Ransomware & Cyber Insurance

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

Ransomware & Cyber Insurance

Additional Topics in This Series

Ransomware How it Works

Ransomware Foundations

Ransomware Trends to Watch in 2021

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.