Ransomware

A threat not to be ignored

TOKIO MARINE HCC

tmhcc.com

Executive summary

In the ever-evolving digital world in which we live, it is becoming increasingly difficult to stay abreast of the cyber risks we face and understand how best to stay protected. Ransomware is highly pertinent to today's cyber threat landscape, with total costs reportedly reaching a staggering US$170 billion in 2019 alone.[1]

Throughout this paper, a dedicated team of cyber specialists at Tokio Marine HCC have consolidated market research and supplemented this with their own experiences to make this an "all you need to know about Ransomware in 2020" resource or single point of reference.

Key insights:

Beginner's guide to ransomware:

- There are two main ransomware categories: Locker and Encrypting
- A typical total for a ransom demand now stands at US$111,605, a little over double the previous figure.[2]
- Ransomware attacks usually take advantage of open security vulnerabilities and are spread in several ways, typically infiltrating a computer system through malicious attachments or links embedded in phishing emails, 'drive-by downloads', or through infected USB sticks.

Evolution of the threat:

- From the simple AIDS Trojan attacks in 1989 using infected diskettes, ransomware continues to increase in sophistication with catastrophic capabilities.
- In recent years, we have seen the rise of nation state attacks such as WannaCry & NotPetya. WannaCry alone is estimated to have affected more than 230,000 computers across 150 countries, with damages totalling US$4 billion globally.[3]
- First seen in 2018, the Ryuk ransomware is the most lucrative targeted ransomware attack to date, customising the attack based on the victim and generating US$61 million in less than a year.[4]

Claims trends:

- A shift from spray n' pray attacks towards big game hunting, driven by the ability to make higher ransom demands. Average ransom payments increased by 104% in Q4 2019 alone.[5]
- Rise of the Ransomware-as-a-Service (RaaS) model is enabling further specialisation of malware as responsibilities are broken down. Developers only need focus on development rather than distribution, enabling increased sophistication of attacks.
- Concerning increase in data exfiltration capabilities, with Maze being the first ransomware family to apply this technique.
- Covid-19 and the consequent increase in remote working increases the attack landscape for ransomware, with more vulnerabilities exposed in the home working environment.
- Ransomware claims can be catastrophic. A pharmaceutical company hit by Ryuk in 2019 suffered an estimated Business Interruption (BI) loss of EUR 60 million and further Incident Response costs of circa EUR 20 million.

Tips for Risk Managers:

- Cyber risk and readiness should be approached in line with the golden triangle model: People, Process, & Technology
- Key recommendations for risk managers address: employee awareness & phishing campaigns, securing back-ups, vulnerability management & patching processes, business continuity planning, network segmentation, resilient disaster recovery infrastructure, data protection methods, access management and the use of artificial intelligence.
- Recommended readings: ISO 27001 and the NIST framework

Introduction

Locky[6], WannaCry[7], CryptoLocker[8], GoldenEye[9]…

Do not be fooled by their fun and quirky names. This modern curse is costing the global economy billions every year. Ransomware is the new black in the cyber-criminal world – a trendy attack vector with a significantly increasing financial impact around the globe.

Most of the time, victims are unaware of this threat or wrongly underestimate its potential. However, they will certainly never forget the first time they encounter ransomware. As just one of many examples, we could ask the UK National Health Service (NHS) about the estimated US$113 million financial impact of WannaCry in 2017.[10]

Throughout the following pages, a group of Tokio Marine HCC (TMHCC) cyber underwriters will decrypt the key elements of the threat, analyse its evolution, share ransomware incident trends and provide some useful tips for organisations to protect themselves against ransomware attacks.

Ransomware – a threat not to be ignored

Previously, ransomware was a tool for opportunistic hackers. Today it is a highly profitable, extremely technical and sustainable business for organised criminals.

It is safe to say that, in recent years, this threat has been keeping risk managers and cyber security experts extremely busy. Its catastrophic capabilities make it impossible to ignore. Cyber criminals are continually finding new imaginative ways to execute their attacks and effectively extort their victims, leveraging the increasing importance of data to add gravity to their demands. A good example of this is the Jigsaw attack in 2016, which gradually deleted the victims' files minute-by-minute until the ransom demand was met.[11]

In recent years, hackers have become progressively more creative when it comes to spreading ransomware. Bad Rabbit, a ransomware released in 2017, found great success with the "drive-by downloads" method. This saw victims downloading seemingly legitimate software, such as Adobe Flash Player, from trusted websites, completely unaware that the site had in fact been compromised and their devices were consequently infected by the embedded malware.[12]

The financial impact of some of the most recent ransomware campaigns has also been alarming. The Ryuk ransomware attack, for example, raised over US$640,000 in just one month![13]

Are you ready to find out more? Let's journey through the different ages of ransomware!

