2nd Edition

The Broker's Guide to Ransomware

CORVUS

2nd Edition:
The Insurance Broker's Guide to Ransomware

As we look back on 2020, it is an understatement to say much has changed since we published the first Broker's Guide to Ransomware.

When we first published this guide for insurance brokers in January 2020, Covid-19 was barely known to most of the world. That changed within weeks. But even as we dealt with living through a global pandemic, there's been one constant: ransomware has remained in the headlines and continued to weigh heavily on the minds of insurers and brokers. So while we have new information and data to share with brokers, the urgency of understanding ransomware and how it is covered by Cyber and Tech E&O policies is unchanged.

For any brokers who are getting up to speed on the current environment, this edition retains all the foundational information on ransomware, but also adds more about specific threat vectors, and the industries most affected by the trends in 2020. We hope you enjoy it.

Cheers,

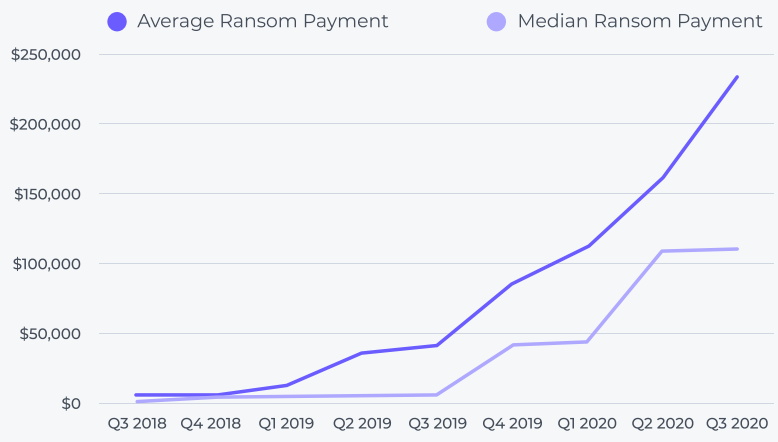
Mike Karbassi,
Head of Cyber Underwriting, Corvus Insurance

Table of Contents

01 Ransomware Foundations

At its core, "ransomware" is a category of cyberattack in which a criminal endeavors to lock up (through encryption) files or devices that are critical to an organization, and demands a ransom payment in exchange for the return of control over the encrypted property.

This year, reports showed continued increases in overall ransomware attacks, including a 715% increase through the first half of 2020 **by one count** with 30% of all attacks this year **coming from one** ransomware "family" of operators. The **average payment has increased sharply as well**.



Ransom payments by quarter. Source: Coveware

The $233,817 average ransomware payment in Q3 2020 represents a drastic 31% increase from Q2 2020. As the coronavirus pandemic spread throughout the year, healthcare providers became a favorite target of attackers. But as we'll learn, no industry or type of organization is ever immune. Attack trends will continue to shift to wherever there appears to be fertile ground.

Cyber Insurance can be a solution to transfer the financial risk of ransomware, and also to mitigate the risk of an attack thanks to value-added services attached to cyber policies.

By gaining a better understanding of ransomware, brokers can confidently advise their clients on **appropriate cyber coverage, risk mitigation services, and how to develop a response plan.**

Where Have All the Breaches Gone?

Despite being one of the earliest forms of cyber attack -- first witnessed in the late 1980s -- ransomware didn't dominate headlines until recently.

For most of the 21st century, attackers focused on stealing -- then selling, publishing or destroying -- important data. As the internet grew and industries like health care, banking, and retail digitized records and warehoused more customer information online, databases became a treasure trove for attackers. They could steal information and quickly sell it on the black market to other criminals seeking to commit fraud. The list of major data breaches in the past decade is too long to recount quickly -- some of the nation's largest retailers, health care companies, financial institutions, and government agencies were hit.

While these data breaches ruled the headlines and the minds of risk managers, Cyber Liability insurance was still in a nascent state. Being that data breaches were the most significant threat, coverage was primarily focused on those impacts.

Coverage for ransom payments and other costs typically associated with a ransomware event, like business interruption, were either an afterthought tacked on as an endorsement, or excluded because they were too poorly understood.

In the past few years, reported breaches have fallen slightly. Into the breach *(pardon the pun)* has stepped ransomware. Even as data breach activity was peaking in 2017, two ransomware attacks rocked the international community *(see below)* and brought on a new era of cyberattacks.

