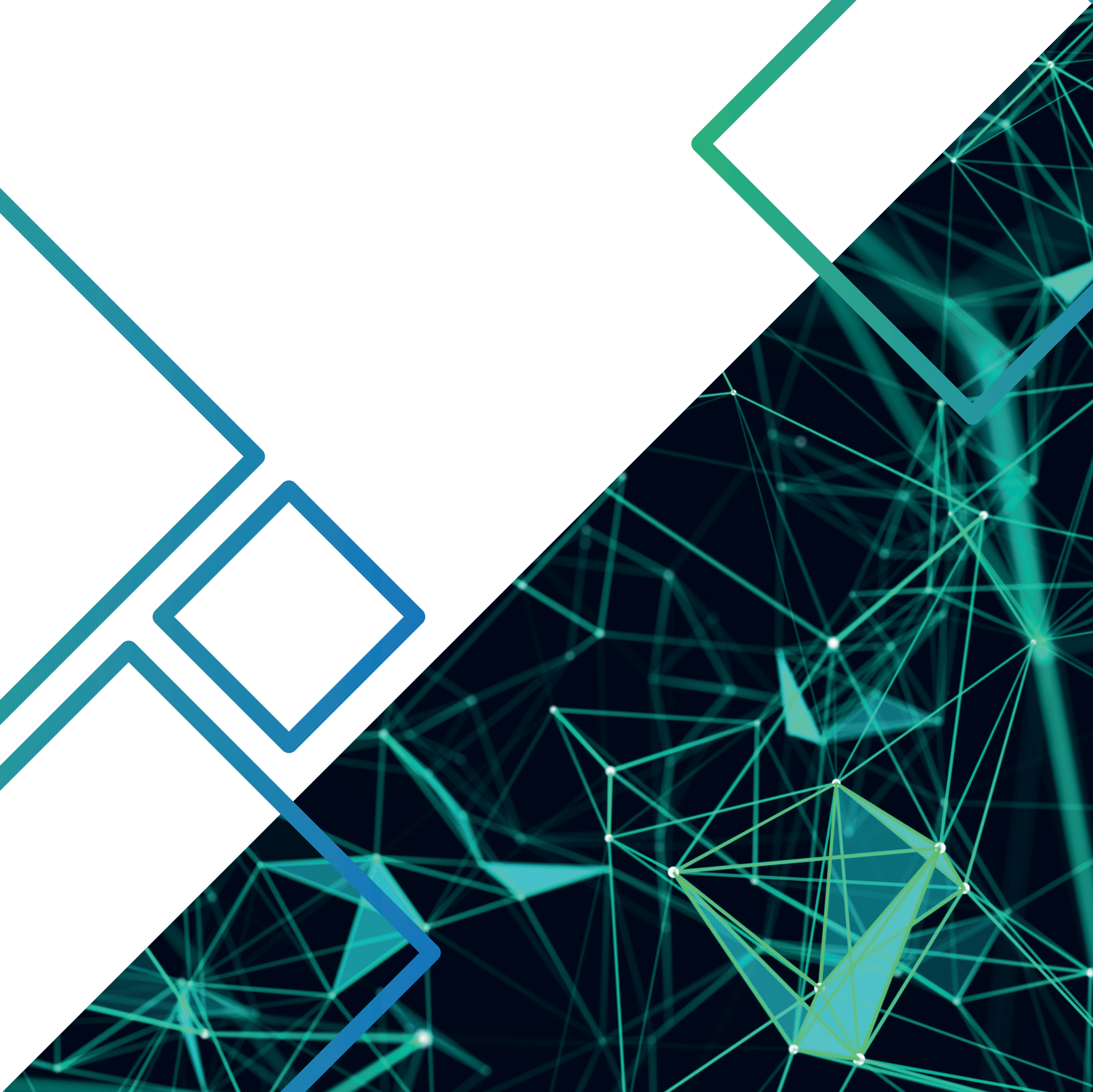
Enterprise Ransomware

Assessing the future threat and what it means for (re)insurers

CyberCube

www.cybcube.com



As the threat of ransomware has evolved in recent years, it has been placed firmly at the top of the agenda for cyber insurers, reinsurers and brokers.

This report will highlight the latest trends in ransomware. It will summarise current techniques being used by criminals, discuss risk mitigation methods and predict where CyberCube believes this threat is headed in the future and the implications for the insurance industry. It will provide practical guidance as to how insurance professionals can adjust their working practices to minimise risk and maximise opportunity in this rapidly evolving space.

