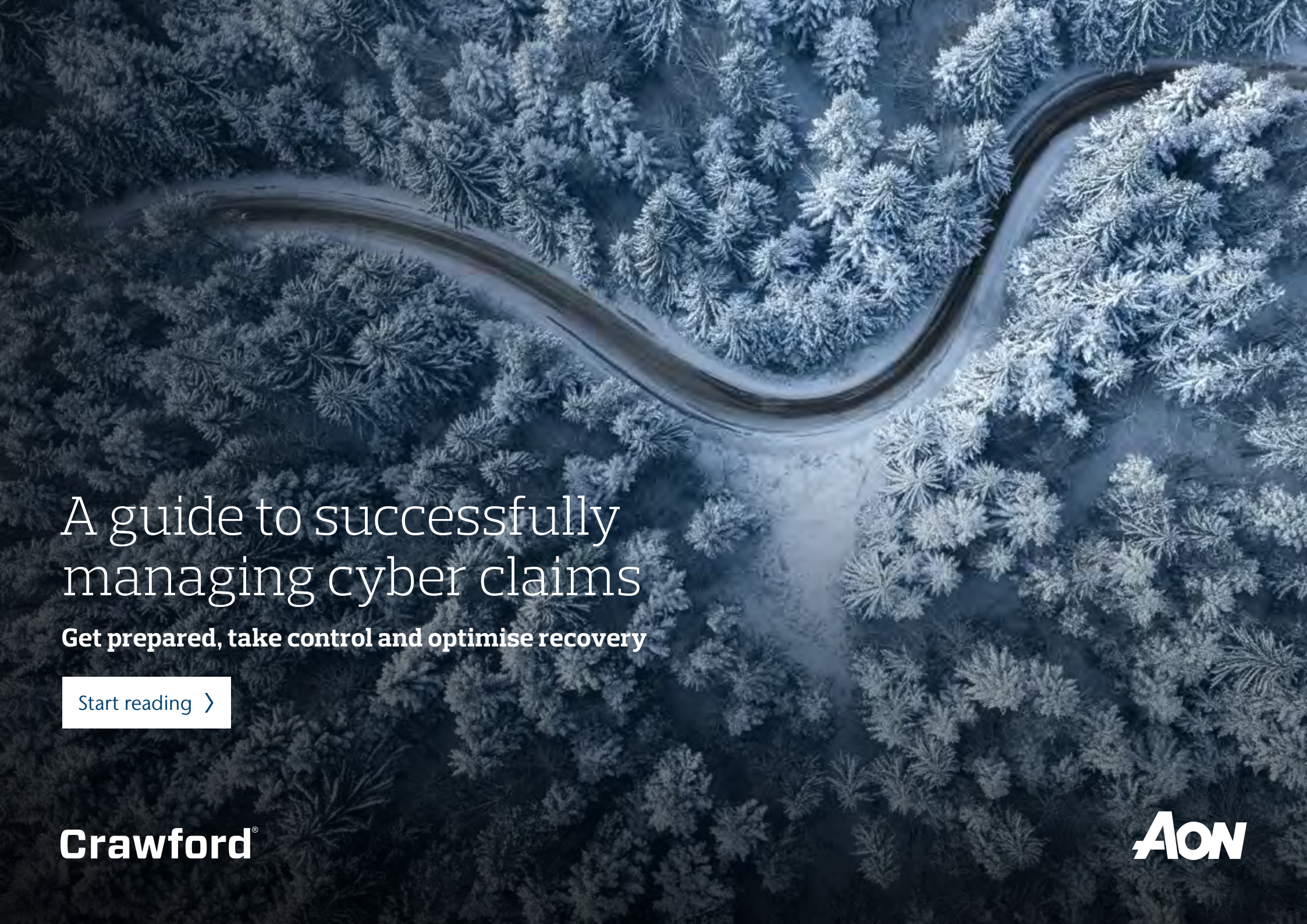

A guide to successfully managing cyber claims
Get prepared, take control and optimise recovery
Start reading
Crawford®
AON

Introduction

Managing and mitigating a changing cyber threat

The cyber threat environment continues to evolve and change at a rapid pace. In the relatively short history of cyber risk, the rise of ransomware has been the quickest to evolve as threat actors have realised they can profit more by threatening to disrupt the operations of a business, than they can by simply stealing confidential data alone. Cyber criminals have become more sophisticated and now understand the economic pain points for different types of organisations and are learning how to leverage these to maximise their financial return.

Against this challenging backdrop, cyber risk was ranked as the number one current and predicted future risk globally in Aon's 2021 Global Risk Management Survey. As organisations respond to this mercurial threat by reinforcing their cyber defences using methods such as investing in IT security, improving employee awareness — human error is still the main route in for cyber criminals — and electing to transfer risk using insurance, the possibility of experiencing a cyber related business interruption continues to be a significant concern.

The use of ransomware has changed in recent years. Used initially just to disrupt a business, this tactic aadd the exfiltration of data — such as Personally Identifiable Information (PII) and confidential business information — from the businesses they attack, their customers and business partners.

1 Colonial Pipeline: US recovers most of ransom, justice department says - BBC News 2 Meat giant JBS pays $11m in ransom to resolve cyber-attack - BBC News 3 US companies hit by 'colossal' cyber-attack - BBC News

While the model of stealing and selling PII in its own right has declined because it is getting harder to monetise (these records have little value on the dark web), an organisation facing the threat of having to disclose to clients that their valuable data was exposed, or inform regulators that millions of PII records were released, is willing to pay to prevent this from happening.

Threat actors have also improved the technology around ransomware, making it more difficult for organisations to restore compromised systems from back-ups. They are targeting organisations whose disruption impacts other businesses that cannot wait for the victim organisation's back-ups to be restored. Attacks on Colonial Pipeline[1], JBS[2], and Kaseya[3] demonstrate the impact an attack can have on the supply chain. It's not just the organisation's own business interruption, but the potential damage caused to customers and business partners, that also raises the stakes.

It's against this uncertain backdrop that this guide — drawing on the deep knowhow of Aon and Crawford cyber incident and claims experts globally — seeks to shine more light on the potential threat for organisations and, just as importantly, help them to mitigate the risk and understand how, if an incident should happen, they can manage their cyber insurance claim as effectively and efficiently as possible.

A cyber insurance claim may share similarities with a more traditional first party property or third-party casualty claim particularly given the growing focus on spiralling business interruption costs. However, the issues are more complex and there are pitfalls to navigate in order to ensure an organisation can maximise the benefits of its insurance policy.

We hope you find this guide a useful contributor to your organisation's preparedness in the event of a cyber claim.

