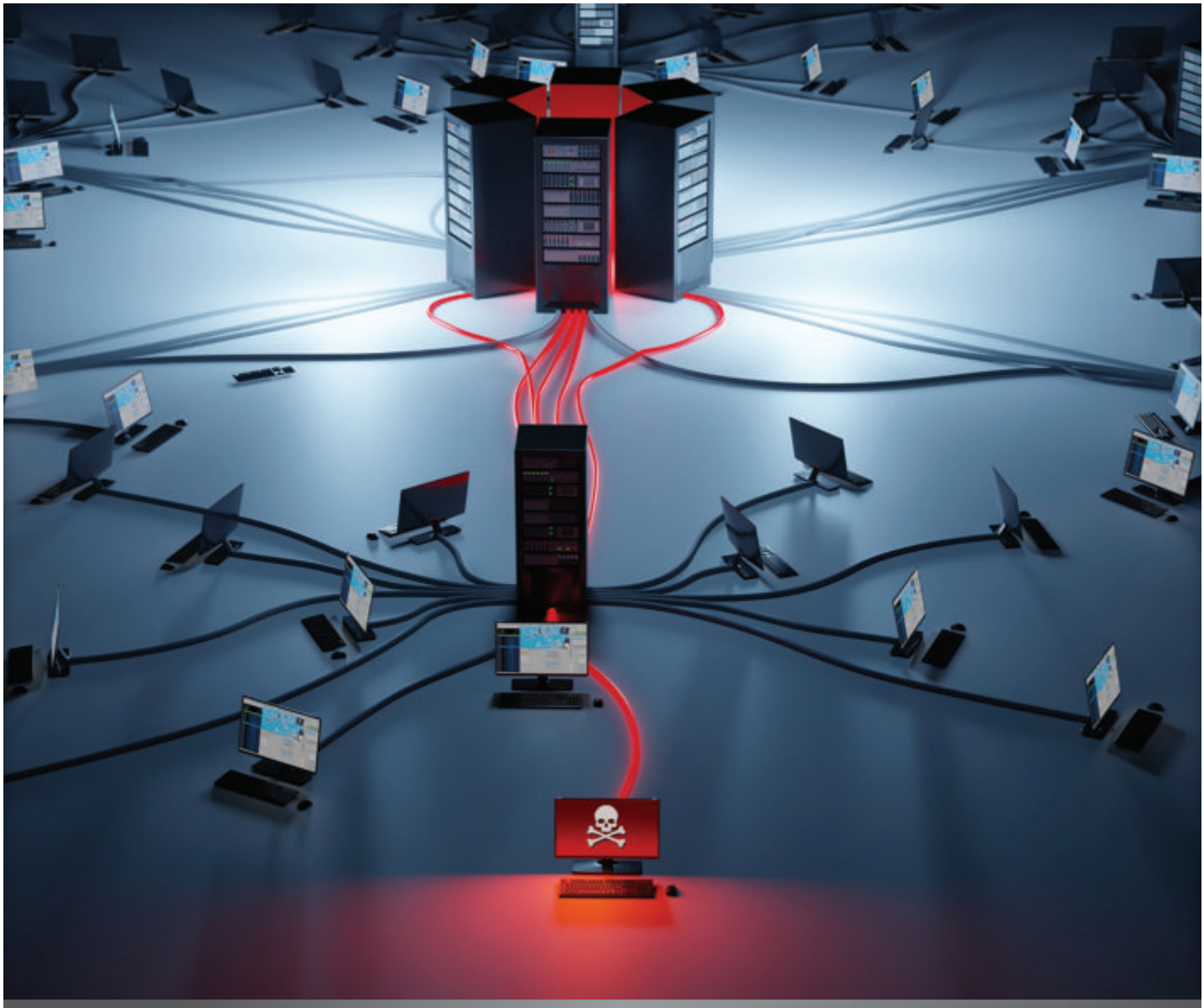


Insurance BUSINESS CANADA

EXECUTIVE INSIGHTS SERIES

CYBER 2021

What trends and threats do brokers need to stay on top of in a tightening cyber market?

Coalition®

Insurance that stops hackers in their tracks

Coalition, the leading provider of cyber insurance and security solutions, partners with brokers to protect their clients from cyber threats.

- ✓ Automated data collection and online platform to rate-quote-bind in under 4 minutes
- ✓ Industry-leading policy form
- ✓ Risk management services and tools included for every single policyholder

Don't just take our word for it.

See testimonials from our broker partners.

"I never thought I'd say I was passionate about an insurance platform, but what you guys have built is exceptional."

"Easy to rate, competitive pricing and coverage, great customer service. Coalition is the first place I go to for cyber business."

Learn more at coalitioninc.ca

CYBER INSIGHTS 2021

Insurance Business Canada takes a closer look at some of the most complex cyber issues to emerge so far in 2021

CYBER RISK is everywhere. It's an enterprise problem that can trigger a string of losses well beyond the technology or systems that were initially compromised. Cyber events can result in business interruption (both primary and contingent), productivity loss, reputational damage, physical damage, and significant legal repercussions and recovery expenses. It's no wonder the scale and frequency of cyber insurance losses continue to soar.

Ransomware is arguably the most pressing issue the cyber insurance community is dealing with today. This variation of malware allows hackers to lock businesses out of their systems until they pay a ransom, usually in cryptocurrency. In recent years, there has been a significant uptick in the frequency and severity of ransomware attacks, impacting businesses of all sizes and in all sectors. Hackers have grown more sophisticated and targeted in their attacks, aiming for larger organizations that can afford bigger ransoms.

In the past five years, the average ransom demand has shot up from US$15,000 to US$175,000 – an almost twelve-fold increase – according to the NetDiligence 2021 Ransomware Spotlight Report. Total ransom demands crossed the US$1 million threshold in 2018, the US$3 million threshold in 2019, and publicly available data indicates that they surpassed US$50 million in 2020, although this was likely negotiated down.

The ransomware headache doesn't stop there. In 2020, a new wave of ransomware attacks known as 'double extortion' hit the market. With these attacks, threat actors are maximizing their chance of making a profit by threatening the victim with an additional abuse of the information they've encrypted, such as selling or auctioning it.

In this fast-paced and ever-changing risk landscape, cyber insurers have reacted by seeking more rate and shoring up their underwriting guidelines to control their costs and protect their books. Some have even started sub-limiting ransomware and applying co-insurance provisions, forcing insureds to share more of the risk.

The firming of the market is having a big impact on brokers. Not only do they have to work harder to secure adequate coverage for their clients, but they also have to educate themselves and continue to develop technical skills around cybersecurity controls and best-practice cyber risk mitigation.

Proactive cybersecurity controls are absolutely essential in today's evolving threat landscape. Many would argue that cyber insurance should not be seen simply as a financial risk transfer product; rather, it is a holistic risk management solution that protects not only insureds, but also the cyber insurance market itself. As rates rise, coverage constricts and cyber threats boom, we will only succeed with an 'all in this together' approach.

With that in mind, *IBC* reached out to four experts in the space to explore the key themes and questions in the sector, from best practices for risk mitigation to up-and-coming cyber threats. Through their insights, we hope to provide brokers with an enhanced understanding of the current state of the cyber insurance market.