Ransomware - A brief history

The first ransomware code has been attributed to Harvard-trained evolutionary biologist, Dr. Joseph Popp in 1989. The virus was commonly known as PC Cyborg. This ransomware hid and encrypted files on PC equipment and demanded that $189 be sent to a post office in Panama after which the victim would be mailed instructions detailing how their PC could be restored. Not long after this, with the growth of the Internet cyber criminals started to realise its potential for monetizing Dr. Popp's idea on a much larger scale. The next decade saw a fairly slow and steady evolution of the ransomware attack, although attacks were still limited by the relative immaturity and scale of the Internet and focused on individual PCs.

By 2006, more robust and effective encryption technologies started to be employed, making attacks much more impactful and difficult to recover from. By 2011, the ubiquity of the Internet, dependence on computing systems for processes such as communication and automation of business, combined with the relative immaturity of security controls created a boom for ransomware attacks with around 60,000 individual attacks being detected. This number has more than doubled every year since that time.

In the 2017-2018 period, a noticeable shift occurred and criminals started to focus on the idea that successfully attacking business enterprises could, potentially, reap far greater profits than targeting individuals. This hypothesis has indeed been well and truly proven in the subsequent period, making ransomware the foremost security concern for businesses, the public sector and the insurance industry alike.

In 2017, the WannaCry ransomware attack put the concept of enterprise ransomware firmly in the minds of insurers when it took large portions of the United Kingdom's National Health Care Service (NHS) offline. Later that year, the NotPetya attack caused billions of dollars of damage when it swept through global systems, shutting down multinational companies. Experts estimate that ransomware attacks on US entities alone netted cyber criminals around $8 billion in 2019, and losses caused either directly or indirectly from these types of attacks continue to climb exponentially.

Ransomware attacks are evolving rapidly

As the focus of ransomware attacks has shifted from consumers to enterprises, criminals have invested heavily in advancing the technologies and techniques deployed to carry out attacks. have evolved to a point today where a sophisticated and virtually unbreakable hybrid combination of AES 256 and RSA 2048-bit encryption is used commonly. Ransomware payment transactions are carried out with anonymity in mind using cryptocurrencies. Sophisticated coding techniques are utilised to make the ransomware code more reliable and investments in obfuscation have enabled attacks to be almost impossible to detect by security software.

Whilst increasingly sophisticated technology has been deployed, criminals have also relied on social engineering techniques to snare victims with the use of advanced phishing commonly used to steal user credentials and gain system access privileges, then used to deploy the malicious ransomware payloads.

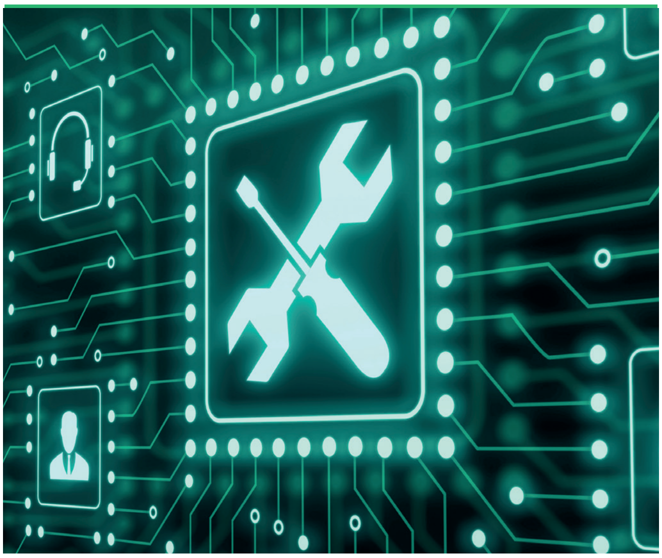
The concept of "double-extortion" ransomware was first introduced in 2019, and enjoyed great popularity in 2020, with criminal groups replicating their successes and others copying the tactic. In these attacks, enterprise data is encrypted by ransomware code as usual but the criminals also exfiltrate sensitive data to storage systems that are controlled by them so that this stolen data (often confidential or sensitive) can be used to further exploit a a victim. This trend essentially represents a morphing of data breach and ransomware together into a sophisticated hybrid attack. CyberCube expects to see more ransomware victims threatened with data exposure as a means of incentivizing payouts.