Section 1: The growing cost of business interruption from cyber attacks

Section 2: Prevention and preparedness

Section 3: Control and containment during the response

Section 4: Cyber claims case studies

Section 5: Lessons learned from managing cyber claims

Next steps

Section 1

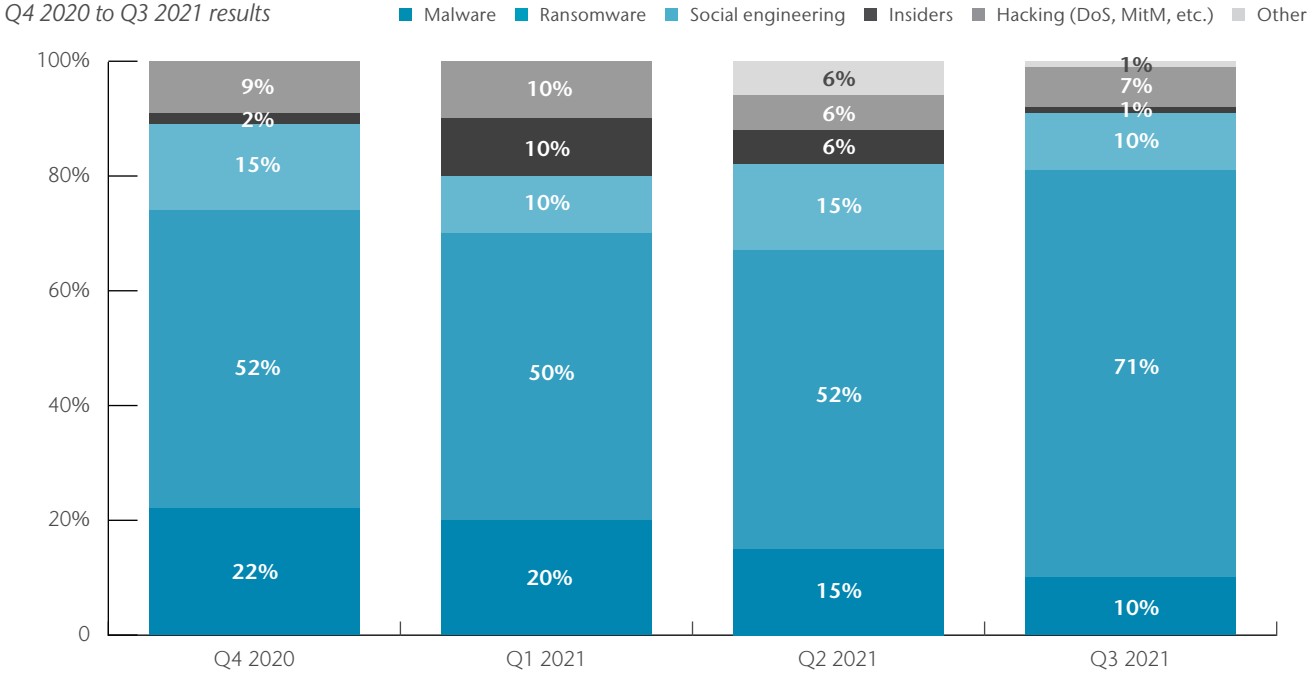
The growing cost of business interruption from cyber attacks

Throughout 2020 insurers reached a tipping point as loss frequency and severity outpaced cyber rate increases, and cyber criminals exploited the distraction and disruption sewn by COVID-19.

Aon recorded a typical cadence of three new cyber matters per business day globally throughout 2020 — a near 100% rise from 2019[4] — while the average loss severity climbed in each quarter of 2020 and, in many cases, became eight figure losses. This chart shows that ransomware remains the vector attributed to the highest % of losses suffered by insurers in 2021.

Portion of losses attributed to threats and vulnerabilities

Q4 2020 to Q3 2021 results



Source: Aon Global Cyber Broker Survey Q3 2021

4 https://www.aon.com/cyber-solutions/thinking/aons-errors-omission-cyber-insurance-snapshot-a-focused-view-of-2021-risk-insurance-challenges/; https://www.aon.com/cyber-solutions/thinking/aons-cyber-insurance-snapshot-emea/

An increasing focus on business disruption

The big driver behind this rapid inflation in loss frequency and severity is the widespread use of ransomware. Whilst the criminal focus had been on getting hold of PII and personal health information (PHI) for identity theft, organised criminal groups have realised that it is more lucrative to not only stealing data, but also effectively disrupt an organisation by disabling its IT systems and operations, and extort a large ransom payment. To achieve that aim their attacks have become more sophisticated and targeted, while they have also professionalised and commoditised their offerings for use by others via models like Ransomware as a Service (RaaS)[5].

Threat actors realised that exfiltrating data and holding that to ransom was more effective and lucrative than deploying ransomware alone. Business interruption costs can be exacerbated by the costs associated with PII getting into the wild — there's the cost of notifications, for example — plus there is the potential for regulatory investigation, fines, penalties, and the potential for victims to be granted statutory standing under new data privacy laws, leading to class action lawsuits.

Extraordinary leverage over victims

All of this provides threat actors with extraordinary leverage over the victim organisation that either feels they have the choice of paying the ransom to "cover up" the fact that the data has been stolen, or paying the penalties associated with publication and face the consequent litigation, reputational harm and other legal consequences. In addition to PII, there are potential costs associated with the loss of confidential business data of the victim organisation as well as customers and business partners — the impact of having confidential information in the market can lead to third-party lawsuits as well as loss of business and loss of customers — which may lead a business to pay a ransom.

Ransomware damage costs spiral

To further understand just how big the problem has become in such a short time, it is worth taking a moment to look at insurers' results, with US insurers reporting loss ratios of over 72% for standalone cyber insurance in 2020, versus just over 47% in 2019[6]. Global ransomware damage costs are predicted to reach $20 billion this year, 57 times higher than five years ago[7].

How this looks in practice can be seen through the numerous examples of major cyber attacks in recent years where we can identify two forces at play. Firstly, there is the damage that a cyber incident can do in terms of harm to business operations, as illustrated by NotPetya (FedEx reported costs of $400 million[8], Mondelez — $188million[9], while Maersk lost between $200–$300 million when an outage left it unable to process shipping orders[10]) or the Colonial Pipeline attack[11], and all the knock-on effects throughout the Northeast US. Secondly, there is the extortion demand that is leveraged primarily against that level of damage potential, plus reputational damage, liability to and loss of clients, and regulatory penalties. A combination of these factors led Colonial to pay the extortionists $4.4million[12] and JBS meatpackers to pay $11million[13].