WannaCry & NotPetya: The Paradigm Shifts

In May and June of 2017, two global-scale attacks hit. Within the span of several weeks, ransomware went from being one of the lesser-known risks to something that caused alarm bells to ring for CISOs and risk managers across the world.

Affecting more than 200,000 computers in over 150 countries, the WannaCry ransomware attack is estimated to have caused total damages ranging into the billions of dollars. Shortly after, the NotPetya global incident brought on another $1.2 billion of damages to only a fraction of the number of targeted computers.

The key similarity between the two? Both attacks exploited the same leaked vulnerability in outdated Windows software simply referred to as EternalBlue. The two attacks immediately brought some of the targeted countries' largest companies – *including Merck, Maersk, and FedEx* – to a screeching halt and sent an important warning to the world about the far-reaching impacts of ransomware attacks.

While the events of 2017 encouraged the improvement of cyber defenses globally, the threat continues to grow. According to the McAfee Labs Threats Report *(August 2019)*, **attacks grew by 118% in the first quarter of 2019** led by three new families of ransomware. The rising threat has not gone unnoticed and is driving huge investments in the cybersecurity sector. A Report from Fortune Business Insights predicts that the global cybersecurity market size will grow from **$131.1 Billion in 2018 to $289 Billion by 2026**.

Why Ransomware, Why Now?

In guiding brokers to better understand ransomware, we've found answering the "why" questions to be helpful building the context of the overall enterprise. Why the shift away from the seemingly lucrative business stealing and selling data? How did criminals around the world come to the same conclusion so quickly?

There's a surprisingly short answer to these questions that we can unpack: **the business of ransomware has proven to be, simply, better business**. And when it comes to untapped opportunity, news travels fast.

An important point to understand is that attackers are not, as security expert Brian Haugli puts it, "some kid in their mom's basement." They are well-organized, well-funded corporations. "They have HR, they have payroll, they have accounting. They go on vacation." And as with any professional business enterprise, the criminals need a return on investment. **Over time, the return on ransomware has gotten better than the return on selling stolen data.**

Consider what needs to take place to make money from a data breach.

First, an attacker must gain access to the IT system of an organization that has something of value.

Wherever the attacker gains access, it is very unlikely to be where the most valuable data is. So attackers then need to search through an organization's IT system, piece by piece, to locate data they believe to be valuable -- all without being discovered and shut out by the targeted organization.

Then, assuming they find something potentially valuable, they have to exfiltrate the data, put it up for sale (advertised and priced according to its value, of course) and wait -- hoping for enough sales to come in to recoup the time and effort expended.

What if instead the criminal could cut out nearly all of the intervening steps between gaining access to the system and getting paid, and replace them with one relatively simple transaction? They'd do it in an instant.

In this sense, the value of ransomware is readily apparent.

There are two drivers that have enabled this hypothetical to become a reality.

The first is the rise of cryptocurrency. Prior to the advent of cryptocurrencies, criminals using extortion would need to extract payment in standard wire transfers to foreign bank accounts and then "pinwheel" the funds to several financial institutions around the world to make it more difficult for the victim to "claw back" the money after the fact. Cryptocurrencies have smoothed this process considerably.

The second driver is the sophistication of the "-ware" part of ransomware: the actual programs that enable hackers to encrypt systems. With less sophisticated scripts, a would-be attacker who broke into an IT system would then have to locate something in the network *(a database, file, or machine)* important enough to be an effective ransom tool – potentially painstaking work, and not much different than the effort required for stealing data.

Breaking into a single employee laptop, for instance, won't convince a major corporation to pay anything: they can just replace the laptop and move on.

Now, though, modern ransomware scripts can worm their way through an organization's IT system so quickly and efficiently that they can cripple even some vast systems in minutes.

Rather than encrypting something specific of value, hackers can shut down the entire enterprise – **why not!** – with the cost of business interruption being enough of a problem to justify a demand.

As ransomware has evolved in the past year, criminals have moved beyond IT shutdowns to find new ways to twist the knife. Hackers will exfiltrate valuable data, using their old tricks from the era of data breaches, to act as an effective "plan B" if the victim is unwilling to pay the ransom right away.