Maze and double-extortion

Since December of 2019, and throughout 2020, the Maze ransomware gang has been very active, targeting many high-profile victims in almost every vertical, including: finance, technology, telecommunications, healthcare, government, construction, hospitality, media and communications, utilities and energy, pharma and life sciences, education, insurance, wholesale, and legal.

Maze ransomware affiliates have been known to exploit RDP Open Ports to enter their target's systems, as well as via phishing attacks. No matter which method was used to gain a foothold in the network, the next step for the Maze operators is to obtain elevated privileges, conduct lateral movement, and begin to deploy file encryption across all drives. However, before encrypting the data, these operators are known to exfiltrate the files they come across. These files will then be used as a means to gain extra leverage, threatening public exposure.

Maze affiliates have already released data from companies such as Cognizant, Canon, and Xerox.



The types of data often exposed in the attacks can include:

- Sensitive internal files and communications
- Proprietary source code
- Credentials
- Credit card data
- Bank identification numbers (BIN)
- Personally identifiable information (PII)
- Protected health information (PHI)

There are now many prolific double-extortion ransomware gangs – including Maze, REvil, Sodinokibi, DoppelPaymer, Nemty, Nefilim, CLOP and Sekhmet – creating their own websites where they publish the stolen data of non-paying victims.

Ransomware threat actors continue to innovate both their technology and their criminal modus operandi at an accelerating pace. According to Security Boulevard, 337 confirmed ransomware events also resulted in a data breach in 2019. That number doubled to 676 in 2020. The research team at Security Boulevard has speculated there are a limited number of malicious actors with the skills and perseverance to engage in the type of attacks that can result in meaningful monetary returns. It is their belief some operators that once pursued sensitive data to sell on the Dark Web have now pivoted to more lucrative extortion schemes.

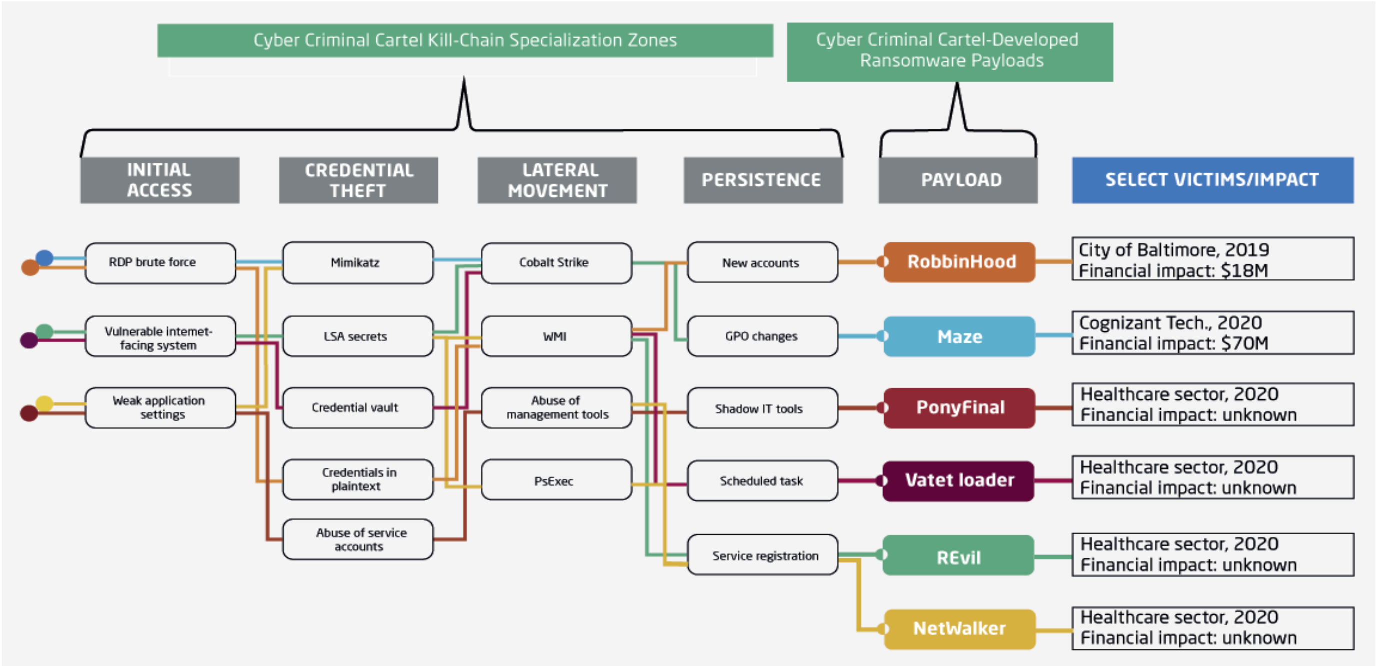
The rise of cyber criminal ransomware cartels

Distinct threat actor groups that engage in ransomware attacks appear to be collaborating more closely with their peers in the criminal underground, behaving more like cybercrime cartels than independent groups. CyberCube expects more activity from highly-coordinated ransomware cartels, with ransomware attacks that previously took weeks or days now only requiring hours to complete in some instances.