5 Ransomware as a service (RaaS) is a subscription-based model that enables affiliates to use already-developed ransomware tools to execute ransomware attacks. Affiliates earn a percentage of each successful ransom payment. Ransomware as a Service (RaaS) is an adoption of the Software as a Service (SaaS) business model. 6 http://thoughtleadership.aon.com/Documents/20210609-2021-cyber-market-update.pdf
7 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/ 8 FedEx-Annual-Report-2018.pdf (q4cdn.com)
9 7b15afc8-5461-4f7d-a80a-b03b61b6efa5 (mondelezinternational.com) 10 https://investor.maersk.com/static-files/5d68faa5-f869-4c08-8a1d-9660fe889360
11 Colonial Pipeline: US recovers most of ransom, justice department says - BBC News 12 Colonial Pipeline: US recovers most of ransom, justice department says - BBC News
13 Meatpacker JBS says it paid equivalent of $11 mln in ransomware attack | Reuters

Scale and speed of an attack

For organisations, the scale and the speed to which they can be impacted from a cyber incident has dramatically escalated from the days when data theft was the main goal, and business interruption has become one of the major risks from a cyber breach. Prior to the deployment of sophisticated ransomware, it was unimaginable that a whole operation with multiple sites around the world could come to a standstill from one threat actor.

Natural catastrophe risks like wind and flood, or traditional perils such as fire or terrorism can shut down one manufacturing facility for a single organisation, or perhaps a couple at the same time depending on their proximity. However, these traditional risks do not possess the destructive and all-encompassing infiltration of a well-coordinated ransomware attack. While the attack itself can be limited in time to perhaps a week or two of system encryption, the longer-term operational interruption can extend to weeks through a full network restoration, as organisations balance crisis response and customer service against lost production and sales. Moreover, there are risks of aggregation and accumulation of ransomware exposure i.e. multiple sites reliant on the same technology (aggregation) or multiple sites being impacted by the same event (accumulation).

Threat actors are looking for efficient ways to leverage or magnify their efforts by targeting the software /data supply chain (NotPetya, SolarWinds, Accellion, Centreon), but also manufacturing, including vital resources (such as gas, food) or targeting data-rich environments where the consequences of a breach are magnified by the social impact (such as hospitals, municipalities), or the sheer number of individuals impacted (such as school districts, healthcare) or the high value / sensitivity of data (such as professional services).

The rapid scaling of technology all along the value chain — particularly with many organisations changing their business models in response to the pandemic — has helped to create an eco-system of interdependencies which can be ruthlessly exploited by cyber criminals intent on causing extensive financial and reputational damage. When the game was just about PII, hackers would focus on those businesses who had rich data seams to mine – which was why sectors like retail, health and financial services were often in the firing line and sectors like manufacturing, food and beverage, and construction were not – but now, the criminals have become more sophisticated. They understand the economic pain points for different types of organisation and are learning how to leverage those to maximise their own financial gain.

Disrupted operations

Major operational risk from a cyber attack with the ability to take down entire networks applies to almost every organisation. Many potential victims — such as manufacturers who have perhaps never had big databases full of valuable client information and never saw themselves as targets — may not have taken the same precautions against possible cyber attacks that other sectors prioritise. As a result, they may find themselves behind the curve in securing their systems from attacks even though their automated systems from material inventory, through to production systems and logistics, can be hugely vulnerable.

Manufacturing systems, for example, are reliant on enterprise resource planning software to be able to functionally operate interconnected and seamlessly. If malware intrudes the network environment, these software programmes may be arrested, creating a halt to production or operations. Organisations stress test for continuity strategy, but are they prepared for the same enterprise system(s) — which multiple global facilities rely on — being affected?

Often, organisations suffering a cyber attack have to switch to manual processes at reduced efficiency and increased operating cost to protect a fraction of revenue. It's not even rare to find organisations handling business activity outages without ready disaster planning in place, further exposing them to wider operational and reputational risk.

From a loss perspective, it means that a successfully targeted organisation could easily find itself either having to pay a big ransom and have some business interruption loss, or potentially suffer an even bigger business interruption loss if electing not to pay the ransom and attempting to recover its encrypted systems itself. The economics of that decision are thrown into sharp relief by the Norsk Hydro incident; Norsk made a stand on principle and suffered a loss of at least €75 million[14]; whereas if they had elected to pay the ransom the overall cost could have been materially less through faster remediation of systems and reduced loss of revenue.

Changing claims impact

What does this change of emphasis from a cyber attack mean from an insurance claims perspective? Importantly, it's vital to recognise that understanding the cause and assessing the period of disruption requires additional accounting and IT forensics.

A cyber attack is generally not a one site incident and the onus is on the insured to aggregate their total global losses for presentation of their claim in as much detail and quality as necessary, to help insurers and loss adjusters comprehend the loss for accelerating how the claim is reviewed and paid. The geographic impact can be a significant driver in how long it takes for recovery, but how should they treat the period of restoration? When do they determine an organisation is fully up and running again? While there is an immediate impact and costs related to managing the crisis and recovery, what about revenue losses related to lost sales and longer-term reputational damage as clients turn to other suppliers?

Wordings also vary greatly in the extent to which the insurers treat the "restoration period". Some, but not all, grant varying periods of indemnity beyond the period of restoration that recognise the possibility of loss impact that goes beyond the point when systems are "back up and running"; while others will only cover interruption for the period when systems are actually impaired.

14 https://www.hydro.com/en-NL/media/news/2020/fourth-quarter-2019-firm-response-in-weak-markets/

Manage business interruption complexity

The challenge to insureds is working through the losses incurred across the organisation in a way that comports with the insurance policy language. Different business models mean it can be a lengthy process and it can be difficult for insureds to collect the necessary supporting documentations to prove the loss. Many organisations aren't aware of this complexity, simply expecting that it's enough to provide some high-level financial records. If there is a cyber attack, the ramifications can lead to a catalogue of unseen costs; many employees will need to work longer hours to rectify the situation, for example, and the opportunity cost of work lost elsewhere needs to be accounted for. These additional costs or losses could be evident in numerous operating jurisdictions of the insured which are also reliant on the same platform systems that run the organisation.

Calculating cyber business interruption losses is an intricate process; using a mix of empirical data and evidential factors to demonstrate the impact. While the concept for cyber is similar to a property claim, it's generally more complex considering the multiple geographies that may be affected by the incident, and with organisational interdependencies to consider. It should not go understated that as much as insurers want to support an insured through their recovery, substantiating financial losses is still a requirement to validate any indemnification.