Bethan Moorcraft
Senior editor
Insurance Business Canada

CYBER INSURANCE

MEET THE EXPERTS

Angela Feudo
Manager, professional solutions
Trisura Guarantee Insurance Company

As the national E&O and cyber product manager at Trisura Guarantee Insurance Company, Angela Feudo is responsible for product development, strategy and training in Canada. Prior to joining Trisura, Feudo worked in underwriting for more than 17 years. She has a diverse underwriting background, having started her career in property & casualty before moving into crisis management and ultimately E&O and cyber.

Ian Fraser
AVP, tech/cyber and professional lines
Sovereign Insurance

A seasoned leader with more than 20 years of professional lines/ technology insurance experience, Ian Fraser offers a breadth of knowledge and expertise. At Sovereign Insurance, Fraser develops commercial strategies for cyber and professional lines with a strong focus on product, pricing and customer requirements. He regularly speaks on technical insurance panels and is recognized among his peers as a thought leader in the areas of cyber, professional liability and management liability.

Miki Ho
Business development team lead – Canada
Coalition

Miki Ho leads business development for Coalition in Canada. He joined the company in early 2020 and helped launch Coalition's insurance operations in Canada in May 2020. With a background in underwriting large, complex cyber and tech risks, Ho is a resource for Coalition's broker partners and policyholders as they work to solve cyber risk. He believes that insurance is just part of a cyber risk management strategy and is always eager to share insights on how to better manage and mitigate risk.

Lindsey Nelson
Cyber development leader
CFC

Lindsey Nelson oversees the global distribution strategy across CFC's cyber portfolio, undertakes key account management and provides in-depth training within the business line. Nelson has more than a decade of experience underwriting cyber and technology risks, which has put her in demand for a wide range of conferences, and she continues to play an active role in underwriting.

● How would you describe the current state of the Canadian cyber insurance market?

Angela Feudo: The cyber insurance market has, for the most part, continued to tighten over the last year. There have been numerous carriers that are reducing their capacity, increasing rates, restricting terms and implementing tighter underwriting controls. While capacity contractions generally are becoming more common, there has been a focus on limiting network extortion.

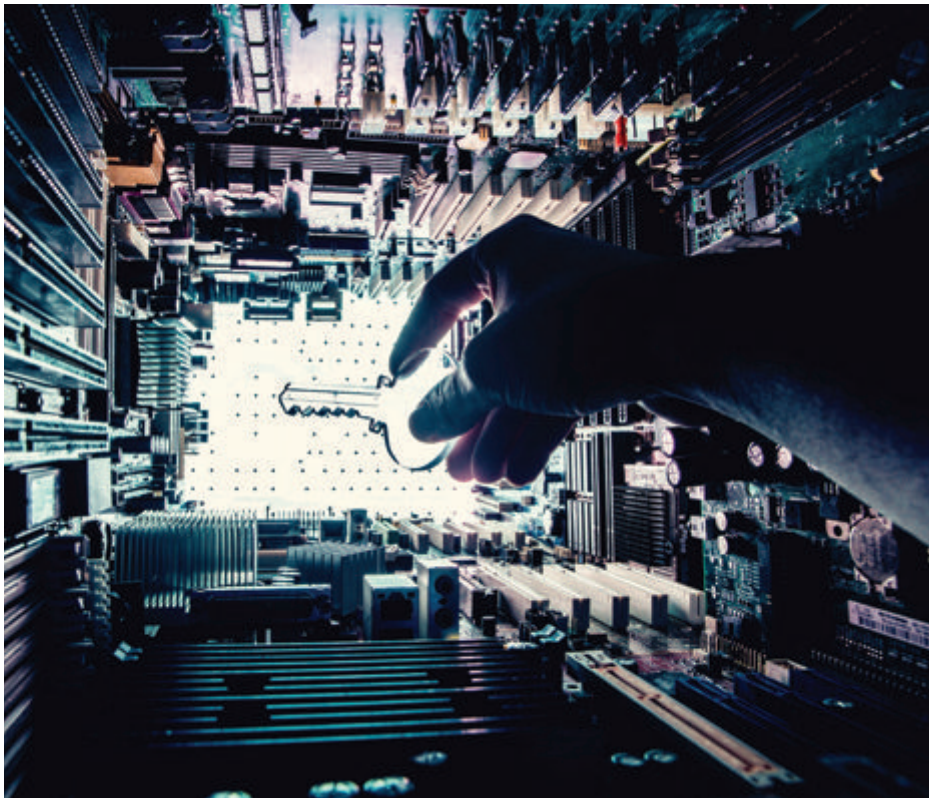
There continues to be an increased number of ransomware events, which has led to this response from the market. As both the frequency and severity of claims have increased, the rates have also increased significantly to compensate. There has been a greater focus from insurers on their clients' cyber risk management and security awareness.

An increase in cybersecurity awareness and risk management will ultimately be beneficial for everyone. The awareness in cyberattacks has also brought an increased interest in cyber insurance. We are seeing more requests for cyber insurance from first-time buyers, as ransomware attacks are no longer viewed as just a large organization concern. Smaller companies have become acutely aware that they too can be targeted.

Ian Fraser: With the Canadian cyber insurance industry loss ratio in excess of 400% in 2020, it is fair to say considerable change is being felt across the marketplace. Similar to hard market cycles experienced in the past across traditional P&C lines of business, the cyber market is in the midst of a hard market, which is yielding significant rate increases, tighter policy conditions and a general reduction in capacity.

As a line of business that began as a frill toss-in grant of coverage years ago, cyber insurance capacity is quickly becoming tactically deployed under a heightened scrutiny of underwriting – and carriers are selective, offering protection to policyholders who can demonstrate best-in-class IT controls and above-average cyber hygiene.

Lindsey Nelson: Obtaining coverage today has become more difficult as the class experiences the first hard market cycle in its history, driven almost exclusively by the



"With the Canadian cyber insurance industry loss ratio in excess of 400% in 2020, it is fair to say considerable change is being felt across the marketplace"

Ian Fraser, Sovereign Insurance

severity of ransomware claims. Canada is further challenged by the fact that cyber is still in its infancy, with the total Canadian cyber market sitting at around $300 million.

There has been a unanimous acceptance in the market that more rate is required to return to a position of profitability – a fact continuously highlighted through the loss ratios expressed in quarterly reports from OSFI – and brokers are experiencing different renewal terms and conditions. Increased deductibles are not uncommon, and in some instances, co-insurance is being applied by insurers as a way of managing capacity provided and ensuring there is mutual investment in avoiding a large-scale attack.

Insurers are using their data to determine what security measures are preventing claims, what industries are more susceptible to cyber risk by exposure alone and ensuring that the price reflects the fact that ransomware events now cost millions, not the hundreds of dollars of years ago. Minimum security measures are increasingly being required before an insurer will entertain providing coverage.

However, it's not all doom and gloom. CFC is more committed than ever to providing a broad cyber product and is uniquely positioned to navigate through a hard market, as we are better equipped to manage claims frequency through our CFC Response app and to manage severity through what is now the largest dedicated cyber incident response team globally.

Miki Ho: If the events of the past year are any indication, cyber risk is set to become the defining risk of our age. Cyber risk knows no boundaries, and we've observed an escalation of attacks on a global scale. This has resulted in a perfect storm for the cyber insurance industry between widespread technology risk, increased regulations, increased criminal activity and carriers pulling back coverage.

In Canada, we are beginning to see cyber and privacy liability capacity constraints as losses have increased, and carriers are beginning to increase their underwriting scrutiny. Until recently, most carriers covered ransomware at full limits. Now that ransomware attacks are frequent and more severe, some carriers have started applying co-insurance and sub-limits on a widespread basis. Given the dramatic shift both to a work-from-home culture and monetization of cyberattacks, the underwriting considerations carriers could rely on from just a few years ago have essentially become irrelevant and outdated.