Evolution of the threat

Hackers executing ransomware attacks are not dissimilar to kidnappers – the two criminal activities have a lot in common. Ransomware is a type of malware (malicious code) that will hold a victim's data and computer systems hostage. Data and/or access to the computer systems will be released once the demanded ransom has been paid.

There are two main categories of ransomware: locker and crypto ransomware. Crypto ransomware encrypts the files on a computer so that the person or company cannot access them. Locker ransomware does not encrypt files. Instead, it locks the person or company out of their system so that they are unable to use it.

Once encrypted or locked, the victim will receive a demand for payment to restore access to their files. Online payment methods and virtual currencies, such as PayPal and Bitcoin, are preferred by the attackers, as these are not easily traceable and, therefore, protect the hacker's identity. Only when the ransom is paid will the hacker deliver the cryptographic key which can be used to restore access to the computer or decrypt the encrypted files.

The ransom demands made by the cyber criminals are also rising. According to a new report by the ransomware incident response service provider Coveware,[14] in Q1 2020, the average ransom demand made against a business was reported as US$111,605. This represents a 33% increase from the previous quarter (US$84,116), and a staggering 170% increase from Q3 2019 where the average demand was just US$41,198.

Not everyone is so lucky, however. To give you an idea of just how crippling these attacks can be, the largest ransom recorded in 2019 was an astonishing US$12.5 million, as illustrated in Crowd Strike's 2020 Global Threat Report (see table below).

Ransomware attacks usually take advantage of open security vulnerabilities and can be spread in a variety of ways. A typical ransomware attack will infiltrate a computer system through malicious attachments or links embedded in phishing emails. Other common vectors of infection include the use of infected websites, fake advertisements that cause "drive-by downloads", or infected USB sticks inserted into the victim's device.

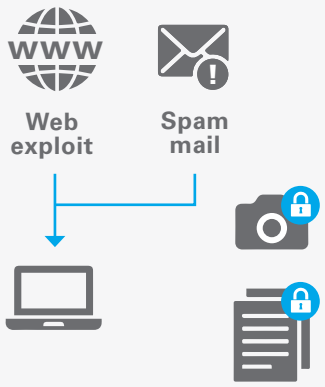
Largest Ransom Demands Reported in 2019 (CrowdStrike, 2020)[15]

USD	BTC	Malware
US$12.5M	1,600	Ryuk
US$10.9M	565	DoppelPaymer
US$10.0M	1,326	REvil
US$9.9M	1,250	Ryuk
US$6.1M	850	Maze

Once a computer or network is infected with ransomware, there are three key types of damage caused:

1

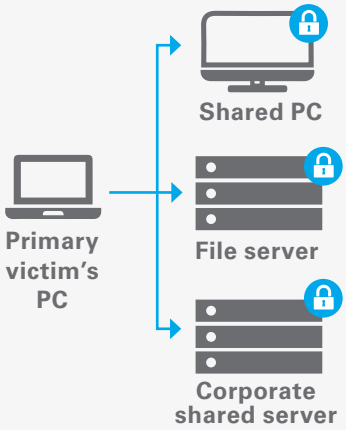
Encryption of corporate and personal data



Ransomware is introduced via routes including email and web, and encrypts corporate/personal document/data

2

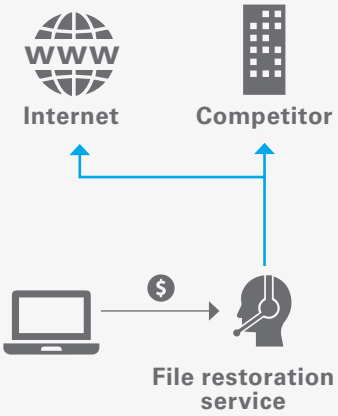
Secondary and tertiary damage as the encryption extends to, for example, file servers or network drives



File servers/shared PCs are exposed to secondary/ tertiary damage via network drives, etc.

3

Disclosure of information during restoration attempts



Confidential documents could get leaked via file decryption service providers

Source: FireEye, 2016[16]

To better grasp all the components of this ever-expanding threat, it is important to understand its evolution and increased sophistication over time.