Understand the process

With cyber related business interruption such a costly and potentially ruinous expense, organisations should not only focus on the prevention of the risk, but also on the preparedness in the event they become a victim. Organisations can do this by understanding the claims process. They should know who is involved and be ready to work with their broker, loss adjuster, insurer and other partners to manage the process to optimise the outcome both in the immediate crisis phase and in the recovery.

Section 2
Prevention and preparedness

The best defence against any sort of cyber incident — not just ransomware — is, of course, to prevent it happening in the first place. Understanding an organisation's core operational risks is key as is knowing, if subject to an attack, which part of the business is likely to be exposed, and how that exposure could inhibit revenue generating operations. An emphasis on pre-loss investment in IT security — adopting practices like multi-factor authentication[15] and privileged account management — and really understanding the risk and mitigating controls should be at the forefront of an organisation's prevention strategy.

Recent attacks such as SolarWinds, Hafnium, and Kaseya show that whereas organisations may have previously thought that they might have weeks or even months from finding out they are vulnerable until they have to implement an IT security change, they may well only have days if not hours before attackers start the attack. Many organisations are not prepared for that pace of IT security change management and flexibility.

15 Coveware's blog of June 24 2021 states: "Coveware has NEVER seen a ransomware attack, where domain administrator credentials were compromised after multifactor authentication (mobile, not token based) was overcome. 100% of ransomware attack victims LACK true multi factor authentication for the domain administration accounts https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports *16 Aon's 2021 Cyber Security Risk Report*

Pre–planning is vital

No organisation — however well defended — can assume it is bullet proof when it comes to cyber, which means that preparation and routine iterations to a business continuity plan or an incident response plan prior to an incident are crucial and will have a direct impact on the ability to recover operations quickly. Part of the reason for many recent cyber losses is that the 'traditional' business continuity plans that were designed to mitigate the revenue-at-risk associated with a fire, flood, or labour dispute for example, were not intended to manage the complex or systemic (aggregation) nature of cyber triggered disruptive losses. This is leading to longer downtime and greater revenue loss. Aon's Proprietary CyQu data suggests that two in three organisations have not developed cyber ready business continuity plans[16].

Organisations must instil a preparedness posture towards cyber events and the potential exposures: deciding how involved all management parties will be following an incident; and what vendors will be called upon for specialist help in a crisis such as IT forensics, forensic accounting, legal (breach counsel) and communications.

Getting protocols in place and ready to go when an incident does occur can be vital to ensure the organisation isn't losing valuable response time trying to identify and source expertise to form a response team. That means, given everything happens very quickly, it's important to have organisational acknowledgement that cyber incidents could happen, and the right specialists should be identified or engaged beforehand. It can be a differentiator and big part of the planning process to have agreements in place – and insurer's approval if necessary — for the first responders.

Establish a risk management framework

Part of the preparation should also be focused on pre-scenario planning to understand how the organisation would be impacted by a cyber attack. What happens, for example, if a critical enterprise resource planning system or other operating system goes down, or is taken down due to a critical vulnerability? This knowledge helps to create visibility and collaboration around potential weaknesses and can help make sure organisations are in the driver's seat during an incident; making informed rather than reactive decisions.

Table top exercises are invaluable in helping think through the possible consequences of different scenarios from data breach to ransomware. Incidents are often far more significant and impactful than organisations anticipate and the conclusions from 'wargaming' scenarios can lead, for example, to carrying out honest assessments of a back-up process; what happens if attackers hit the back-ups and encrypt or delete them?

Vulnerability scans are another useful tool, not used often enough, to uncover some of the most likely ways for hackers to find their way into a system, particularly given the increasing exposure for many organisations to ransomware attacks from the widespread use of remote desktops in the pandemic era.

Tools like table top exercises and vulnerability scans help to establish a better framework for understanding what type of incident response is needed as well as helping to ascertain whether the cyber insurance policy in place fully aligns with the identified risks. How would the insurance policy respond in the event of a cyber attack? Is there a need for a deeper dive into the business to see if the wording is clear from a coverage perspective and the limits are suitable given the exposure? If the consequences of a particular incident are likely to create business interruption, for example, will the policy provide sufficient financial protection for what could be a hugely impactful event on the balance sheet? Too many organisations buy a cyber policy before clearly understanding what IT assets their business relies upon, and how an attack on them could result in that worst case scenario.

Review cyber policy wording

It's possible that a cyber insurance policy — where most wordings have historically been developed for a data breach scenario rather than operational disruption — may not fully respond because the maximum indemnity period is too short for the ensuing business interruption. If the policy lists a 90- or 120-day indemnity period (or even worse sometimes as little as 30 days — many cyber policies specify that the period of indemnity ends at the earlier of either the time taken to restore systems or 90/120 days) — what happens to organisations who aren't able to restore systems within that period, or who suffer a downturn in revenue months after an attack was resolved? This can impact organisations with business models where revenue is actually incurred at a later date, for example those who enter into contractual relationships with performance and payment over the course of the contract, or who have a long tail between taking orders and providing the product or service and collecting revenue.

Some policy wordings can be restrictive by covering business interruption losses occurring only during the actual time that an organisation's systems are down — the period of restoration. While systems may be able to return to partial operation, the ensuing restoration period must be considered for indemnification. Losses beyond that relatively narrow period of the exact outage may fall short of the total organisational impact. If a customer went to an alternative supplier, for example, those associated lost sales may exceed a 90-day indemnity.

The period of indemnity / restoration is just one area in which insurance policies may inhibit the opportunity to fully recover. Despite efforts to the contrary, policy wordings can sometimes be found open to interpretation, which penalises those organisations who only examine it closely after an attack has happened. Pre-planning should include a thorough review of the policy to identify areas where additional steps may be needed to provide further protection.

Prepare the claim

Once an incident has been notified, initial claims preparation and project management is a critical phase. This process will start to look at what the probable losses are, framing the incident in line with the policy and insuring agreements. A skill here, particularly given the complexity of a cyber incident, is in organising how losses are compiled and presented so they are more digestible to the insurer, making sure the appropriate vendors are engaged. It's also critical that organisations adhere to the policy provisions with respect to engaging vendors and incurring expenses.

Experiencing a financial impact during a cyber incident and having a cyber policy does not guarantee insurance reimbursement. The policy will define what is needed to trigger coverage as well as parameters for recovery. Typically, as an initial step, breach counsel and IT forensics assist with investigating the incident and in providing information supporting additional coverages under the policy. Additional vendors may also be retained to assist with the actual quantification and presentation of the total losses to claim in accordance with the terms and conditions of the policy. The onus is on the insured to prove their losses.