Despite changing market conditions, Coalition remains an industry leader, with lower claims frequency and loss ratio compared to other carriers. While other companies are making drastic changes, we are holding strong. We have not sub-limited ransomware coverage, added co-insurance to our policy or added exclusions for end-of-life software.

● How have you seen the ransomware threat evolve in recent years, and where do you see this challenging risk headed?

Ian Fraser: Without a doubt, ransomware is the fastest-growing cyber threat vector that keeps most companies' IT professionals and chief information security officers up at night. This is not surprising, given the impact of losing closely held personal and confidential client records, the potential to cause catastrophic financial damage, and the reputational harm to the organization.

The frequency of ransomware attacks has increased exponentially over the last five years, as has the cost. The average ransom fee requested has increased from $5,000 in 2018

CYBER INSURANCE

THE GROWING COST OF RANSOMWARE

Source: 2021 Ransomware Spotlight Report, NetDiligence; all figures in US$

> "There has been a unanimous acceptance in the market that more rate is required to return to a position of profitability"
>
> Lindsey Nelson, CFC

to around $200,000 in 2020, according to the National Security Institute. *Cybercrime Magazine* reports that experts estimate that a ransomware attack will occur every 11 seconds in 2021. This alarming trend is only expected to get worse, and detection and mitigation of these attacks is only getting more difficult.

In addition to a comprehensive cyber insurance policy backed by a panel of InfoSec vendors specializing in pre- and post-breach risk mitigation, breach preparedness and cyber hygiene serve as leading factors that mitigate the overall cost and impact to any business hit with a cyber breach. We know ransomware threats won't go away, so implementing cyber loss control measures and being prepared to navigate through one if – or when – your organization is impacted is the best approach to take.

Lindsey Nelson: There have been two main developments in the evolution of ransomware over the past 12 to 18 months. First, threat actors have switched to data exfiltration – we've seen this in over 50% of the ransomware cases that CFC has managed in this period. Second, there has been a distinct shift to attacks aimed at MSPs or cloud service providers, which has seen more and more small businesses becoming collateral damage.

CFC has seen frequency of events flattening over the last quarter, which we would attribute to the proactive approach that we've adopted – monitoring our policyholders, scanning for external vulnerabilities and informing them where we have detected a match or compromise via our CFC Response app. We have countless examples of clients that we've identified as being compromised, reached out to and remediated, all before they've even realized they might need to file a claim.

Despite the efforts that we and others are making and the positive impact these efforts are having, severity is still skyrocketing. There was a small dip in extortion payments being made by clients in the first quarter of the year, as clients were either fearful of violating sanctions or simply didn't believe that they would get their data back, but the threat actors are evolving, new variants are emerging, and ransomware continues to be a profitable industry for criminals.

Angela Feudo: Ransomware has increased in the number of companies and types of companies being compromised. Ransomware as a service has allowed for an increase in the number of individuals who can launch a ransomware attack. Threat actors no longer necessarily need to be a technically skilled hacker to deploy ransomware because it is now more accessible than ever to utilize.

Individuals and organizations have become more cyber savvy in their defences against cybercriminals, and many have concentrated efforts and resources in creating, maintaining and encrypting backups, as well as focusing on their restoration processes. Due to these efforts, and in the event that files

A good cyber defence is a strong offence

Be proactive. Protecting your organization with the right coverages can be a real game changer. Learn about Trisura's cyber solutions today!

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.

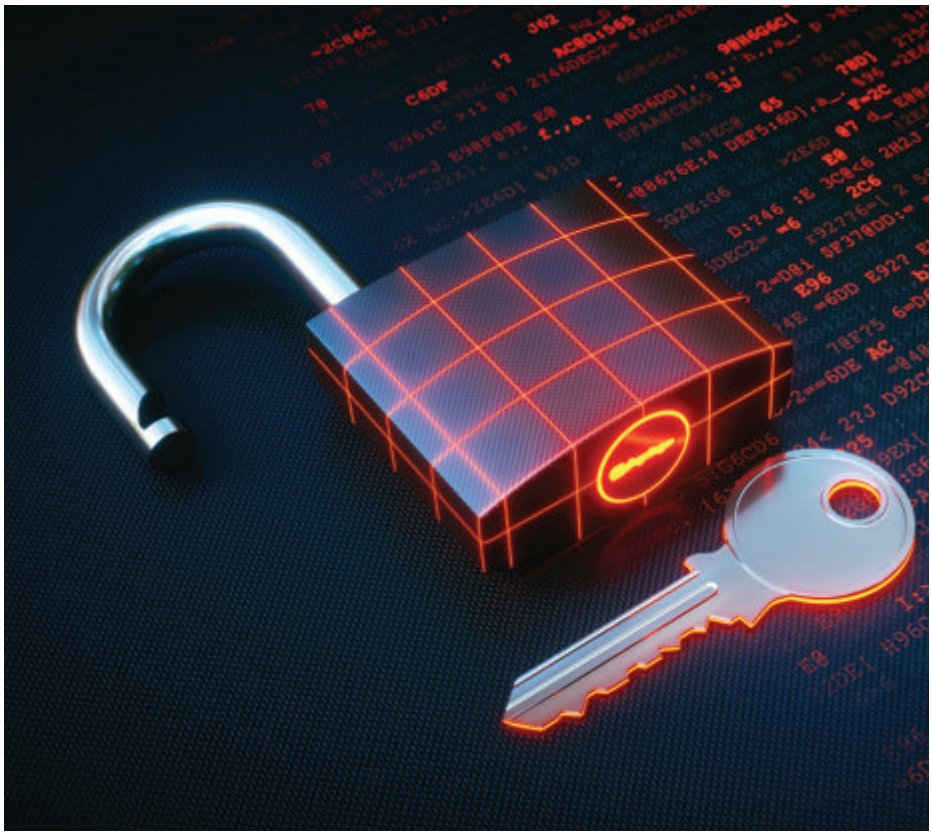
were corrupted, companies didn't necessarily have to pay the ransom.

Threat actors have moved to engaging in double extortion, meaning that the hackers will threaten to release private information if the organization doesn't pay. Threat actors are also using distribution denial of service [DDoS] attacks on their victims to put pressure on them to pay the ransom. Hackers have expanded ransomware into a business model whereby they will use the best method against the victim. This can include encryption, DDoS or releasing private information to cause the most disruption.

Miki Ho: The threat of ransomware has escalated considerably in the past few years. Attack techniques have become increasingly sophisticated and more automated, which has enabled criminals to extort ever-growing amounts from organizations. The average ransom demand made to our policyholders in the first half of 2021 was $1.2 million. That's a large price to pay for any organization – and is a nearly 170% increase from the average demand in the first half of 2020.

"As the business impact of ransomware attacks has grown, so too has the leverage of criminals to demand larger ransoms"

Miki Ho, Coalition



As the business impact of ransomware attacks has grown, so too has the leverage of criminals to demand larger ransoms. The ability to target small businesses through automated attacks and leverage higher ransom demands has also made smaller businesses more attractive targets than they once were.

While the threats of business email compromise, social engineering and funds transfer fraud are still very much present, the cyber insurance community agrees that the hardening of the market is primarily being driven by ransomware attacks. Ransomware remains the most lucrative cybercriminal activity, and the widespread use of poorly secured remote access protocols and tools on the internet will continue to leave organizations open to cyber extortion attacks.