Timeline of key developments

Following the major milestones, as set out by Stu Sjouwerman,[17] we consider that the evolution of ransomware can be divided into three key eras: The good old days, the age of sophistication, and the Cyber '9/11'.

1. The good old days

1989, AIDS Trojan, 1st ransomware virus

Also called PC Cyborg, the AIDS Trojan was created by Harvard student J. Popp. Some 20,000 infected diskettes labelled "AIDS Information — Introductory Diskettes" were sent to the World Health Organisation's international AIDS conference delegates. The AIDS Trojan is considered "generation one" of ransomware and used simple symmetric cryptography. Tools were rapidly available to decrypt the filenames.[18]

2006, The arrival of RSA encryption

Archiveus Trojan arrived on the scene 17 years later, with increased tenacity compared to its predecessors. This was the first use of RSA encryption[19] and the ransomware specifically encrypted everything in the 'My Documents' directory. Victims had to make purchases from an online store to get the password.[20]

2007, "Lock Out" virus

By 2007, locker ransomware had started to circulate. Instead of encrypting files or systems, this type of ransomware aimed to lock users out. WinLock, for example, displayed pornographic images until the victims sent a US$10 SMS to be able to unlock their systems.

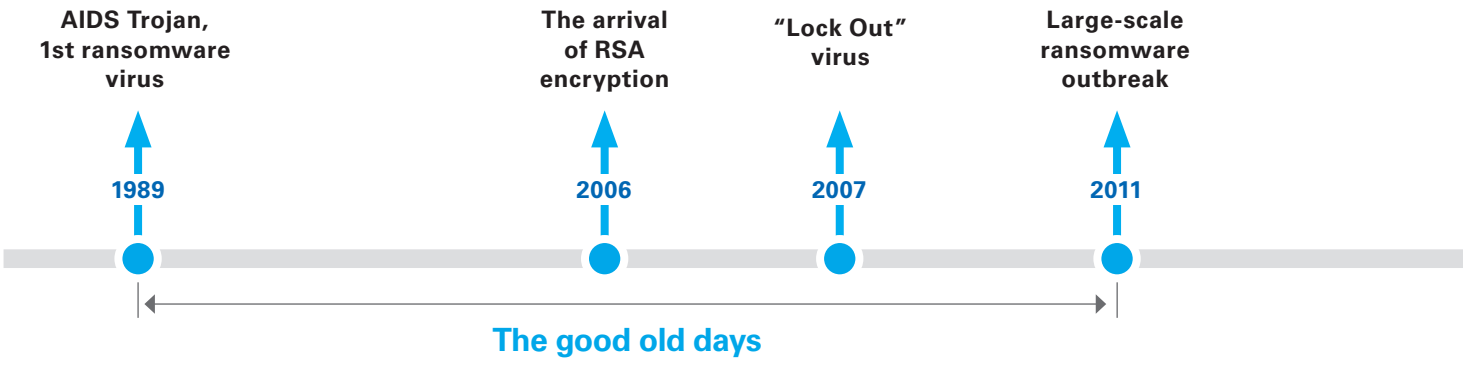
2011, Large-scale ransomware outbreak

The drastic shift towards large-scale attacks was made possible by the availability of anonymous means of payment, which facilitated untraced ransom collection. While at the beginning of 2011 around 30,000 attacks were detected, by Q3 that figure had already doubled to 60,000.

2. The age of sophistication

2012, A pivotal year for ransomware

Citadel is a malware that became available in 2012. This made ransomware more accessible for the less sophisticated cyber criminals who were eager to take a slice of the highly profitable pie. With Citadel, attackers were able to implant ransomware viruses on already infected devices in exchange for a small fee, paving the way for an unprecedented increase in the number of attacks that surpassed the 100,000 mark in early 2012 and reached over 2,000 per day by the end of the year.[17]



The combination of Citadel with another type of ransomware – the Lyposit "crime kit" that enabled charging false fines by posing as a specific law enforcement authority – led to the development of the Reveton worm. This scaremongered victims into paying a fake criminal fine for the possession of pirated software or child pornography. The attack tailored the "law enforcement agency" to the user's location, making it all the more believable. Users were locked out of their device, informed on the screen of their "crime", and requested to pay a "fine".