By engaging with a claims preparer with full time responsibility to support the insured through the assessment and quantification, policyholders can be much more confident in achieving their desired outcome. These experts are skilled in financial analysis, business interruption measurement, and cost presentation, enabling the business to focus on its day to day activities while an advisor manages the insurance process.

Claiming in unfamiliar territory

Navigating the claim can be challenging. Organisations are often in unfamiliar territory around demonstrating the operation and financial impacts of an event. While a cyber insurance policy defines the coverages available, it does not provide much guidance around how the various costs and expenses will be quantified. Loss adjusters, brokers or to a limited extent, a breach counsel, can provide policy insights at these early stages, advising of the interplay between coverage and the incident response for work that is typically covered — such as IT forensics activities around investigation of the nature of the event, and remediation; and for work that may not be covered — such as security betterments.

Loss adjusters and brokers can also inform organisations as to what documents may support quantification, such as receipts, monthly profit and loss statements, payroll ledgers, sales information, time sheets, and narratives from various employees. In the early stages of any claim, for example, it's good practice to quickly put in place an offline mechanism to capture all incident related costs and losses; it makes it much easier to capture that information and present it to the insurer.

Keep track

When an incident occurs, the natural reaction is to respond to the incident. There is a great deal of direction to provide at the onset of the claims process to keep personnel on top of tracking the impact. Organisations aren't always thinking about quantifying the loss or about tracking expenses related to the incident or properly recording losses; expense and loss evidence that can be difficult to recreate after the fact. Pre-planning should include a strategy for tracking these, and should offer alternative tracking methods if systems are down. The strategy should also identify those responsible for ensuring this happens. Early retention of a forensic accountant can assist with ensuring appropriate actions are taken to identify and quantify losses.

Resilience and recovery

Getting the prevention and preparation phases right is crucial. In today's hard insurance market where capacity is tighter and insurers have a keen eye on their loss ratios, they may look to reduce exposure to firms that lack cyber resiliency. They also require transparency from their insureds, expecting that they have taken appropriate steps to reduce the exposure to common threat actor attack paths. Equally, insurance buyers must understand the requirements of demonstrating their security frameworks in a renewal process; while also demonstrating tact with mitigating losses arising from an event.

Section 3

Control and containment during the response

Control and containment are the watchwords from the beginning of a cyber incident and the management of a claim. Engaging crisis communications experts (generally a covered expense) can be a very important component of the response. It is critically important for the victim to manage, among others, the following key channels of communication: internal (so employees understand what is going on and know what they should and should not say), clients (to manage their expectations and concerns, and to ensure consistent messaging), as well as other external channels like the press and the public.

With the organisation's C-suite focused on and concerned about communicating externally and internally, a priority must be to protect the business and recover as quickly as possible. Cyber incidents tend to advance quickly, particularly once the threat actor thinks they have been detected. There is an immediacy with cyber that doesn't often apply to other claims. Managing and controlling the message may have a huge influence on the reputational impact of the event. This can be particularly significant in incidents where the hackers have stolen sensitive information and then contact the third-party owners of that data to tell them that the data will be published if they do not either pay a ransom themselves, or pressure the victim firm to pay. Managing and controlling the message may also impact third party cyber claims. Communication is equally important to protecting the business and recovering; this all needs to be balanced and highlights the importance of the preparation work.

This should be the time where the pre-incident preparation work begins to pay off with a well drilled incident response plan swinging into action and a core response team taking control. Close coordination between the organisation and its insurer must not be lost in those early stages. Claims advocacy around cyber insurance policy wording is complex and demands among other things, prompt engagement with insurers to establish the decision-making tree between lead examiner, adjustment, and insured.

Organisations need a level of certainty around the recoverability of their costs at the earliest possible time and it is in everyone's interest to engage and resolve the incident as effectively and efficiently as possible, with a joined-up approach between incident response and the insurance claim.

Avoid delays

Contact with experts like breach coach and IT forensics to triage and contain the incident needs to happen immediately. In many situations, evidence that might be required to substantiate the claim is inadvertently destroyed as part of a haphazard containment strategy. Equally important is the forensic evidence that might be needed by law enforcement and attorneys general. Loss of this can result in increased fines and penalties as well as leaving the victim organisation without critical defence evidence in subsequent litigation. This is all the more important for insureds that host large quantities of PII or PHI given the increased penalties associated with recent privacy legislation and the new trend towards statutory standing that may open the door to mass tort litigation in North America. Experienced experts can quickly engage to help make sure that evidence is set aside and protected in case it is needed. However, not all organisations understand that urgency and given incidents often take place outside of office hours, or just before weekends or public holidays — a deliberate destabilising tactic by threat actors — it can lead to unnecessary delays which can hinder an efficient response.

Many insurers offer a hotline number, which opens the door to the use of a pre-approved panel of advisors from areas like breach counsel, forensics and public relations. Once there is an understanding that the breach is more challenging than those that the in-house team is experienced in managing, prompt action is a necessity. Ideally, an organisation will have determined its response team in advance of an incident as part of their response plan and will have received prior approval from the insurer to use these vendors.

Pre-agree third party vendors

Some organisations will choose to use their own resources and chosen vendors. It is not uncommon for organisations to have longstanding relationships with business partners, but are they suitable to respond to a major breach event? Caution should be exercised by using 'experts' who are genuinely tested and proven in this particular field. An organisation's usual 'go to' for IT — often a managed service provider who may themselves have held some degree of responsibility in the prevention of a breach for example — is probably not familiar with forensics and decrypting data. As well as potentially destroying or compromising forensic evidence, there may be concerns about or allegations of conflicts of interest if a managed security service provider is investigating a breach of the security that they manage. Even the appearance of such a conflict can draw attention from attorneys general and law enforcement, and can materially disadvantage the victim firm in consequent litigation.

Having approved vendor networks ready and working with someone who understands cyber claims will help cost containment. They understand the investigation and support process and will bring in the right personnel to respond to where the risk and exposure to the organisation is most acute.

Don't jeopardise cover

Organisations who wish to choose their own vendors could jeopardise coverage of expenses incurred. Insurers have pre-approved panel vendors, including breach counsel or loss adjuster led solutions, who have been thoroughly vetted and are experienced in incident response, but it's important to note that policies vary with respect to use of panel vendors. For example, some policies require use of panel vendors for coverage, while other policies require prior written consent, and still others only require that expenses be reasonable and necessary. Regardless of the language, organisations should seek approval from insurers in advance of going off-panel or the organisation could risk the expenses being refused all or in part.