Even if the IT system is resilient enough to withstand a ransomware lockdown, the victim may be convinced to pay by the threat of publication of sensitive data, with all of that regulatory pain, or by the inability to function without it should it be destroyed.

02 Ransomware Today: How It Works

Now that we know why ransomware is having its moment, let's go deeper on the basics of how an attack works. This section goes end-to-end: from the attackers' initial entry, through the demands and negotiation, all the way to resolution and recovery.

Infection: Getting Inside

At the initial point of infection, a ransomware attack is typically no different than some of the other forms of cyber malfeasance that involve hacking, like malware (of which ransomware is a subcategory), cryptojacking, or data theft. The attacker first needs to get inside the IT system in order to get whatever it is they want.

The most common method used by ransomware groups is the exploitation of Remote Desktop Protocol (RDP), a protocol developed by Microsoft and used by many organizations to enable remote control of a computer. If properly secured with a VPN, multi-factor authentication, and proper patch management, there's nothing inherently unsafe about RDP. But that's a big "if". criminals are able to exploit RDP by scanning the web for open ports (the default RDP port is 3389) and brute-forcing weak passwords. Criminals have also been able to scan for and exploit RDP servers left unpatched to certain vulnerabilities, like one known as BlueKeep, although that vulnerability is well-patched now.

As part of the pandemic-driven shift to working from home, there's been an increase in the number of open ports with RDP exposed. Criminals anticipated the trend, and that led to a reported 6x increase in this style of attack. Amid the increase in attack activity surrounding Covid-19, the constant evolution of malware continued. In June 2020 it was reported that a "lesser-known" trojan called Sarwent had undergone an upgrade making it more effective, demonstrating how constantly malware strains evolve and build on one another.

The second most common attack vector is through social engineering. That's a technically-minded person's way of saying "tricking or manipulating a human into taking a desired action or giving away private information" – often with a phishing email sent to employees of a target organization with the intention of tricking the user into clicking a link or downloading an attachment that starts running software on their computer. Attackers seem to

always be a step ahead of software systems' ability to catch them. And once they reach the computers of an organization's employees, it's a numbers game. No matter how much training is provided to identify phishing, human fallibility eventually triumphs.

That is not to say that phishing is the only way in. Some particular software vulnerabilities, with nicknames like BlueKeep or HeartBleed, enable the remote exploit of a server without a phishing expedition. These kinds of attacks often have severe consequences, but active work on the part of software makers and good patch management (i.e., software update) policies can reduce the risk of this kind of exploit substantially.

To summarize:

Social engineering (phishing) is the constant, consistent risk, while a software vulnerability can present a huge, imminent risk for a short time, but be solved.

Spreading within the system

However a criminal gets in, whether by a successful phishing exploit or a software vulnerability, **it is at this point that the specific type of ransomware script being deployed comes into play.**

Old-school ransomware scripts, which were more limited, might have succeeded at locking up an individual laptop, or a particular database that the attacker had searched for and located on the network. Now, though, more advanced ransomware scripts are able to worm their way across an IT system and proliferate through the organization, encrypting systems **with the intent to disrupt business broadly rather than seeking something specific of value.**

The scripts themselves have nicknames that sometimes become associated with high profile attacks, like RobinHood, WannaCry, NotPetya, Ryuk, or Locker. These pieces of software are sometimes developed and sold on the web for any aspiring criminal to use, while some remain proprietary to the criminal group that developed it.

They can cripple a business by preventing employees from accessing email or internal operations systems, halting accounting processes or other critical business operations that rely on digital tools.