2013, The "download spreading" revolution

In 2013, CryptoLocker malware was released. It was the first cryptographic malware spread by downloads from a compromised website and/or sent to business professionals in the form of email attachments. It was usually disguised as customer complaints. Cryptolocker scrambled the victim's data using certain file extensions and demanded a fee to unencrypt it. There was also the added pressure of a countdown clock which threatened to delete the private key if payment is was not received within three days.[21] CryptoLocker compromised an estimated 250,000 devices within only the first 100 days, leading to instant profitability. Ransom demands varied by currency but were usually set at US$100, or two bitcoins.[22]

2014, Tor is the new black

CryptoDefense and CryptoWall were released, both reliant upon Tor and Bitcoin for anonymity purposes. Instead of victims needing to open an infected attachment, CryptoWall exploited a Java vulnerability. Malicious advertisements on domains belonging to Disney and Facebook, among many others, led people to CryptoWall-infected sites, where, subsequently, their drives became encrypted. More than 600,000 systems were infected in less than six months with 5.25 billion files encrypted.[23] Symantec reports that crypto-style ransomware saw an increase of more than 700% in 2014.[24]

2014 also saw the arrival of the ransomware-as-a-service model. By accessing a Tor website "for criminals by criminals", hackers were now able to advertise their ransomware for free in exchange for giving the site a 20% cut for every bitcoin ransom payment received.[25]

3. The "Cyber 9/11" moment

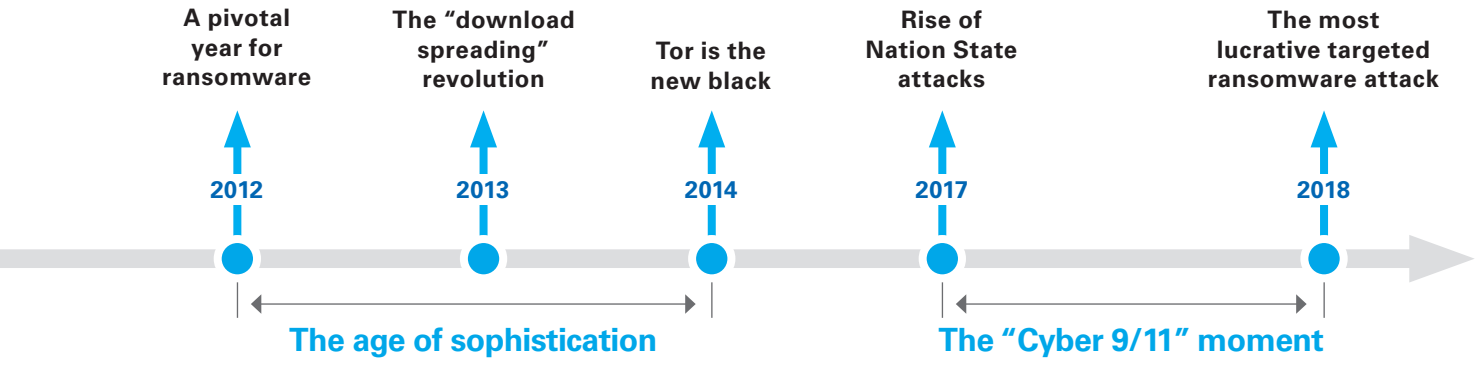
2017, Rise of Nation State attacks

The WannaCry ransomware attack was executed exploiting a vulnerability within the Microsoft Windows operating system, stolen from the US National Security Agency (NSA). Microsoft had, in fact, previously released patches to close the exploit, but much of WannaCry's success came from organisations that had not applied these or were using older Windows systems that exceeded their end-of-life support. The attack was estimated to have affected more than 230,000 computers across 150 countries, with damages totalling US$4 billion in losses across the globe. In December 2017, the US, UK and Australia formally asserted that North Korea was behind the attack.[26]

The NotPetya attack also occurred in 2017 and was a Wiper (malware focusing on destroying data and software) disguised as ransomware. According to the UK National Cyber Security Centre, it is highly likely that the Russian military was behind the attack.[27]

2018, The most lucrative targeted ransomware attack

The Ryuk ransomware generated US$61 million in less than a year.[28] Ryuk is specifically used to target enterprise environments and customises the attack based on the victim, ensuring a high Return on Investment (ROI) in the process. Ryuk identifies and encrypts network devices along with deleting shadow copies stored on the endpoints.