Many cyber policies also require that the work carried out by the response team is 'reasonable and necessary' and if that isn't squared away before the work is done, an organisation could end up paying more than anticipated or more than the policy will indemnify. As cyber losses have ballooned, insurers have become sensitive to cost containment on first party response activities. There is less room for negotiations and many insurers are limiting use of third parties to those firms they have validated and included on their own panel where they have agreed to scope and type of activity.

A warning for organisations using a breach counsel to manage a cyber claim is that even though the insurer might have appointed the breach counsel, there are cases where the counsel has recommended a course of action that has not been agreed to by the insurer, resulting in the insured incurring expenses outside the policy conditions. It is good practice to attempt to obtain the insurer's approval in advance of work being done even if the policy does not require prior written consent.

Project management at onset

One of the big differences in the cyber claims process is the need for clear project management to organise the response workstreams and coordinate the key roles of all parties involved. It's about understanding what requirements will be necessary across the security team, the investigation, restoration, financial tracking, communications, and legal decision trees; while wholly documenting key decisions taken to best restore the operation.

There needs to be transparency over all work streams and knowledge shared between teams but equally, the experts must be able to focus on their tasks at hand in mitigating losses and reinforcing a strong position to the customer base. And, while all this is ongoing during that onset crisis phase, the insurer cannot be discounted in their awareness and / or involvement in all key activities, as the policyholder quickly turns to the speed and certainty of cost recovery.

Open and honest communication

It can take a long time for the full business interruption picture to develop but all sides — insurers, loss adjusters, brokers among others — need to be kept appraised of developments and progress made by the insured to the mitigating actions taken. It is why open and honest communication and engagement is so vital. On occasion, organisations who have suffered a cyber incident may go insular and inwardly focused, perhaps withholding key information, or attempting to fix what they can. They try to deal with it themselves and present a 'fait accompli' to their insurer with the expectation that they will reimburse all those costs. It then becomes a harder claim to resolve because the insurer is having to retrospectively validate actions and adjust the loss.

One strategy to help minimise the potential for conflict is to engage a third-party expert forensic accountant to calculate the loss. Some cyber insurers will agree to provide a sub-limit of insurance to cover (or contribute to) the costs of hiring such a consultant. Experience shows that having a forensic accountant as a mediator generally results in a less fraught negotiation process with an end result agreeable to both parties.

Manage expectations

Early engagement with an insurer, direct correspondence, approvals where required, and agreement to certain causes of action means there is a far smoother journey to resolution of the claim. Even if the organisation is unclear about what has happened and what the implications are, it is important to keep the insurer appraised with what it does know to manage expectations. There should be no surprises. If there is an aspect to the response that potentially falls outside the scope of cover, this can be addressed with insurers.

In a hard insurance market, there is more focus by insurers on what was disclosed at the time the policy was taken out and while claims are rarely declined on the back of a disclosure issue, any problems are likely to cause delay and diversion at a time when the organisation is trying to recover.

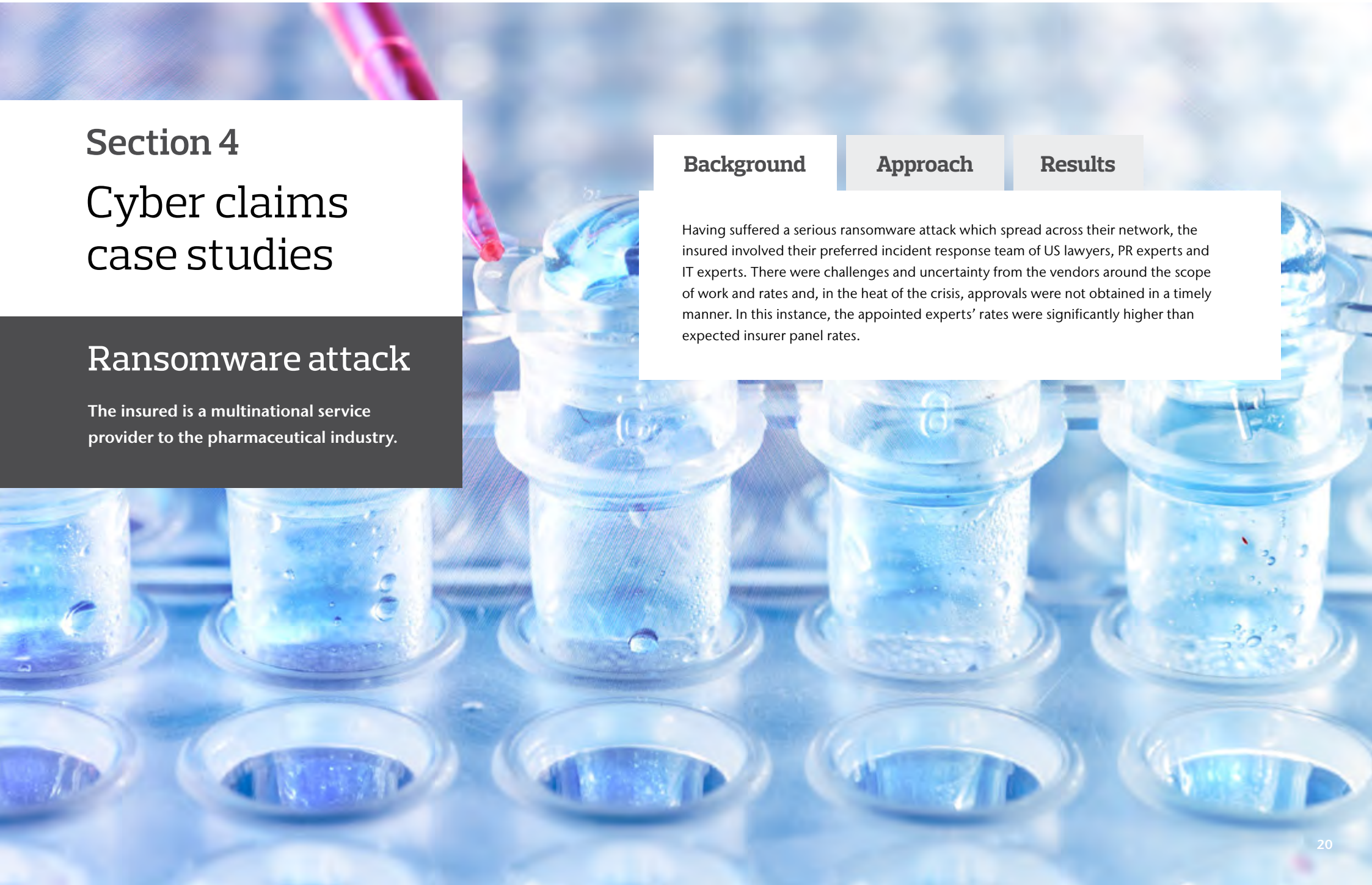
Third party losses

Beyond the potential losses to the organisation affected by the cyber incident, there is of course the possible impact on its suppliers, customers and other third parties. Legal actions from third parties related to data breach have been the most obvious in recent years, but that's beginning to change as the incidents become more about operational risk and business interruption. If an organisation can't supply its product because its systems are down and their customer suffers a financial loss, then there is a potential liability.

