Ransomware Foundations

for Commercial Insurance Brokers

CORVUS

An excerpt from the 2nd Edition:
The Insurance Brokers 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,

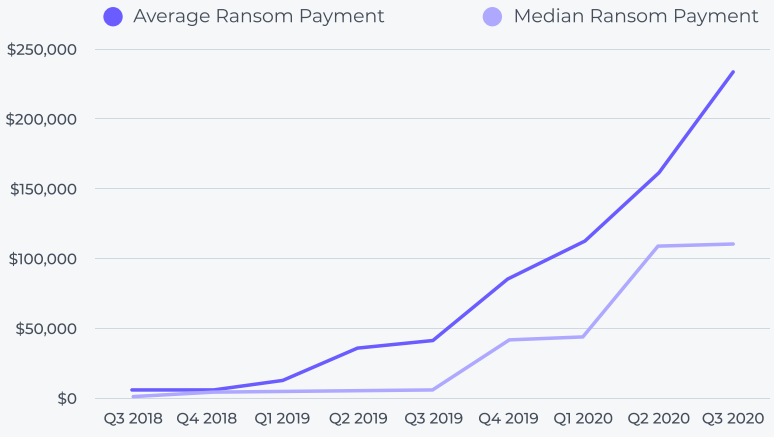
Mike Karbassi,
Head of Cyber Underwriting, Corvus Insurance

Additional Topics in This Series

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.

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.