Claims trends

Recent incident trends:

1. Shift from spray n' pray towards big game hunting:

In recent years, the number of ransomware attacks appear to be decreasing. In June 2019, "only" three million locker malware attacks were detected, compared to 5.7 million in August 2018.[29] However, this does not necessarily indicate that ransomware is going out of fashion. Instead, criminals have changed their strategy and are shifting away from spray n' pray techniques in pursuit of the larger ransom opportunities found within big game hunting.

Previously, spray n' pray was a favoured strategy based upon the principles of economies of scale. Criminals would fire out vast numbers of untargeted phishing messages or fake advertisements, hoping to reach victims and receive regular yet modest pay-outs. In recent years, however, they have found a more efficient way to make even larger profits. It is now more profitable for criminals to target large companies who have the ability to meet higher ransom demands. To illustrate this shift, in 2017, 42% of all attacks were focused on consumers, yet in 2019 this number had shrunk to just 19%.[30] Through changing their target group, cyber criminals are able to demand higher ransoms, playing upon the company's desperate need for access to their systems and data to ensure business continuity. As criminals re-direct their attacks towards larger companies, these become increasingly sophisticated in order to bypass detection and prevention tools.[31]

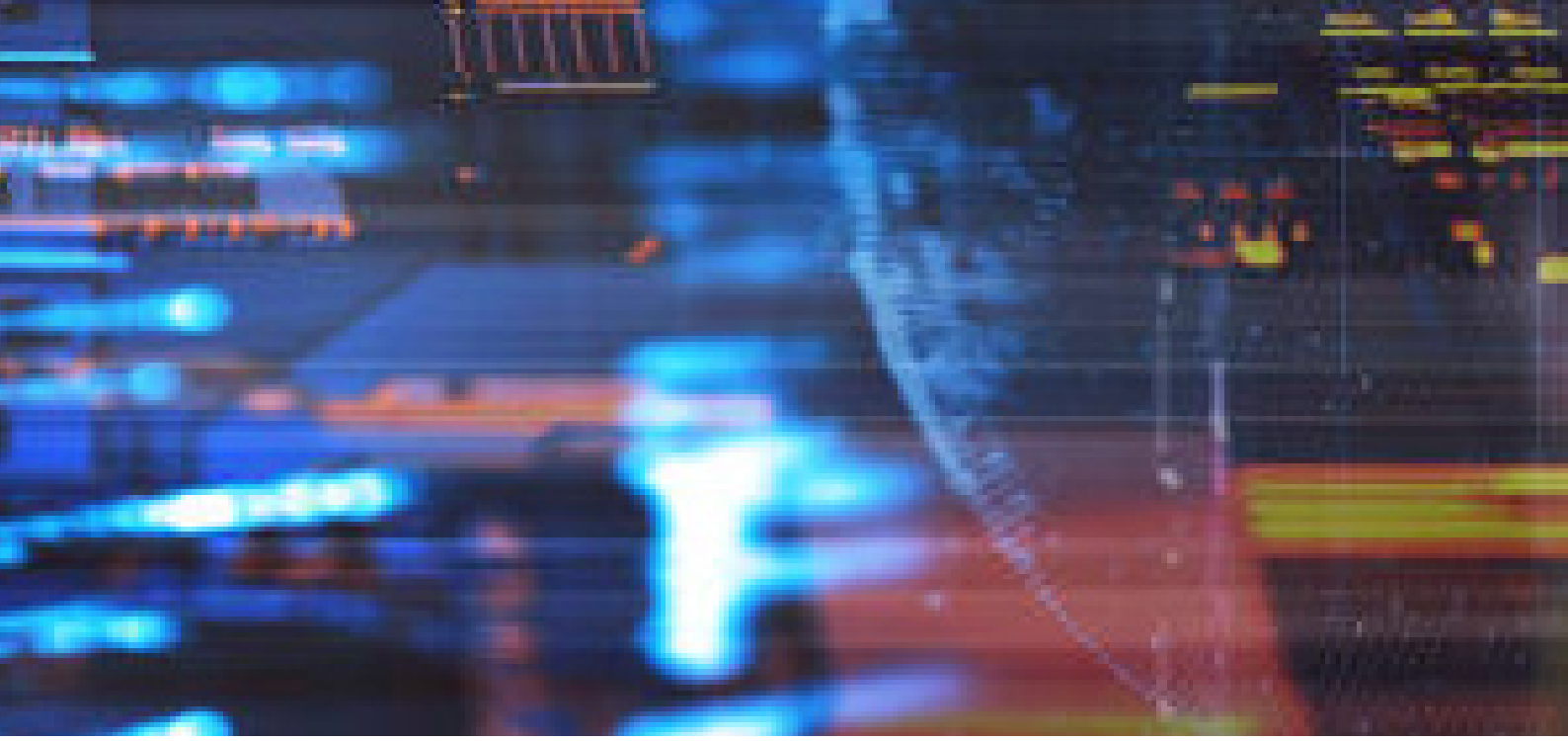
2. Increase in ransom amounts demanded:

As mentioned earlier, in the section entitled *Evolution of the Threat*, there has recently been a sharp increase in ransom amounts, which is largely attributed to the arrival of Ryuk ransomware. Ryuk is a targeted crypto ransomware that often resides within infected systems for a period of time to conduct reconnaissance before launching the attack. During this dwell period, the attacker is able to gather vital intelligence which facilitates execution with maximum impact.

Ryuk usually leverages previously installed malware dropped onto the target system. Therefore, forensics often find both TrickBot and Emotet present where Ryuk is involved in the attack. Entering via Remote Desktop Services is also popular. On average, a ransom of US$288,000 per incident is demanded, which is considerably more than other common ransomware demands of US$10,000.[32] Attackers are also becoming aware that companies may have a cyber insurance programme under which ransomware might be covered, which further tailors (and increases) their ransom demands.

3. Ransomware-as-a-service:

GradCrab put Ransomware-as-a-service (RaaS) on the map in 2018 and it has continued to operate as a highly professional and profitable business model. RaaS is a subscription-based model that allows unexperienced cyber criminals to play a part in launching ransomware attacks without needing in-depth knowledge of the topic. RaaS divides responsibilities of a ransomware attack into a supply chain, thus allowing each role to execute their part to perfection. As a result, ransomware specialisation has accelerated, with developers now only focusing their time on development rather than successful delivery or dissemination. Ransomware



developers are responsible for constructing the malware, advertising and the recruitment of affiliates. Affiliates are then tasked with distribution and negotiating ransom amounts. Revenues are usually split 50/50 between developers and affiliates, but this varies depending on the model. Various RaaS packages are available on the Dark Web, with notorious examples including Satan, Dharma and Snatch & Cerber.[33]

4. Increase in average downtime:

According to Coveware, the average downtime caused by a ransomware attack is increasing. In the fourth quarter of 2019, the average downtime increased to 16.2 days, up from 12.1 days in the third quarter of the same year.[34] A key reason for this trend is the increasing complexity and sophistication of attacks. Ryuk ransomware, for example, is often able to encrypt back-ups, which makes data recovery more complicated and time-consuming.

5. Bitcoin remains the main currency:

According to Coveware, 98% of ransom payments are made in Bitcoin. Crypto currencies Monero and Dash are also frequently chosen for their ability to conceal the hackers' tracks from authorities. Sodinokibi ransomware, for example, publicly stated that they have switched from Bitcoin to Monero.[35]

According to a report of Malwarebytes, nearly 40% of the victims pay the ransom and receive the decryption key in return 96% of the times.[36] This high percentage can be explained by the fact that if the attackers do not provide the decryption tool, their business model would not be sustainable. However, even when victims receive the decryption tool, they are not always successful in decrypting their data. Often, this is also dependent on the type of ransom. For example, Dharma variants were on the whole unsuccessful, while GrandGrab TOR decryption tools were usually successful.[37]

6. Exfiltration of data:

A worrying new trend has emerged recently: the dangerous combination of ransomware and exfiltration of data, which allows criminals to extract sensitive data before executing the ransomware attack, locking or encrypting the targeted systems.[38]

Through data exfiltration, the criminal has an extra weapon of persuasion in their artillery. When demanding payment, they are able to blackmail the victim by threatening to publish or leak their data, the PR and regulatory consequences of which could be fatal.[39] Using this method, cyber criminals can be confident in their demands, effectively rendering any of the victim's back-up solutions useless.

The first ransomware family to apply this technique was Maze, but others have since followed suit and have replicated the behaviour, notably DoppelPaymer and Sodinokibi. One of the most recent victims of such an attack is ExecuPharm, a pharmaceutical company in the USA.[40] The company got hit by a ransomware attack in March 2020 and decided not to pay the ransom. As a result, social security numbers, financial information, driver licenses, passport numbers and other sensitive data were published online.