In 2021, the cyber criminal cartels behind these ransomware payloads will be responsible for the majority of attritional losses, and potentially even aggregation events due to cyber attacks. These groups are made up of hackers combining their functional kill-chain skills to execute attack campaigns collaboratively.

Ransomware cartels are increasingly leveraging skill sets that include conducting stealthy surveillance on systems before stealing or encrypting data.

They are researching financials and other internal information to help them understand whether the targeted organization is capable of paying a ransom. For high-value targets, they may monitor internal company communications during the ransom process to gain further leverage during negotiation.



The most devastating cyber cartels are based in countries where they maintain loose affiliation with the government, which permit their activities if they can also be called upon by the state. Rumors in the security community suggest that intelligence agencies in countries such as Russia, China, and Iran are contracting cybercriminals for intelligence operations, either directly or through intermediaries. An example of this first came to light in 2017, when the U.S. Department of Justice (DoJ) indicted two officers of the Russian Federal Security Service (FSB) for hiring a known criminal hacker to break into Yahoo's network. In 2020, the DoJ indicted two Chinese criminal hackers and accused them of stealing terabytes of information from computers around the world while working with the Chinese Ministry of State Security. More recently, in 2021 security researchers linked ransomware attacks to a group of Iranian state-sponsored hackers.

The recruitment of cybercriminals into intelligence operations can lead to an exchange of more sophisticated techniques, tactics and procedures (TTPs) that can then be used in criminal activities as well.

Cyber criminals now have access to nation-state technology to launch more sophisticated attacks, as well as plenty of open-source penetration testing tools.

Ransomware demands skyrocket

The motive for the huge amount of investment that cyber criminals and nation states are making in ransomware remains financial gain. Shifts from individual attacks on consumer PCs to a focus on the enterprise, improvements in technology and a maturing of processes have all occurred in the criminal world with return on investment (ROI) in mind. In 2017, the average ransom demand was between $500 and $1,000. Demands on corporations by ransomware gangs can now total tens of millions of dollars.

From an insurance perspective, huge ransom demands are only part of the story. Insurance claims that occur as a direct result of ransomware are triggered by various policies including business interruption, legal costs, and fines, as well as (in certain contexts) the ransom payments themselves.

> From an insurance perspective,
> **huge ransom demands**
> are only part of the story.

In recent years, a ransomware attack on the consultancy firm Cognizant by the Maze ransomware group resulted in losses of around $70 million. The City of Baltimore was hit by ransomware and suffered an $18 million loss in 2019 and, in 2021, a ransomware attack facilitated by the well-publicized Microsoft Exchange vulnerabilities is believed to have created a ransomware demand on computer manufacturer Acer of $50 million. CyberCube predicts the world's first $100 million ransom demand will be made within the next two years.

Ransomware gangs hunt the Fortune 500

On July 23 2020, Garmin, a company that makes $4 billion a year in revenue, was hit with ransomware known as WastedLocker, a strain associated with the Russian criminal hacking group Evil Corp. Note, it is believed among security researchers that Evil Corp is connected to Russian intelligence. The Evil Corp ransomware known as WastedLocker is purpose-built to encrypt critical data on a large company's network. Garmin's website, customer support, and applications including aviation services such as flight planning and mapping all went dark for days. Garmin reportedly paid $10 million to unlock its data. The attack is a sign that attackers are on the prowl for the biggest targets and paydays.

In April 2021, the REvil gang hit a key supplier for Apple, one of the largest companies in the world. REvil reportedly stole sensitive design schematics for Apple products from the supplier, and threatened to expose the schematics if the supplier (and Apple) did not pay a $50 million ransom.

Insurers whose client base is made up of large enterprises, should be aware that criminals are going to great lengths to understand the corporate structures of large enterprises through the reconnaissance phases of the ransomware attacks. These insights can include details of organizational structures, staff details, computer systems, supply chains, financials and even cyber insurance coverage.