Hackers are getting more specific about who they target and the amount of ransom they hope to collect. They are also using increasingly sophisticated attack techniques and ransomware variants to execute their attacks. As a result, we expect ransomware frequency to increase moderately. While threats continue to evolve, we believe that ransom demands have likely hit their highest levels and will flatten, as there is little additional leverage for criminals to gain beyond taking an organization's operations hostage.

● Which industries are most exposed to cyber risk, and are these industries buying cyber insurance?

Angela Feudo: Any individual and organization that uses the internet is exposed. Some industries and businesses, however, may be at a higher risk. Historically, the focus has been on healthcare, government, utility companies, schools and financial institutions. This has not changed; today, these industries continue to be at a higher risk, for different reasons.

The healthcare industry has many older legacy systems that go unpatched. That,

coupled with holding patient records, makes them an attractive target. Governments, financial institutions and universities also hold a lot of confidential information. The larger organizations in these industry groups have been buying cyber insurance for years. Now the smaller companies are also purchasing cyber insurance more regularly.

We have also seen an increase in claims in the manufacturing, professional services and construction spaces. While there has been an increase in cyber purchases in these spaces, there are still a lot of companies that do not purchase cyber insurance.

Miki Ho: Cybercriminals are opportunistic, particularly when it comes to small businesses, and the technology and processes that organizations use are far more indicative of their risk than their industry. No company is too small to be an enticing financial opportunity for attackers.

Still, some industries did experience notable increases in claims in the past year. From H1 2020 through H1 2021, we saw an increase in claims frequency of 30% for non-profits, 46% for IT and 53% for professional services. Industrial and manufacturing businesses experienced a notable surge, with industrials increasing 263% and manufacturing increasing 99%.

Ian Fraser: Years ago, it was common to hear that the financial services and healthcare industries stood out beyond all others as it relates to exposure to cyber risk. While it still holds true that these segments are considered high-risk, the reality is that companies in nearly all industry segments have exposures that need to be quantified and addressed.

Cyber insurance has been brought to the forefront of nearly all commercial insurance placement discussions as a result of many high-profile cyber breaches, and we have seen most mid-market and large commercial clients purchase it for the first time in recent years. Small and medium-sized enterprise client take-up rates have historically lagged behind that of their larger mid-market and large commercial peers; however, recent data has shown that SME take-up rates have increased sharply in 2020, largely due to an increase in cyber risk awareness on account of COVID-19.

Lindsey Nelson: Any business that uses a computer and has employees is at risk. CFC has countless case studies of policyholders of all shapes and sizes across every industry that have fallen victim to a cyber incident.

However, we're seeing a real difference between those industries that might be expected to have cyber claims and those that are actually suffering from cyber incidents. Public sector, education and not-for-profits are typically assumed to be the largest at risk – and it's true, they have a heightened exposure. This also applies to retail, financial institutions and healthcare. However, the data in the last year points squarely at professional service firms, especially small law firms and financial services businesses.

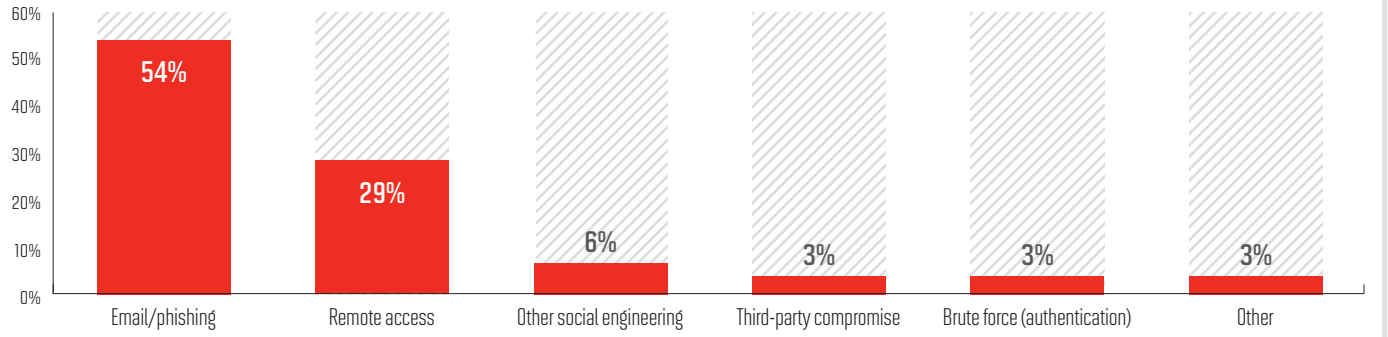
> "The real opportunity for brokers lies in selling to the 85% of Canadian companies that aren't currently purchasing affirmative, stand-alone cyber cover"
>
> Lindsey Nelson, CFC

It appears that professional service firms in Canada have been hit particularly hard, primarily due to the confidentiality of the data they store. Six of the largest ransomware events involved professional service firms that faced demands in excess of $5 million – and given the nature of the data, these firms have a propensity to pay.

In general, small companies consistently fall victim to ransomware attacks. They're less likely to have dedicated security staff and more likely to have flat network structures, with simple access control policies that aren't well maintained.

The pandemic highlighted the need for system continuity, and we've seen a slight growth in new buyers in the Canadian market, but this is still outpaced by organic rate growth. So, as only 15% of businesses are purchasing cyber insurance, the real opportunity for brokers lies in selling to the 85% of Canadian companies that aren't currently purchasing affirmative, stand-alone cyber cover.

MOST COMMON CYBERATTACK TECHNIQUES



Source: H1 2020 Cyber Insurance Claims Report, Coalition

"The better controls a company has in place, the more likely they will be to obtain better terms" Angela Feudo, Trisura Guarantee Insurance Company

How does the hardening cyber market impact insurance brokers? How can they navigate this market successfully and secure the best solutions for their clients?

Lindsey Nelson: Planning is key. Increasingly, the question is changing from what risk measures a client should adopt to get lower premiums to how they can get cyber insurance altogether in the face of shrinking capacity and expectations around minimum security controls in place.

Be prepared to challenge false positives that come from external scans of a client's network that underwriters use to aid their assessment of the risk. These reports are valuable, but dangerous in isolation as a true measure of a client's vulnerability and can often do damage at point of sale when presented to someone in the client's IT function.

Look for stability and consistency in the market – those committed to growing cyber as a class of business and with a Canadian data set built up over years are likely to take a more sensible approach in responding to a hard market. Also look for markets that offer proactive solutions that will respond from the moment their client buys a policy, rather than only providing financial compensation reactively.

Finally, plan ahead and engage with clients to ensure they have the basics in place – MFA for remote access, offline backups and advanced endpoint protection solutions, for starters. Clients won't always want their cybersecurity dictated to them, but where cyber insurers are seeing lack of these controls leading to cyber claims across their portfolios and across a meaningful sample set of clients, this has prompted the market to require companies to make some investment in risk management before transferring entirely to insurance. With the right cyber insurer, brokers can provide both to the client through in-house security teams.

Angela Feudo: The hardening cyber market has created additional challenges for brokers. With markets reducing capacity, it has left brokers looking for replacement markets for those towers. It is now even more important for underwriters to clearly communicate their appetite to brokers so they know who might be a viable option for their clients.

Cyber is no longer just privacy-based; for example, the exposure that a manufacturer has versus that of a law firm is very different. It is critical that insurers understand their client's exposure in order to develop a trusted advisor relationship with their client. It is important for brokers to stay on top of emerging cyber threats, as this will enable them to educate their clients on where the exposures are.