Third parties impacted are seeking recovery for their losses whether related to notification, investigation, use of breach counsel, or business interruption, for example. They may seek costs directly from the business that suffered the breach or look to recover from their own cyber policy leading to that insurer attempting to subrogate its costs from the original victim and their insurer.

Ensure maximum possible recovery

It's important to note that the response to a cyber incident is very front loaded — a few weeks for a large attack — and an organisation moves swiftly from the crisis phase into the recovery phase. This means that it quickly becomes a claims environment focused on effective claims management to ensure maximum possible recovery of costs under the terms of the insurance policy, as well as recovery of the organisation and protection of its reputation. If the management of the incident and the claim is wrong, the financial and reputational damage can be devastating.



Section 4

Cyber claims case studies

Ransomware attack

The insured is a multinational service provider to the pharmaceutical industry.

Background

Having suffered a serious ransomware attack which spread across their network, the insured involved their preferred incident response team of US lawyers, PR experts and IT experts. There were challenges and uncertainty from the vendors around the scope of work and rates and, in the heat of the crisis, approvals were not obtained in a timely manner. In this instance, the appointed experts' rates were significantly higher than expected insurer panel rates.

Approach

Results

Security event and consequential operational impact

The insured is a multinational organisation in the telecommunications industry.

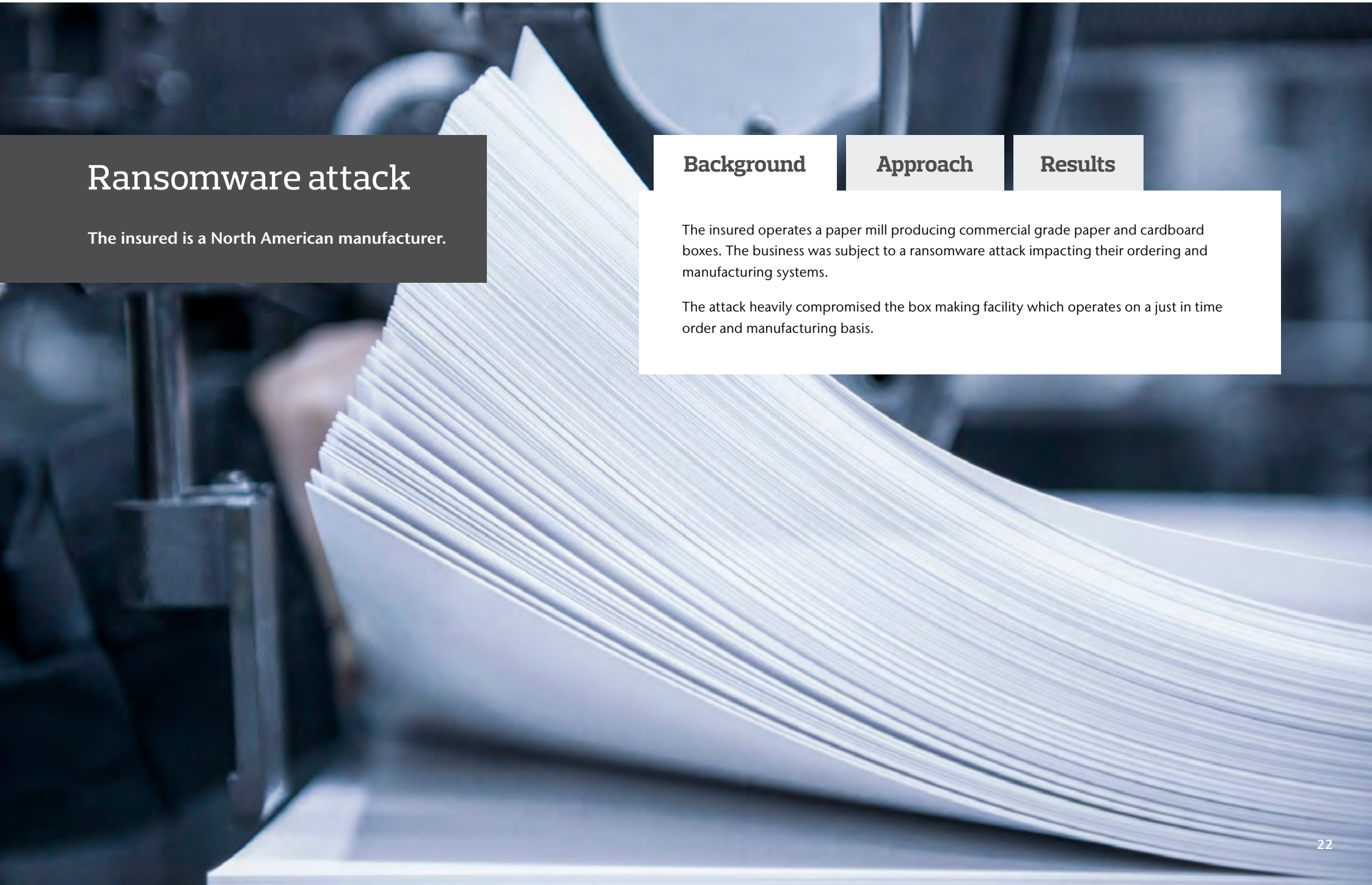
Background

Approach

Results

A multinational organisation suffered a sophisticated attack on its systems. The attack was a form of ransomware that is extremely complex, embeds itself deep within the systems, and is difficult to eradicate. Although it did not mature to point of decryption, three of the insured's locations were impacted, and instances of reinfection occurred through the remediation process.

While the ransomware had not matured to the point where a ransom was demanded, the nature of the malware made it extremely time consuming and difficult to remove other than through taking down the computer system and network for an extended amount of time. To restore services and to keep malware from infecting end point devices and data, the insured was forced to replace their entire network system.



Ransomware attack

The insured is a North American manufacturer.

Background

The insured operates a paper mill producing commercial grade paper and cardboard boxes. The business was subject to a ransomware attack impacting their ordering and manufacturing systems.

The attack heavily compromised the box making facility which operates on a just in time order and manufacturing basis.

Approach

Results

Ransomware attack

The insured is a global food and beverage organisation.

