notification, extortion threats, public relations, credit monitoring, forensic investigation, defence costs, the costs of judgments or settlements, regulatory claims, business interruption, and media liability, among other things. Every business has an exposure and should be protected accordingly. Exposures come in the form of employee information, customer information, internet access, electronic and network activities, and the overall use of technology.

Specifically, the most important element of any good cyber insurance policy is the claims handling service and response team associated with it. A cyber insurance policy should give clients access to experts in all fields of cybersecurity and make them feel comfortable throughout the whole process, whether it is a full-blown claim, a possible breach or a system hack. A good response team should include law firms and breach coaches, forensics and investigation professionals, public relations and communication specialists, and breach notification, identity repair and credit monitoring firms.

Legal experts can help minimize the risk of litigation and fines in the wake of a breach. They can provide legal advice based on your specific incident, such as determining how to notify affected individuals, government agencies, third parties and others who may be impacted. The law firms and breach coaches can also manage breach response teams and oversee all aspects of the response.

Forensic and investigative providers can advise your organization on how to stop the current data loss, prevent further harm and secure evidence as necessary. They can also determine where, when and how the breach or hack occurred, analyze data sources to determine what information has been compromised, and assist in data restoration.

Public relations providers can help develop both the internal and external communications needed during an incident, as well as oversee crisis management services. They can also provide advice on how to best position the incident to key audiences, update social media and help manage media questions related to the issue.

Breach notification providers can help in the form of credit monitoring, credit reports, call centre services and direct mail campaigns.

Jacqueline Detablan: Claims servicing should be the main driver when choosing a carrier, as well as which vendors they use. Experience is also key. Cyber policy language within the market has become pretty broad, but value-added services such as pre-breach are an asset, while claims response remains key. I feel the market has lost sight of the reason clients are buying the coverage.

Darren Peters: A good policy – cyber or otherwise – is, above all else, fully understood and deemed to be valuable by the insured. It should be tailored to the insured and reflective of the unique exposures they are up against in their lives or businesses. A thorough consultation with a client may reveal such vital elements as media liability, regulatory privacy proceedings, regulatory fines and penalties, notification to affected individuals, services to affected individuals, public relations services, electronic data recovery and replacement expenses, legal services, and information and network security, such as unauthorized release of information.

We call this cyber coverage; however, keep in mind when educating your business clients that this can just as easily occur when paper documents, contracts, photos or other forms of literature are not properly secured. IB

Insurance BUSINESS CANADA

Insurance Business Canada is the leading business magazine for insurance professionals

- Profiles and case studies of successful brokers and agents
- Interviews with industry leaders
- Special reports and surveys
- In-depth features on specialist lending
- Business strategy content

Find out more and subscribe at insurancebusinessmag.com/ca