A lot of markets are asking for more underwriting information; understanding where

potential exposures lie allows markets to get ahead of risks and be proactive in preparing the necessary increased security measures. The better controls a company has in place, the more likely they will be to obtain better terms. Better controls are beneficial for the client, as their systems will be better protected from exposure.

With the evolving digital landscape, it can be difficult to stay on top of the market, particularly if you are not a cyber specialist. Finding a specialist you can trust to help navigate the market will help.

Miki Ho: The hardening market and increased capacity constraints are concerning for brokers. Many brokers will have an increasingly difficult time placing cyber coverage, particularly for challenging accounts that require specialized underwriting or security improvements before they would qualify for coverage.

As other markets have pulled back coverage and increased prices, we still see opportunities for cyber insurance buyers who are proactively managing risk to access better coverage and more attractive pricing. Coalition continues to lead the market by offering organizations that implement strong security controls more competitive premiums and broader coverage. In the past year, Coalition launched several new services and software products to help our policyholders proactively manage cyber threats, including pre-breach services, employee training, incident response planning, compliance assistance and IT security services.

Ian Fraser: During a hard or hardening market, insurance brokers arguably have the most difficult job within the insurance supply chain. Acting with a duty of care and responsibility to their clients, insurance brokers are responsible for presenting and articulating their clients' risk exposures to insurers and for negotiating the most favourable terms available for their clients.

To facilitate the best solutions for their clients, it is imperative that insurance brokers are deeply connected into the cyber risk marketplace. Beyond understanding the technical nuances of a cyber insurance policy, an astute broker has a much broader understanding of the cyber risk landscape – including but not limited to common and trending cyberattack vectors – and can successfully articulate their client's cybersecurity risk posture to assist with the underwriting of their client's insurance placement.

● What are the most common cybersecurity attack vectors and breach methods?

Lindsey Nelson: Taking advantage of open RDP ports, which are essentially the digital doors and windows to an organization, is still the cheapest and most profitable attack vector. Threat actors exploit these open RDP ports, and these attacks accounted for over 50% of the cyber claims we saw at CFC last year. However, software vulnerabilities are growing at a faster rate than exposed RDP ports.

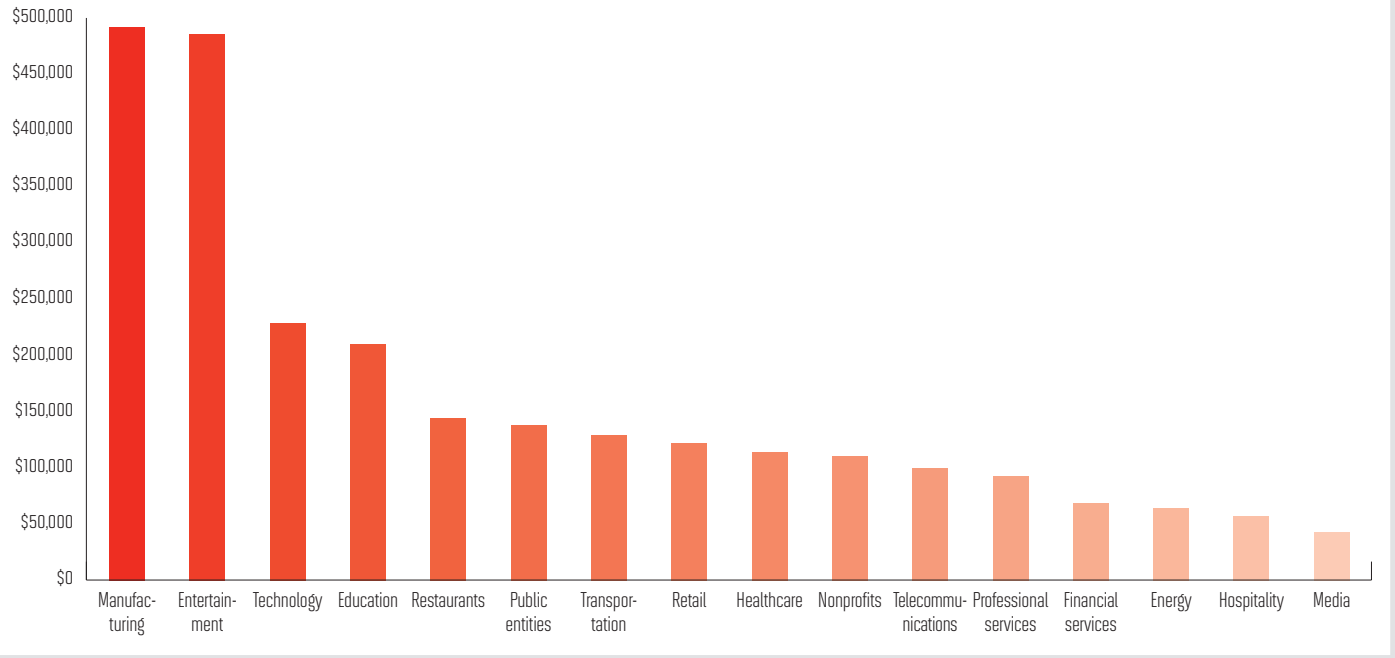
Email phishing remains the simplest to conduct, playing on the human and/or employee error element. Threat actors are capitalizing on remote and hybrid workforces and the susceptibility of employee and human error, enabling them to override any IT security solutions that do work in practice.

While ransomware undoubtedly remains a significant threat and dominates headlines, it's important that brokers remind their clients that theft of funds and business email compromise have not gone away. Nor should reputational harm be ignored. It's become a growing issue as regulations such as PIPEDA oblige businesses to notify customers when their data has been compromised. Reputational harm can include greater and more long-term costs such as cancelled contracts or customers taking their business elsewhere, yet it's a threat and a cost that few talk about when discussing cyber policies.

Miki Ho: While ransomware and funds transfer fraud are the main ways criminals immediately monetize cybercrime, they use a wide array of attack techniques and tactics to gain access to systems in the first place. Social engineering leading to business email compromise, insecure remote access exposed directly to the internet, and third-party

CYBER INSURANCE

AVERAGE CYBER INCIDENT COST BY SECTOR



Source: 2021 Ransomware Spotlight Report, NetDiligence; all figures in US$

"Taking advantage of open RDP ports, which are essentially the digital doors and windows to an organization, is still the cheapest and most profitable attack vector"

Lindsey Nelson, CFC

vendors targeted in supply chain attacks are the most common attack vectors in claims experienced by Coalition policyholders, and all can lead to potentially catastrophic cyber events. So far in 2021, the top attack techniques experienced by Coalition policyholders include phishing (48%), exploitation of vulnerabilities on public-facing applications (27%) and exploitation of insecure remote access (12%).

Angela Feudo: We are still seeing a lot of losses arising from either weak or compromised credentials. Usernames and passwords continue to be exposed in data leaks and phishing scams. When this type of information is stolen or lost, cybercriminals can easily access the company's systems. If an employee uses the same password for both personal and business systems and the individual's password gets compromised on their personal device, the hacker can use this opportunity to hack into the company's system. Having good password hygiene, using multi-factor authentication or even biometrics can help combat this risk.

Phishing continues to be a common method used by hackers, likely because it works. Cybercriminals are expanding on the methods they use in phishing; for example, during the pandemic, we've seen phishing scams where criminals are imitating health organizations or use the guise of providing relief money. Continued employee training, phishing tests and employing the principle of least privilege for access in systems can help to combat this risk.