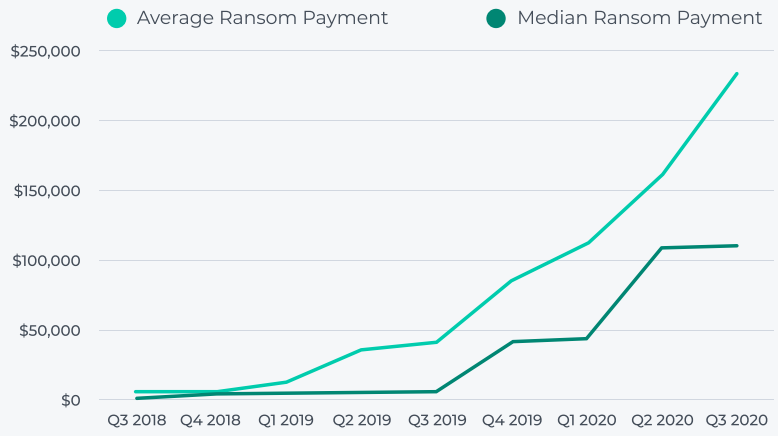
Often, these scripts are designed to exploit a particular software vulnerability that enables a ransomware virus to jump from a single computer to numerous entities across an organization's IT system. EternalBlue, for instance, is a vulnerability that was exploited in some of the biggest ransomware attacks the world has seen, in 2017 *(see p.4)*, and in the 2019 attack on Baltimore's city government. In the case of the NotPetya attacks, an infection sourced from a single piece of accounting software was able to spread to the entire corporate IT infrastructure of Dutch shipping giant Maersk SA within minutes, thanks to EternalBlue.

The demand

Once criminals have encrypted all or part of an organization's IT system, they will attempt to determine what the organization is likely to pay. They may sit on an infected system, going unnoticed, for some length of time; they may send a demand immediately.

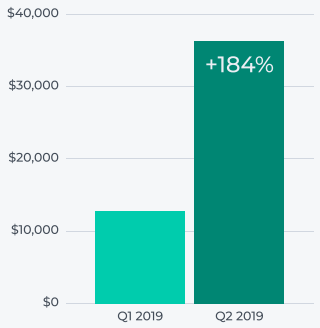
As Brian Haugli, the security expert, notes, criminals are getting more sophisticated in determining how much to demand. He tells a story of a ransomware attack on an organization in a very poor nation, who were given a large ransom demand that was simply not possible for them. In the end, the hackers unencrypted the system for nothing when it was clear that the organization was unable to pay anything close to the amount demanded. Situations like that are a waste of time and effort for the hackers.

Today's ransom demands are more finely honed to the size of the business and the value of the IT system or business interruption.



Ransom payments by quarter. Source: Coveware

The ransom note itself is often pushed directly onto the screens of infected computers via a basic text file format like a .txt, showing the user that their computer is completely locked down and conveying the important information: what is at stake, how much ransom is demanded, where to send the Bitcoin, and often a time frame for how long they have before the criminals will do something even more catastrophic, like permanently deleting files.



Ransomware Payment Increase Q2–Q3 2019. Source: Coveware

While exact ransom demands and costs are not regularly reported in the media when privately-owned firms are attacked, there are estimates put together by security researchers to get a pulse based on surveys and public company reporting. The **$233,817 average ransomware payment in Q3 2020** *represents a drastic 31% increase from Q2 2020. Reports of seven-figure ransoms, almost unheard of before, are now almost commonplace.*

Paying: What, How, How much, and When

At this point the targeted organization must make the choice to pay or not pay. This decision is fraught with many factors. *(Hopefully the organization is working with a trusted Breach Coach who can help through the process – see the last chapter on Cyber Insurance for more on this.)*

The FBI will always instruct an organization not to pay the ransom: it is a criminal act to participate. That is the party line, at least. In reality it is unlikely that the FBI would pursue action against an organization that pays a ransom. And **many organizations choose not to report the situation to law enforcement authorities at all,** preferring to keep as low a profile as possible. There are also efforts by some groups of organizations to limit the effectiveness of ransomware by having their members pledge not to pay ransoms, but they lack any binding authority.

It is estimated that 90% of ransomware demands are met.

It is recommended that targeted organizations think of the demand as a negotiation. Haugli, the security expert, says that it bears remembering that this is a two-way street, like any negotiation. **The attackers may have most of the leverage, but not all.** They stand to walk away with nothing if the target organization doesn't comply.

If your organization is comfortable with alternative options, such as walking away from the damaged system and rebuilding from scratch, or if you have adequate backups that are not infected, **you have negotiating power.**

Criminals would rather take something – say half, or two thirds of the original demand – than nothing.

Payment is most often demanded in the cryptocurrency Bitcoin. An organization will have to exchange dollars for BTC through an online exchange service, and wire the Bitcoin to the wallet provided in the Ransom note.

Honor among thieves?