Background

A global food and beverage organisation had been locked out of their computer system from a ransomware attack, impeding revenue generating production and business operations for two weeks. The restoration of the global network continued for months.

Approach

Results

Section 5
Lessons learned from managing cyber claims

Aon has responded to some of the most high-profile breaches in the last decade[17], managed more than 2,000 cyber claims globally since 2012 and handled over $1 billion of cyber insurance recoveries on behalf of insureds since 2016. Crawford has also managed over 2,000 cyber claims globally since 2015 with 600 significant instructions in 2020 and over $750 million indemnity spend. Based on this collective experience, here are some examples of key lessons learned from managing cyber claims:

Prompt insurer notification

Delayed insurer notification can be a challenge for organisations, particularly if they underestimate the scale of the incident and try and deal with it inhouse before engaging insurer support. It is critical to keep insurers appraised in the immediate term to support the response, so all parties can work to reduce the cost burden. There can also be a question of knowing who to call which is vital in order to quickly mitigate any further damage.

Pre-agree access to external vendors

Organisations should know well before an incident ever happens who its response partners are in critical areas like forensics, legal and public relations, and ideally have the key responders identified and pre-agreed with insurers.

Get consent for third party support

An organisation may want to use their own legal and IT contacts, but they must get consent from their insurer or risk their fees not being paid. There is also a risk of the experts engaged not being expert in the field of a cyber incident.

17 McMillan, Robert and Ryan Knutson. "Yahoo Triples Estimate of Breached Accounts to 3 Billion." The Wall Street Journal, October 3, 2017; Finkle, Jim and Anya George Tharakan. "Yahoo says one billion accounts exposed in newly discovered security breach." Reuters.com. December 14, 2016; Volz, Dustin and Jim Finkle. "U.S. senator seeks SEC probe of Yahoo disclosure on hacking." Reuters.com. September 26, 2016.

Address issue of client privilege

It's important to make sure that the organisation takes steps to protect privilege, and / or consideration thereof, to ensure confidentiality for discussions with legal counsel and other documentation that may surface during a breach or in any pre-loss work, as well as putting the victim in the best position possible given the potential for future litigation and regulatory investigation. There are different laws of privilege in different areas and inhouse counsel, for example, might not always have that protection.

Understand what is and what isn't recoverable under a cyber insurance policy

There is often an expectation in the organisation that everything is recoverable, but there might be a betterment component (restoring a system beyond its original state) or additional expenditure for reputational and commercial reasons which aren't covered. Likewise, some organisations miss out on what they could have claimed for, such as overtime payments to IT staff who are working with external consultants to respond to the incident. Cyber policies typically have an explicit exclusion of wages / fees and other remuneration of the organisation's own employees, but overtime payments incurred specifically in response to the event will usually qualify as a covered extra expense.

Transparency and communication

Poor communication with all stakeholders — insurer, clients, regulators, and partners — can cause significant delay and disruption in relation to recovery. It can occur as a result of legal advice around privilege and the disclosure of information. As such, an understanding as to what documents are or can be subject to legal privilege is important.

Timely communication is also important. Do not wait for perfect information. It's natural not to want to inform stakeholders — insurer, clients, regulators, partners — until all the facts of a crisis are known, but a cyber breach rarely reveals its full impact until much further along the journey. It is critically important to control the message. Employees should be trained ahead of time to understand the importance of communication with clients and the general public, and not to say anything that is not an approved message created by the organisation's crisis communications consultants.

Involve subject matter experts

Rash decision making can leave an insured over exposed to larger losses. There are tried and trusted professionals in this field that can insert confidence to the organisation during a period of crisis around how to inform good decision making to include insurers vendor panel or incident response provisions per the policy. It is important to consider and / or put this subject matter expert team together, to the fullest extent possible, as part of the pre-incident preparation work. A strong core team will be able to assist with adding experts that possibly weren't contemplated.

Understand the timeframes involved

Many organisations expect that a cyber attack can be contained, investigated, and operations returned to normal in hours or days. While that is the case for some types of incidents, it is unlikely for any substantial attack. In the case of ransomware, even where an organisation makes a quick decision to pay the ransom, it still may take days to make payment and obtain a decryptor, and potentially weeks to use that decryptor across all the data.

Next steps

Get prepared, take control and optimise recovery

For organisations in the attack path of threat actors looking to use ransomware for maximum impact, it's critical that they get their response right from the immediate crisis phase through to the rapid evolution of the incident into a claims environment. The emphasis must be on ensuring a successful mitigation of its risk and exposure, together with maximum recovery of costs as per the insurance cover available against the terms and conditions of the policy.

As this guide highlights, pre-incident preparation is critical with the testing and alignment of business continuity and incident plans having a direct correlation to the quality of the outcome. These plans should be dovetailed with the cover available under an insurance policy and provide access to specialist expertise using either the insurer's panel of vendors, or those selected by the organisation and pre-agreed with the insurer.

Achieving this will help to avoid panicked reactions, and ensure a considered, crisis managed approach aligned to the complexity the organisation faces from the incident. Remember, an insurer's priorities at the outset are in lending assistance to the process; helping the insured organisation respond to the incident, aligned to best practice guidelines as per the specific circumstances and the specialist and expert advice available. They are there to help minimise and mitigate the impact of the incident.

A tight control on spend and activity during the incident, as well as being in a position to understand the main drivers of loss and align the response accordingly is important. It is one key factor to ensure continual engagement and communication with all stakeholders from the insurer, through to clients, regulators, and partners.

By addressing the basics, an organisation will be better positioned to come through an incident with its balance sheet and – just as importantly – its reputation intact.

Contacts

To find out more about how to protect your business and to optimise the benefits of cyber insurance through experienced cyber claims management, contact your respective local Aon or Crawford cyber professional.

Thank you to our Contributing Authors from:

Aon: Karrieann Couture, Ronald Hajjar, Jamie Hooper, Kevin Kalinich, Vanessa Leemans, Spencer Lynch, Bianca McKenzie, Darin McMullen, Chad Pinson, Tom Ricketts, Brent Rieth, Brian Rosenbaum, Michael Sgarlata, Joanne Quintal, Jacqueline Waters, Angus Watson.

Crawford: Fabrizio Bufacchi, Paul Handy, Neal Jardine, Edward Leighton, Eddie Walsh.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

aon.com

About Crawford

Crawford & Company (NYSE: CRD-A and CRD-B) is the world's largest publicly listed independent provider of claims management and outsourcing solutions to carriers, brokers and corporates with an expansive global network serving clients in more than 70 countries.

www.crawco.com

Crawford®

AON