7. Rise of new targets:

2019 saw the rise of a big new target, municipalities. Ransomware attacks in this sector went up by 60%. Requested ransoms varied between US$5,000 to US$5 million with an average of approximately US$1 million.[41] A widely referenced example is that of Baltimore, USA, that suffered from a large ransomware attack, costing them a total of US$18 million, including remediation, new hardware, and lost or deferred revenue.[42] Apart from municipalities, the most vulnerable industries include education, government, energy and utilities, and healthcare industries.[43]

8. Impact of Covid-19:

Covid-19 has had a stimulating impact on ransomware attacks.[44] On the one hand, increased remote working possibilities are leading to more connections to the network and, hence, hackers have more opportunities to gain access to the systems. Generally speaking, IT security at home is less mature than in the office. Furthermore, the concerns and interests of employees in the pandemic have been used to make them click on malicious links or download attachments in emails that pretend to be updates on the current coronavirus situation.

AZORult, for example, is a malware contained in bogus Microsoft Word documents attached to email messages purporting to be about coronavirus. It targets industries susceptible to shipping disruption (manufacturing, finance, transportation, pharmaceuticals, cosmetics) and can be used to install ransomware. However, ransomware success rates against organisations are not likely to increase if remote workers are properly segmented from production servers and databases where mission-critical data assets are stored.

Some claims examples:

1. Pharmaceutical industry:

In 2019, a European pharmaceutical testing services company was hit by a ransomware attack, which caused a disruption to the IT system. The type of ransomware used was Ryuk, a crypto-ransomware that blocks access to a system, device, or file until a ransom is paid.

Ryuk is often dropped on a system by other malware, or gains access via Remote Desktop Services. Victims are asked to deposit the ransom in a specific Bitcoin wallet. The ransom demand is usually between 15-50 Bitcoins, which amounts to between US$100,000 and US$500,000, depending on the conversion rate. From the moment Ryuk is in the system, it spreads out through the whole network and infects as many endpoints and servers as possible. Usually, it also encrypts backups.

In this case, the infection cycle started with the uploading of TrickBot malware to the company's IT systems. Ryuk was the last piece of the malware cycle inserted, encrypting the servers and IT systems. In an effort to prevent the spread of the ransomware, the company started to disconnect and shut down their servers and network connections. They found text files on the encrypted systems urging them to contact the attackers and pay approximately 2,000 Bitcoins in order to decrypt the files.

Regardless of whether or not a ransom is paid, the costs of a ransomware attack can be crippling. For this victim, the affected systems were down for several weeks, which caused an estimated Business Interruption (BI) loss of EUR 60 million. Incident response costs alone amounted to approximately EUR 20 million.

With forensic investigation still ongoing, not all details are yet available on how the malware entered the system. However, it is clear that the company had not invested enough in its network segmentation. Their flat network structure is thought to be responsible, in the most part, for enabling such a vast and speedy lateral spread of the ransomware across the different systems. Current analysis also suggests that a more centralised IT security approach might have further prevented the rapid spread of the virus and facilitated both earlier detection and a more streamlined response.

2. Mailing services company:

In 2018, a US-based company that offers digital printing, direct mail communication and electronic document management services was hit by a ransomware attack that managed to encrypt 200 PCs, 20 servers, 20 customer systems and around 50 industrial printers. The criminals behind the attack asked for a ransom of 25 Bitcoins (about US$150,000) in exchange for the decryption key. It is believed that the company fulfilled this request and the attackers remain unknown.

In addition to paying the ransom, the company had to notify approximately 500,000 individuals, as a significant amount of client data appeared to have been stolen by the criminals. Notification costs are estimated at US$350,000. On top of that, the company also suffered BI estimated at US$300,000. The forensics costs are estimated at US$850,000. All in all, the total loss has been estimated at US$1.5 million.

As you can see by the examples illustrated above, the cost of a ransomware attack can differ depending on the case. However, generally speaking and from our experience, the following can be estimated:

- The ransom itself usually amounts up to 10% of the total incident cost
- Emergency costs (IT Forensic, lawyers, PR, etc.) usually make up 30% of the total incident cost
- Business interruption, data recovery and additional costs usually make up the remaining 60%

Obviously, this varies depending on the type of incident, company, criminals behind the attack, maturity of the company, speed with which the intrusion is discovered (and, therefore, the speed and ability to block the spread), geographic location, and more. Regardless, it is clear that investing in IT security can be a wise and cost-effective decision.