It is also important to note that not all threats come from humans. Unpatched applications and servers are also a common vulnerability that can leave systems open to attacks. A good example of this is the January 2021 Microsoft Exchange Server attacks, which affected more than 200,000 servers. Although patches were released by Microsoft in March, they did not retroactively

remove any back doors that might have been installed by hackers. Implementing software updates and installing patches as soon as they are available can help mitigate these vulnerabilities.

Ian Fraser: There are countless cybersecurity attack vectors and breach methods to mitigate against, but some of the most common include phishing, denial of service attacks and malware/ransomware.

Phishing is a social engineering attack, which means that a bad actor is playing on your sympathies or trying to convince you that they're someone else – a trusted entity – in order to obtain sensitive data, like your personally identifiable information [PII], financial information or credentials. Threat actors will send fake emails, texts or websites that look like legitimate correspondence to manipulate you into gaining access to information or corporate systems. While cybercriminals most commonly conduct phishing attacks through email, phishing through text messages has recently become more common.

A denial of service [DoS] attack aims to shut down a machine or network, or make a service such as a website unusable, by flooding it with malicious traffic or data from multiple sources – often botnets – or sending it information that triggers a crash. DoS attacks can have a significant financial impact on businesses, both from a business interruption and reputational perspective.

Malware is the collective name for a number of malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network.

Ransomware is a form of malware that encrypts a victim's files, holding their data hostage. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few thousand dollars to millions of dollars for large, complex organizations, payable to cybercriminals in Bitcoin.

● In the growing threat landscape, what are some best-practice cyber risk mitigation tactics that all companies should implement?

Ian Fraser: Incorporating common preventative risk mitigation features such as installing firewalls, MFA, data encryption and least privilege permissions methodologies can significantly mitigate the severity and frequency of an attack occurrence.

However, understanding that breaches can – and likely will – occur is half the battle, and being prepared for such an event is critically important. An incident response plan is arguably the most important risk mitigation tool and provides a set of instructions to help staff identify, respond to and recover from cybersecurity incidents. The goal is to return to normal business operations as swiftly as possible by removing the threat, minimizing damage and preventing similar incidents in the future.

> "Understanding that breaches can – and likely will – occur is half the battle, and being prepared for such an event is critically important" Ian Fraser, Sovereign Insurance

Lindsey Nelson: There needs to be recognition that the cyber risk controls that we should expect of a mid-sized or large corporate firm are going to be drastically different to small businesses, which probably won't have the best controls in place or IT budgets to do so, and that's what is incentivizing their purchase of cyber insurance. Larger businesses, however, have unfortunately taken a similar approach, and there should be an expectation of minimum security controls in place, parallel to what insurers typically ask for on traditional crime policies.

Perimeter security has been at the forefront of cyber insurers' interests, as it's the first layer for criminals to access a victim's network. Mitigation tactics include looking at open RDP ports and only allowing them to open when necessary to allow traffic to flow in and out of the network. Anyone can view this

from the outside with the right websites and browser plug-ins, so it's a quick, valuable tool to demonstrate to clients.

I'd be remiss if I didn't mention multi-factor authentication as well – lack of MFA caused over 80% of the ransomware attacks we managed in the year prior. Even if email/password credentials have been accessed by threat actors, they won't be able to access the network or victim's email without a secondary authentication measure like a one-time password or token on their phone.

The right cyber insurer will have an in-house security team who will be able to help navigate clients through implementing these measures to become an insurable risk.

Angela Feudo: Cyber risk for both individuals and businesses has continued to increase since the inception of the internet. This will only continue to increase over time as we become more connected to the internet and cybercriminals find new ways to take advantage of vulnerabilities. Companies of all sizes are vulnerable to cyberattacks, and they should be taking steps to help mitigate those exposures.

> "Every password we set, tool we use and network we access leaves us exposed and vulnerable to cyber threats" Miki Ho, Coalition

Human error remains one of the top factors in cyber breaches, and so employee awareness training is key to help combat this risk. Multi-factor authentication is becoming a standard security measure that all companies should implement because it improves a company's security by adding an additional step that a cybercriminal would have to breach to gain access to a company's system. Employing a patch management process allows you to keep your software functioning properly and maintain good security posture. Stay up-to-date with the most current security fixes to combat any known vulnerabilities in the software.

Businesses should also have a current record management system, keeping only records the company needs and getting rid of old data that is no longer useful. If you hold the record, you will need to protect it. If all else fails, it will be useful to have current backups of important data. Backup strategies will be different for each company, but the data in the backups should be current, encrypted and stored securely off-site.

Miki Ho: As small and mid-size businesses become increasingly dependent on internet-connected services and applications, they also become a larger target for cybercriminals looking to exploit vulnerabilities in their systems. Every password we set, tool we use and network we access leaves us exposed and vulnerable to cyber threats. Coalition published a Cybersecurity Guide to provide policyholders and brokers with specific and actionable recommendations to protect their organizations.

Increase email security: Email is not a secure form of communication, and every organization should use caution when sending or verifying sensitive information by email. We recommend using a secure email hosting provider and implementing free security measures to enhance email security, including SPF, DKIM, DMARC and MFA.

Implement multi-factor authentication: MFA immediately increases your account security by requiring multiple forms of verification to prove your identity when signing into an application. MFA should be implemented on all critical business applications, such as email.

Maintain good data backups: A good data backup can mean the difference between a full loss and a full recovery after a ransomware attack. We recommend that all businesses maintain backups both on- and off-site for critical business data and test backups by attempting a full recovery.

Enable secure remote access: Remote access creates more risk for organizations and should be implemented carefully.

Update your software: Cybercriminals exploit vulnerabilities to gain access to systems or spread malicious software. These vulnerabilities can be located and patched through regular software updates.

Use a password manager: Password managers help keep track of multiple passwords and generate new ones at random. They are essentially an encrypted vault for

storing passwords that is protected by one master password.

Scan for malicious software: Endpoint detection and response [EDR], a more enhanced version of antivirus software, is an emerging technology that addresses the need for continuous monitoring and response to advanced threats.

Encrypt your data: Encryption is the process through which data is encoded so that it's hidden from bad actors who manage to gain access. It helps protect private information and sensitive data, and it enhances the security of communication between client apps and servers.

Implement a security awareness training program: Through security awareness training programs, every employee gains the knowledge they need to stay vigilant and avoid becoming the victim of a phishing attack.

Purchase cyber insurance: If all else fails, organizations want to ensure they can recover financially from a catastrophic attack. Cyber insurance plays a critical role in providing organizations the financial resources to recover and resume operations after a cyberattack.

● How has the COVID-19 pandemic impacted the cyber risk landscape?

Ian Fraser: Around the world, cyberattacks and their associated costs have skyrocketed during the pandemic. Criminals are attempting to take advantage of the pandemic and aggressively targeting commercial enterprises; small and medium-sized businesses need to be vigilant. According to a new report by IT firm CDW, in Canada, the cost of cyber compromise now averages more than $1.25 million, a 47% increase from 2019. An alarming 99% of businesses surveyed reported a cyberattack between November 2019 and November 2020.

COVID-19 has created new challenges for businesses as they adapt to an operating model in which working from home has become the new normal. Many companies are also planning hybrid work models, so they'll have to stay vigilant about security for both remote work and physical office spaces. There's a specific focus on securing remote infrastructure and internet protocol [IP] solutions because of the work-from-home shift. Companies are accelerating their digital transformation, and cybersecurity is now a major concern. The reputational, operational, legal and compliance implications could be considerable if cybersecurity risks are neglected.