After the payment is sent, the targeted organization has nothing to do but hope that the criminals comply with their deal. This is never a sure thing, but based on industry reports, the attackers more often than not do what they promised. This aligns to the "professionalized" image of attackers mentioned earlier in this paper. **In order to sustain the business model, attackers can't be seen as entirely duplicitous.**

It bears mentioning here that it's possible a criminal may not comply with their end of the bargain simply because they can't.

"Families" of ransomware attackers, as they are often known, are occasionally taken down in raids by law enforcement, and if a raid is successful in seizing computers and jailing the participants, the encryption keys needed to unlock ransomed IT systems may be forever gone.

How Ransomware Impacts Clients of Different Sizes and Types

Ransomware attacks will impact each business differently. If your client is a multinational corporation, the cost of business interruption can swiftly outweigh the cost of even the boldest ransom demand, with millions of dollars lost every day down. On the other hand, if a criminal has demanded an outsized amount from a smaller business, that client may feel that it's worth taking some time to figure out if there are any remediation options available that would allow them to avoid paying the ransom, and simply rebuild the IT system from the ground up. **The average ransomware attack costs the targeted organization $228,000 in business interruption**, almost 3x the average ransom demand itself.

And those smaller businesses are hardly immune: small- to medium-sized businesses are increasingly falling victim to ransomware.

Since only the largest businesses make headlines, it can lead to a sense that criminals target large businesses at a much higher rate. In reality, a survey from 2019 indicated that **1 in 5 SMBs fell victim to a ransomware attack in 2019.** And keep in mind that certain sectors report higher frequency of attacks than others.

Some organizations have special considerations beyond dollars and cents. Governments may feel they have a duty to their constituents to report on the situation, making the decision that much more complicated by being in the public eye. Baltimore's city government has come under criticism for deciding not to pay a ransom of $80,000 *– thus following the letter of the law –* and incurring millions in costs to rebuild and restore digital services for its constituents. Hospitals, another recently popular target for attackers, have obvious imperatives to restore certain systems because human lives are on the line in a literal and immediate sense. The choice to pay up may be out of the question.

3x

The average ransomware attack costs the targeted organization $48,000 in business interruption, or more than 3x the average ransom demand

1 in 5

SMBs fell victim to a ransomware attack in 2019

62%

of businesses in this category go out of business within 6 months of being hit by a ransomware attack

The bloody aftermath: Rebuilding

After all is said and done, there's plenty of work to do. If the targeted organization has refused to pay, they will likely have to rebuild their IT system from scratch. But even if the organization has paid the criminals and had their system unencrypted, some devices may be beyond repair – too risky to conduct business on again – or have to be wiped clean and set back up. **Forensics groups will likely be brought in to figure out the extent of the attack on the system and recommend ways to improve security.**

03 Trend Watch

Most of the foundational aspects of ransomware haven't changed in the past year, since we published the first edition of this paper. But there are a few trends to watch out for that deserve a mention as brokers and executives look ahead at 2021.

Rising Cost.

Growth in total numbers of reported ransomware attacks has thankfully not kept up its torrid pace. But costs are exploding.

NetDiligence, a provider of cyber risk management software and data, found overall **costs of a ransomware attack increased 57% from 2018 to 2019** *(more if business interruption costs are added)*. The growth in cost is driven in no small part by the ransom demands themselves. While overall costs grew by 57%, the **average ransom grew by a whopping 276% (3.75x) to reach $175,000**. And these figures are only for businesses with up to $2bn in annual revenue. Large enterprises face much steeper demands.

A quarterly report from Coveware that includes larger enterprises put the **average ransom payment at $233,817** for Q3 2020, a substantial increase even from the previous quarter.

Average Costs by Year Source: NetDiligence

Around the industry, the focus is increasingly on the ransoms driving up the average, which sometimes reach into seven figures – *an amount that would have made for the ransomware story of the year just recently.*

It's rumored that Foxconn, the electronics giant, received a demand for $34 million in November 2020. As long as demands continue to result in outcomes for the attackers, they are unlikely to fall.

Exfiltration.

You'll recognize the names from headlines if you follow cybersecurity: Ryuk, Sodinokibi, Maze. These were three of the most active strains of ransomware in 2020, whose operators have successfully stolen data from victims as a way to increase leverage in the ransom negotiation. *(Maze recently shut down as operators moved on to using derivatives of the original software).* In some cases, attackers have been able to make a return by auctioning off stolen data, even when they were thwarted in their attempt to get a ransom from the victim. Or they've gone back to the well to get a second ransom by threatening to release sensitive data.