Ransomware 2.0: Where is the threat headed next?

Cyber criminals will continue to adjust and improve their ransomware approaches to respond to increasingly sophisticated cyber defence and to reap as much reward from the opportunity as possible in the coming years. Analysis and research has led CyberCube to the conclusion that several areas of innovation are currently either being researched or are already showing up in real-world scenarios and insurers should be mindful of these.

Attacking Single Points of Failure (SPoF) technologies

In 2020, cyber criminals started to focus on the opportunity that single points of failure (SPoF) provide in the context of propagating ransomware. Common systems that provide service to many thousands of businesses can provide a powerful launch pad for malware attacks, including ransomware.

The SolarWinds attack in December 2020, whilst not a ransomware attack, demonstrated the value of vulnerabilities in common infrastructure to criminals. In March, 2021, criminals attacked vulnerabilities in Microsoft's Exchange email software, affecting hundreds of thousands of systems worldwide initially with malware focused on espionage and later with ransomware.

Ransomware gangs have recently targeted SPoF cloud computing infrastructure such as hypervisor systems. These systems are used to manage multiple virtual machines and are heavily used by cloud computing providers as well as large enterprises. Indeed, CyberCube estimates that more than 80% of the world's applications are estimated to run on virtual machines today. The infection Ransomware gangs have recently targeted SPoF cloud computing infrastructure such as hypervisor systems. These systems are used to manage multiple virtual machines and are heavily used by cloud computing providers as well as large enterprises. Indeed, CyberCube estimates that more than 80% of the world's applications are estimated to run on virtual machines today. The infection of these types of systems means that attacks can create much larger footprints of compromise than in traditional attacks that infect one system at a time.

SPoF, such as data-hosting firms, are also a recurring target for ransomware gangs that rely on the threat to customer data, helping their chances of a payout. In December 2020, Texas-based data center company CyrusOne said that at least six of its customers were affected by a ransomware attack. Other similar SPoF that have been hit with ransomware include DataResolution LLC, Cloudnine, Netgain, and Equinix.

In 2020, a ransomware attack on just one company, the cloud software provider Blackbaud, affected at least 100 US healthcare organizations. In 2021, a ransomware attack on the US company Colonial Pipeline, cut off critical oil supplies for the US Eastern Seaboard, and caused losses across the nation's oil supply chain.

CyberCube expects future ransomware attacks to leverage SPoF to broaden the footprint of attacks and create larger payment opportunities as a result.

Attacks to firmware

TrickBot is a prolific botnet that can be leveraged to launch ransomware. In late 2020, security researchers observed TrickBot adding a module that probes for firmware vulnerabilities. Firmware is the software that controls the physical processes that happen inside a computer. Firmware vulnerabilities are critical and if exploited they can lead to attackers gaining persistence (i.e. automatically reinfecting a machine) on devices after re-imaging or hard drive replacement.

Firmware-level attacks would allow attackers to write code to low-level system functions, ensuring the malicious code executes before the operating system boots up during the boot process. Potentially, criminals in this scenario could render any device they find vulnerable inoperable. Furthermore, persistent malware could enable them to disable most operating system level security controls, allowing them to resurface at will even after a system has been cleaned.

Recovering from an attack like this is more involved and expensive compared with traditional malware attacks. Corrupted firmware requires replacing or reflashing the motherboard, which is even more labor-intensive than replacing the hard drive.

Ransomware operators are already leveraging Trickbot to help launch data-encryption attacks. In the near future, it is not unreasonable to assume that the same attackers may leverage Trickbot's firmware vulnerability scanning feature to wage ransomware attacks that threaten to permanently "brick" or disable an enterprise's critical computing infrastructure unless a payout is made.

Less encryption and more extortion

Traditionally, ransomware attacks involved the encryption of a victim's files and a simple transaction but, in recent years, attackers have been experimenting with a new approach. Recent attacks have seen the victim's data encrypted with certain data also copied to networks under the criminals' control. This approach has been shown to provide the criminals with additional leverage to ensure ransom payment. Prominent criminal gangs such as Maze have now established this approach and it is now becoming the norm in ransomware attacks.

CyberCube predicts that enterprise ransomware attacks will use less encryption techniques in the years to come. Ransomware actors will likely become thieves, rather than captors and attacks will focus primarily on the extraction of key data, rather than the encryption of it. From a criminals perspective, the extraction method is simpler and less expensive than the complex process of managing ransomware encryption keys.