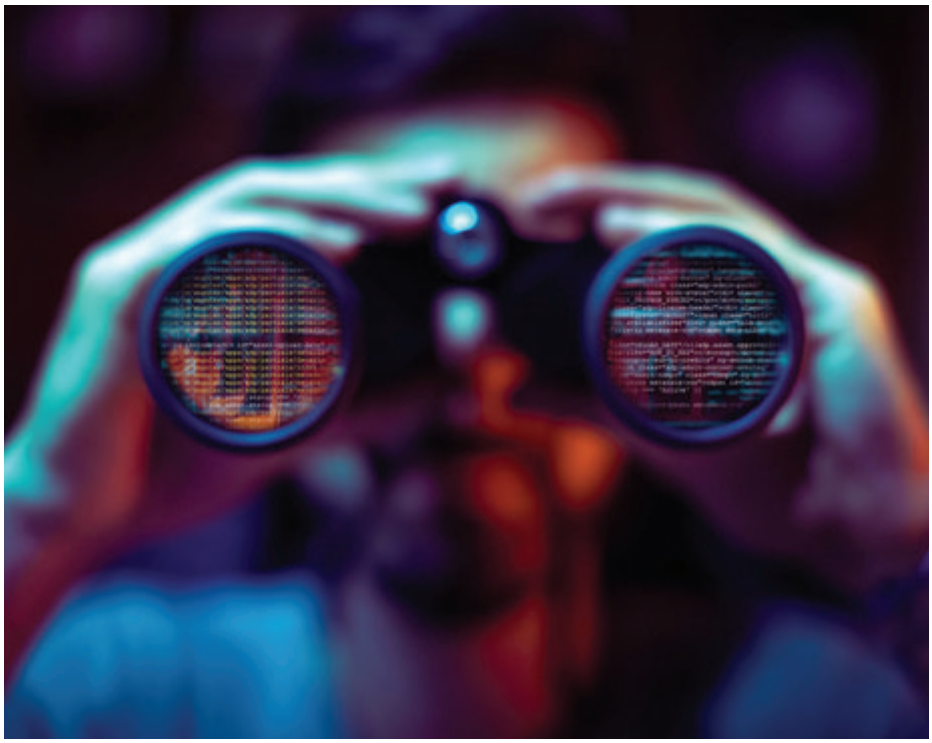
Insurers are grappling to understand how this trend will potentially shift the financial performance of the cyber line of business, and many are allocating considerable resources to quantify new aggregation exposures.

Angela Feudo: Since the COVID-19 pandemic started, we have seen cybercriminals take advantage of people working from home. A lot of businesses did not have the systems or security designed to accommodate the majority of their staff in a work-from-home scenario. As a result, there has been an increase in phishing attacks and malware.

Typically, devices at home are less secure, so multi-factor authentication, a focus on employee training and remote incident response plans are critical. COVID-19 has broadened out the cyberattack surface for cybercriminals to take advantage of due to the increase in employees working from home. Many businesses realized the increase in exposure and invested in IT and additional cyber controls to help manage this risk.

It is also important to look to the future of post-pandemic business models. It is expected that more businesses will allow for a more flexible workplace, whether that be a full work-from-home model or a hybrid that could include desk sharing. Technology, security and employee awareness training plans will need to be updated to ensure the best cybersecurity hygiene is in place for an organization. It will also be important to refresh the organization's incident response

CYBER INSURANCE



plan to include how the company is currently conducting their business and where their employees are located.

Miki Ho: In 2020, as many businesses were forced to transition to remote work, they often settled into the ease and reliability of remote working environments. Because there was a rush to get up and running quickly during the pandemic, security risks were often overlooked. It's easy to forget that what makes it easier for employees to access their accounts and sensitive information remotely also makes it easier for hackers to target and access the same information. The rapid change in how we work gave threat actors access to a largely untapped pool of new targets, and they were often able to remain undetected for longer periods of time when planning their attack strategy.

Remote desktop protocol [RDP], which enables the user to connect to a Windows computer remotely, has many inherent security risks. The rate of Coalition policyholders who experienced a claim due to exposed RDP increased from 29% to 40%, and the severity of these incidents increased by 103%.

Another unfortunate result of widespread reliance on remote capabilities were several noteworthy supply chain attacks, systemically crippling hundreds, if not thousands, of businesses simultaneously, such as the SolarWinds and Kaseya incidents.

Lindsey Nelson: COVID-19 has increased awareness as businesses were forced to critically look at internal practices and transform IT security – or lack thereof – in the shift to remote working. We've seen a surge in demand for cyber policies not only due to the perceived increased exposure, but in response to rapidly hardening market conditions with limited available capacity.

We see two main trends to watch out for. First, cyber events are increasingly a small business issue. Recent statistics show that more than 70% of ransomware incidents impact companies with fewer than 1,000 people and less than $50m in revenue. This resonates with CFC's cyber claims experience. Small businesses are the low-hanging fruit due to their lack of security resources and vulnerability or are becoming collateral damage in larger attacks aimed at MSPs or cloud service providers.

Second, cyber insurance and security services are increasingly merging into one. The cyber market is going through a lot of change at the moment, and it's clear insurers will struggle to compete if they don't have a fully integrated suite of risk management services built into their product.

CFC has a cyber threat analysis team who continuously monitor policyholders, scanning for external vulnerabilities and informing clients where we have detected a match or compromise. We believe that this function truly represents the future of insurance; we've got countless examples of clients that we've identified as being compromised, reached out to and remediated, all before they've even realized they needed to file a claim. Our whole philosophy is that a business will be less of a risk as a cyber policyholder than they will be uninsured.

● What other cyber risks are lurking on the horizon?

Lindsey Nelson: If only we had a crystal ball! The long and short of it is that criminals are going after companies that are vulnerable

as the path of least resistance, rather than the ones that are valuable.

The risk environment itself is likely to evolve as cybersecurity becomes a national security priority and government and regulatory bodies start taking action and enforcing sanctions penalties against businesses that pay demands or require mandatory reporting by those companies who do.

Cyber capacity will be tighter in the next year than it ever has been in its existence as a product line. Those markets that are left will still be writing cyber because of the threat analysis and proactive work they provide clients to prevent incidents from happening in the first place.

Policyholders are likely to see insurers limit the capacity they're willing to provide on extortion cover, either through sub-limits or co-insurance provisions, but brokers have an excellent opportunity to use this to speak to clients upfront about the full limits that typically are available for system rebuild costs should they choose not to pay a demand, and get commitment from clients ahead of an incident as to what their decision will be to avoid paying in the first instance.

Ian Fraser: Cyber threats are constantly evolving, employees will always be subject to human error, and it can sometimes feel like criminals are always one step ahead – so it's important to be aware of, and prepared for, new and emerging risks.

Some of the top cyber risks lurking on the horizon include 5G – simply put, by replacing hardware with software, you introduce an increased risk of data compromise. The proliferation of IoT interconnected devices poses the risk of insecure communications and data storage, as well as the increased potential for devices to be compromised, causing confidential data to be accessed. Quantum computing presents a potential to break current forms of encryption, requiring organizations to explore new ways of encrypting and protecting their data.

Finally, there's the growth in popularity of the cryptocurrency market and the absence of government regulation – the anonymity that cryptocurrency provides for ransomware payments is fuelling growth of this attack vector to troubling new heights.