50%

Exfiltration was used by roughly half of all ransomware attacks in 2020, according to Coveware.

New industry emphasis; bigger fish.

Finally, some evolution is happening in the types of organizations targeted. Much has been made of the governmental entities attacked, such as local school districts, municipal governments, court systems and the like. However there's a reporting bias to consider, given that these are public agencies whose duty is to report an attack.

In reality, there's been a rise the number of attacks on IT and professional services companies, like managed service providers, that is even more worrying.

The attack on Blackbaud was a salient example from 2020 of this style of attack. Hundreds of clients of the cloud software provider for non-profits have been swept up in the fallout from the breach.

Healthcare is another sector to receive attention, particularly given the strain placed on hospitals and health systems dealing with Covid-19. Some ransomware operators claimed they would spare health care from their machinations while the pandemic raged, but there were plenty of others to fill the void.

In whatever industry your clients sit, the trend is up-market.

Given their success in extracting larger demands from victims, attackers are looking to larger enterprises.

04 Ransomware and Cyber Insurance

Cyber liability coverage has broadened significantly in recent years, and today has a number of features that pertain to specific costs relating to a cyberattack, and increasingly for costs that are associated with ransomware attacks.

Coverage

Cyber liability policies run the gamut when it comes to ransomware coverage. **Policy language from some carriers has not changed quickly enough to keep up with the trend in claims activity,** leading to undesirable outcomes for some insureds dealing with ransom situations.

In a ransomware event, there are three primary ways Cyber Insurance coverage will respond.

First, and most obviously, a Cyber Extortion agreement in the policy directly pays for money sent to the attackers. This may also be called, simply, Ransomware Coverage. Normally you will see the extortion demand coverage match the limit. With continued losses plaguing the loss ratios of carriers offering this coverage, though, it's feasible that in the future brokers may start to see some sublimits applied to this cover.

Other potentially covered costs relate to the **IT expenses** necessary to get back up and running. This may fall under a couple of separate covers. **Breach Response and Remediation coverage would cover the cost of digital forensics investigations** to learn about the extent of the attack, why it happened and how to prevent future attacks. These can range from tens of thousands to sometimes millions of dollars, depending on the scale of the organization involved.

Data Restoration is another potentially covered loss that responds for the costs of restoring data this damaged or lost in the process of the attack *(it's not unusual for the process of encrypting and decrypting to result in some damage to files, even if they are eventually returned).*

Lastly, there are non-IT business costs. The key cover here is business interruption. This coverage is increasingly important as ransomware attacks focus more on crippling business operations, rather than locking up a specific set of files. Coveware reported that the average length of an outage reached 19 days in Q3 2020, up from around 16 days the previous quarter.

Business Interruption coverage will pay for lost income during the period the insured is unable to operate because the encrypted system has made them unable to conduct business. In addition to BI cover, there are coverages available for **reputational damage**, which covers lost business in the period after an attack as identified by a forensic accounting team.

All of the above are first-party costs. Other agreements including defense and liability may be implicated if third parties are affected and wish to bring lawsuits alleging financial loss because their business was impacted.

Beyond the Policy: Advising Clients on Risk Mitigation, Preparation, and Response with Cyber Insurance tools

Ransomware is a bad situation, and the pain inflicted on a business will be difficult enough that even the best Cyber Insurance coverage makes it something to avoid at all costs. As a broker, there are steps you can help your clients to take to **mitigate the risk of an attack happening in the first place, and to mitigate the chaos and confusion that inevitably comes if an attack does happen.**

Hardware and Software Defenses

What many security experts will tell you is the first step: **establish multi-factor authentication (or, alternatively, two-factor authentication).** This means the addition of another layer of security, often in the form of a security code sent to the user or accessed on their mobile device, to the traditional password and username combination. Any access points to critical systems -- certainly any IT systems, but also business email -- should require it. This is now "table stakes" considering the litany of attacks that could have been prevented with this comparatively simple measure in place.