A shift in focus to data integrity

The situation whereby our most important data might not be what we believe it to be would be an extremely bad scenario for any business. Modern businesses rely on data, from payroll systems to product designs, for their very survival. Ransomware attacks that also include corrupting the integrity of a target's critical data are now a looming threat, especially with the increased use of AI and automation by cyber attackers to both corrupt and restore data at scale.

In this scenario, an attacker has encrypted and stolen a target's data in a double-extortion ransomware scheme. However, some companies may determine that they can recover encrypted data from their own back-ups and without paying a ransom for a decryption key. Other companies may conclude that they can take the hit of having data exposed and therefore will also not pay a ransom. Attackers are overcoming these obstacles with additional arrows in the ransomware quiver, such as data integrity attacks.

In a data integrity ransomware attack, the threat actors tell the victim they changed some elements of critical data such as patients' health records or customers' bank account balances. Of course, this scenario could adversely impact a business in multiple ways including, business interruption, customer confidence and retention, valuation, and market competitiveness. It is likely that these types of attacks will target businesses and institutions that are very sensitive to the accuracy of data, such as the healthcare and financial services sectors. To find out what data has been corrupted and to restore operations as quickly as possible, companies will be incentivized to payout.

Ransomware worms

According to an analysis from the French National Agency for the Security of Information Systems, some advanced forms of ransomware have developed worm-like self-replicating capabilities. From a functional perspective, this means that ransomware can propagate without human interaction. The addition of new worm-like capabilities to strains of ransomware such as "Ryuk" will be of special interest to the healthcare sector, where Ryuk was responsible for a large portion of the industry's ransomware attacks.

Ransomware worms would represent a significant advancement in the impact of this type of cyber attack. In particular, the ability to clean up networks impacted by ransomware would be severely impacted since worm viruses are well-known for their resistance to mitigation techniques.

Cyber insurance takeaways

CybeCube believes that there are valuable insights that should be considered and acted upon, based on the findings of this report.

Firstly, insurers should expect that criminal cartels will continue to target high-profile, often Fortune 500, organisations and will likely have researched these companies ability to pay a ransom prior to the attack through sophisticated reconnaissance of company assets. In addition, the techniques used to conduct these attacks will become more sophisticated and more targeted in the 2021 period. We should expect the trend from the use of data encryption to a data exfiltration method will continue at pace.

SPoF should be a major consideration for cyber insurers. We will likely see points of potential risk aggregation such as Cloud Service Providers (CSPs), hypervisors and other key infrastructure services attacked by ransomware gangs and used as "jumping off points" for large scale attacks.

The payments of digital ransoms is a shady area in cyber insurance today. In many jurisdictions, it is illegal to pay ransoms to criminal gangs. 2021 will see ransomware payment and negotiation emerge as a business opportunity for mediators and this will start to normalise over the next couple of years. It will be interesting to see how regulators react to this trend.

Safeguarding the emerging global digital economy is now a critical mission that the business sector, cyber security companies and insurers have a role in achieving. Of the potential risks that exist and that potentially threaten this mission, ransomware looms large. The next two years will be crucial in the context of safeguarding businesses, using technology and insurance products to mitigate and transfer risk and bringing criminals to justice.

SPoF should be a major consideration

for cyber insurers.

Authors:

Darren Thomson, Head of Cyber Security Strategy

William Altman, Cyber Security Consultant

Contributor:

Alejandro Sauter, Cyber Risk Analyst

Editorial Content:

Yvette Essen, Head of Content & Communications

This document is for general information purpose only and is correct as at the date of publication. The product described in this document is distributed under separate licences with CyberCube which restricts its use, reproduction, distribution, decompilation and reverse engineering. Whilst all reasonable care has been taken in the preparation of this document including in ensuring the accuracy of its content, this document is provided on an "as is" basis and no liability is accepted by CyberCube and its affiliates for any loss or damage suffered as a result of reliance on any statement or opinion, or for any error or omission, or deficiency contained in the document. This document is subject to change from time to time and it is your responsibility for ensuring that you use the most updated version. This document and the information contained herein are CyberCube's confidential and proprietary information and may not be reproduced without CyberCube's prior written consent. Nothing herein shall be construed as conferring on you by implication or otherwise any licence or right to use CyberCube's intellectual property.

CyberCube

www.cybcube.com