Miki Ho: At Coalition, we have unique insight into the cyber threat landscape and its impact on our policyholders. We expect the market will continue to evolve as losses develop, new threats emerge and attacks become more severe. Our claims, incident response and insurance teams share the following predictions for the remainder of 2021.

Ransomware will remain the single biggest threat for all organizations. Ransomware remains the most lucrative cybercriminal activity, and the widespread use of poorly secured remote access protocols and tools on the internet will continue to leave organizations open to ransomware attacks. As a

> "Criminals are going after companies that are vulnerable as the path of least resistance, rather than the ones that are valuable"
>
> Lindsey Nelson, CFC

CYBER INSURANCE

result, we expect ransomware frequency to increase moderately. Conversely, we expect that ransomware severity will flatten, as there is little leverage left to be gained beyond what criminals already have after taking an organization's operations hostage.

The cyber insurance market will continue to harden throughout the year. It will be harder to qualify for cyber insurance, and the implementation of many common cybersecurity controls will increasingly be required as a condition of coverage. We predict that many insurance carriers will also begin to require companies to address identified vulnerabilities during the policy period or risk losing some – or all – coverage. Price increases, co-insurance and sub-limits on critical coverages are already happening and will continue throughout 2021.

Supply chain attacks will be more common. Criminals will increase their targeting of software and service providers that other organizations rely upon. Supply chain attacks allow criminals to victimize a large number of organizations at once, rather than just one. As organizations increase their reliance on cloud software and service providers, they open themselves up to more risk – risk they will struggle to control.

Criminal attacks will follow nation-state attacks. Several high-profile attacks over the past year, including against Mimecast, SolarWinds and Microsoft Exchange, were believed to be instigated by nation-state actors. While these attacks are typically motivated by espionage rather than financial gain, the exploits used often eventually make their way into criminal hands, as evidenced with the Microsoft Exchange vulnerabilities disclosed earlier this year. We expect this trend to continue.

Angela Feudo: Cybersecurity staffing shortages are a concern for businesses and the insurance industry. As the number of attacks grows and the demand for cybersecurity professionals increases, there has been a continued decrease of cybersecurity staff. According to an article from CNN, there are approximately 3.12 million unfulfilled positions globally. With unfulfilled cybersecurity positions, businesses are more vulnerable to breaches.

> "Cybersecurity is a global concern, not only because hackers can reside anywhere in the world, but also because they can use other companies' systems to breach yours"
>
> Angela Feudo, Trisura Guarantee Insurance Company

Cybersecurity is a global concern, not only because hackers can reside anywhere in the world, but also because they can use other companies' systems to breach yours by utilizing DDoS, man-in-the-middle attacks and cryptojacking techniques. Cybersecurity should be a group effort against cybercriminals.

Additionally, as 5G – which is faster and can support more devices than traditional networks – continues to expand, it will increase the cybersecurity risk, as there is much more software being used in the network, and therefore the attack surface has expanded. The increased speed of 5G, while beneficial to users, can prove to be a challenge for cybersecurity professionals.

With its ability to support more devices, 5G will allow for more IoT devices. Not all IoT devices are manufactured with security in mind. With billions of IoT devices connected, all with mixed security levels, there could be potentially billions of breach points.

sovereign secure™
techpro

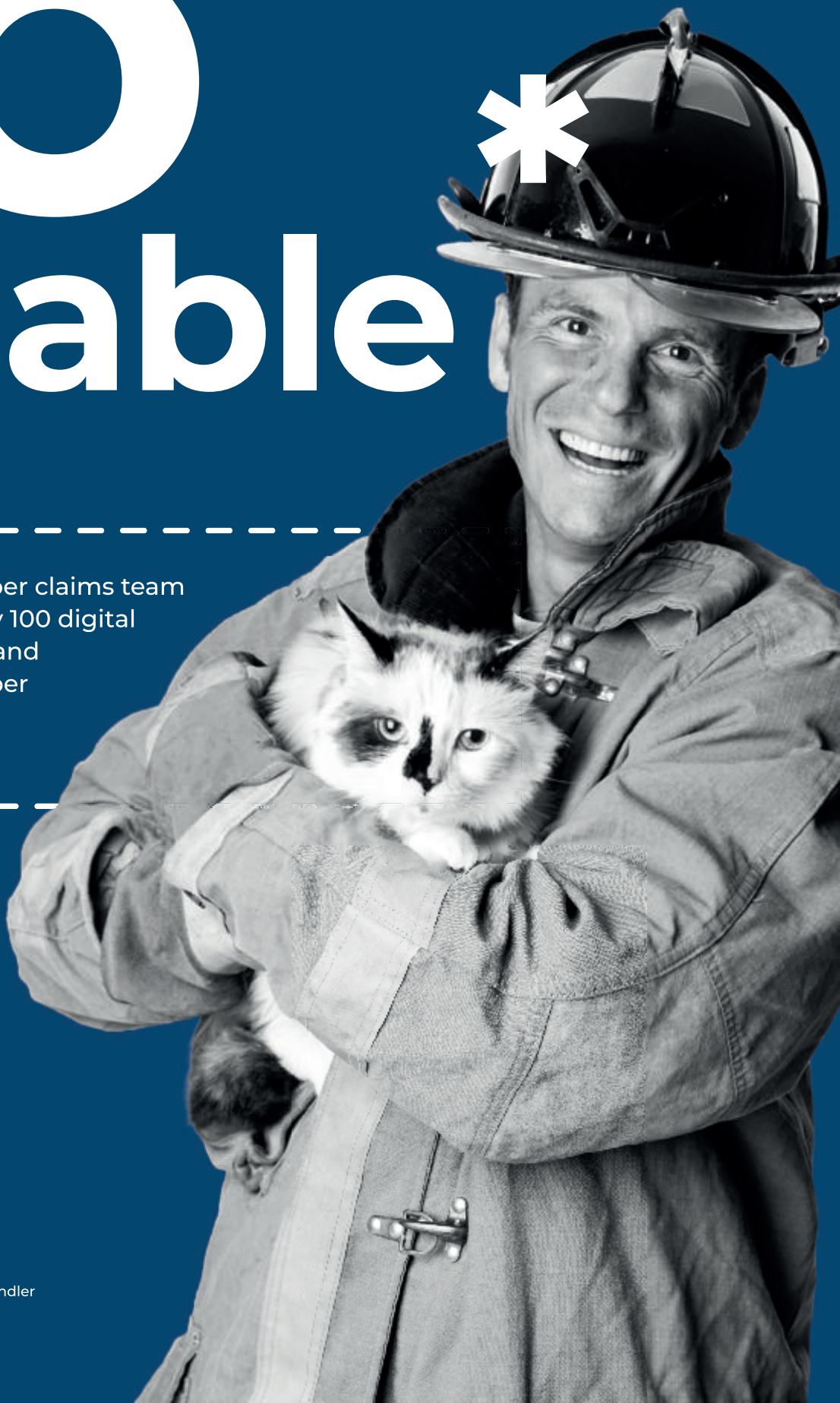
More precise, comprehensive, and flexible Cyber/Tech coverages designed to address the unique and emerging risks to Canadian businesses.

Visit sovereigninsurance.ca to learn more.

sovereign®
INSURANCE

So reliable*

Our in-house cyber claims team consists of nearly 100 digital firefighters on hand to rescue our cyber policyholders in times of trouble.



cfc

*Not an actual CFC cyber claims handler