Next, choose a policy that comes with an IT security scan that helps the policyholder to learn about their risk. Even if the insured has a substantial IT department, there may not be fluid communications from that department across the organization. Helping executives to understand the risk can help them to better manage priorities and assess the suggestions of the IT department as they relate to overall risk management. In cases where the client is smaller and has a very small or outsourced IT resource, the scan is even more impactful.

An IT security scan can, for instance, identify that there is outdated software running on servers that have been neglected and perhaps forgotten about by the IT department. For instance, identifying and rectifying open ports with RDP, the vulnerable Microsoft protocol described in chapter 2, **led to a 65% drop in overall ransomware claims at Corvus.**

< 65%

Corvus helped policyholders identify and rectify open ports with RDP, reducing overall ransomware claims by 65%.

Is insurance fueling ransomware?

Several years ago, ransom demands typically settled below the policy retention of a cyber liability policy. As such, the cyber liability industry had no impact on the calculations for a cyber criminal.

Today, with demand accounts rising there is beginning to be some conjecture that criminals are aware of and actively exploiting cyber liability policies. There have been anecdotal reports of attackers taking time to search their victim's files to isolate the policy and discover limits available, and adjust the ransom demand accordingly knowing that the victim will be likely to pay out knowing that it is covered.

Given the range of potential costs covered by a modern cyber liability policy, this alone shouldn't be reason for pause when recommending coverage to a client – but it is a trend underwriters are watching.

Recommending to that client to improve their patch management policies and procedures could save them from a devastating attack. This example could apply to the presence of adequate email security software,

Going a level deeper, you can discuss data backup and network redundancy with your clients. When it comes to ransomware, backed up data could be the difference between your client having their hand forced in the decision to pay a ransom in full or being able to consider multiple options. When fully incorporated into a security strategy, this is known as "Defense in Depth". Find out if your clients back up data on a separate *(fully "redundant")* system, and the frequency that they back up data onto that system. If their preparations are insufficient, suggest the use of vendors the cyber insurer can provide access to *(see next section)*.

For more technical best practices, see the U.S. Cybersecurity and Infrastructure Security Agency (CISA) ransomware guide, last released September 2020.

Governance and Mitigation

Outside of the IT system itself, there are other ways that organizations can prepare.

Being that phishing is a common attack vector, guide your clients to improving their policies and procedures around training employees to recognize and report phishing attempts. Some insurance policies will have phishing testing or training opportunities as part of a **risk management toolset.**

Speaking of risk management tools, guiding your clients to take advantage of what insurers offer can be an easy win.

> Increasingly, insurers (like Corvus) are offering more hands-on help in prioritizing security measures and understanding their risk.

These can be easy to forget about once the policy is bound, but your client will be leaving value on the table if they don't use them. *(Not to mention being less safe than they could be).* These services can help clients progress from understanding the problem to taking action. *(See Corvus's Risk & Response Services offering here: PDF).*

Cyber insurers will also often have connections with vendors for the kinds of **services organizations need to recover from a ransomware attack.**

Recommend to clients to establish who among the options available will be their choice, and contact those vendors to establish a relationship. This is most important in the case of the **breach coach, a person, typically a lawyer, who acts as a "quarterback" of the entire ransomware response situation.** Knowing who the breach coach is, and having a set of procedures around exactly who and when to call when a ransomware situation arises, will do wonders for the ability of your client to respond effectively.

Finally you can inform clients about other sources of information outside of your insurer. Information Sharing and Analysis Centers (ISACs) are groups that provide sector-specific information and participation in these groups is recommended by the U.S. CISA. A list of sectors with ISAC groups can be found at https://www.nationalisacs.org/member-isacs.

CORVUS

About Corvus

Corvus is reimagining commercial insurance for a digital world by making insurance smarter, companies safer, and brokers more successful.

Corvus empowers brokers and policyholders with actionable insights to mitigate complex risks and reduce losses through the CrowBar digital platform, smart insurance products, and premier risk management services. Corvus is the world's largest specialty commercial InsurTech company.

Founded in 2017 by a team of veteran entrepreneurs from the insurance and technology industries, Corvus is backed by Telstra Ventures, Obvious Ventures, MTech Capital, Bain Capital Ventures, Hudson Structured Capital Management, and .406 Ventures. The company is headquartered in Boston, Massachusetts, and has offices across the U.S.