Next, we discuss how to improve protection against ransomware.

Underwriting considerations and tips for Risk Managers

With the ever-evolving strains of malware and methodology of the modern-day cyber criminal, sadly there is no quick fix when it comes to defending your company from the threat of ransomware.

At Tokio Marine HCC, we believe that Cyber risk and readiness should be approached in line with the golden triangle model: People, Process, and Technology. Strong cyber security practices in all three of these interlinked fields are essential for overall cyber preparedness and will form the basis of our recommendations for risk managers in this paper.

Whilst there is no "one size fits all" solution, we have selected a few key practices from all three areas that will give a strong basis by which to strengthen cyber security against ransomware attacks.

PEOPLE:

Ensure your employees are united and confident in the best cyber and data security practices.

Enhance employee awareness:

Employee awareness should not be overlooked within an organisation. In fact, many Chief Information Security Officers (CISOs) think that there is no firewall as effective as the human firewall itself. Ensure training on data security and privacy best practices is delivered to all employees upon their arrival at the company and supplemented with annual refreshers. It may sound obvious, but make sure that employees know not to provide personal information when answering an email, unsolicited phone call, text message or instant message. Phishers will often try to trick employees into installing malware by claiming to be from an internal function such as IT, internal audit, or other positions of authority.

Formalised incident reporting processes should also be defined so that employees are aware of the protocol following an incident. This will allow streamlined incident response times by the relevant security teams and limit any potential damage or future attacks.

Phishing campaigns:

As an extension to the standard employee training phishing awareness campaigns, simulations are advisable, as they can help better prepare the workforce to recognise an attack.

- 1 in every 99 emails is a Phishing Attack[45]
- 98% of attacks in user inboxes contained no malware[46]
- Phishers are opportunistic: a 600% uptick in phishing emails was reported during the first month of the Covid-19 crisis[47]

The second point here is particularly poignant as it highlights that for the large part of all phishing emails, the widely used malware detection tools are useless. Without the presence of malware in the offending email, it is incredibly hard for detection and traffic filtering tools to identify the attack and raise a red flag.

As such, human judgement is imperative when it comes to detecting and avoiding phishing threats. Running frequent and varied phishing campaigns are a simple way to raise awareness of the threat within the company. They help increase report rates of suspect emails thus reducing the overall incident rate.

Failures to identify phishing emails should always be followed up with additional training to ensure there are no weak links in the business. Senior executives and those with elevated access privileges should also be subject to a more enhanced and targeted training, as it is likely that educated hackers will often target such employees for maximum impact.

PROCESS:

Make sure that your approach to Cyber Risk is consistent and that there is a good level of cyber hygiene.

Take regular back-ups:

It is a common misconception that back-ups are a 100% safeguard from ransomware attacks. In reality, your backup solution is also vulnerable if connected to a computer that gets hit with ransomware. To protect your ability to successfully restore your data from a back-up in the event of an incident, follow these key guidelines:

- **Isolate back-ups:** A recent study by Kaspersky Lab found that cyber criminals are increasingly targeting back-up storage, with internet connected storage proving to be the most vulnerable. Ensure that all back-ups are isolated from both your network and the internet to avoid infection. The more barriers there are between an infected system and its backups, the harder it will be for the ransomware to get to it.[48]
- **Test back-ups regularly:** The key message here is that you should not wait until the ransomware attack is activated to find out that your back-ups are also encrypted or deleted.
- **Use two methods concurrently:** For ultimate back-up security, use a variety of back-up methods concurrently so that if one is corrupted by ransomware, you still have other options. An option here could be to use both the cloud method (offering very quick Recovery Point Objective or 'RPO' duration) as well as taking physical tapes and storing these offsite, totally disconnected from the internet and network.

Most companies will rely on an external provider, at least for cloud-based back-up options, so it is important to identify these providers and make sure that they also have adequate IT and risk management procedures in place, as well as contractually defined indemnification agreements in respect of provider-side errors and negligence.

Vulnerability scanning and regular patching:

Vulnerability scanning should be rolled out across the cyber estate as a means of identifying any potential points of weakness on the network, or security holes that cyber criminals can exploit.

According to a recent study by the Ponemon Institute, there has been an increase in the average annual spending on vulnerability management activities to US$1.4 million in 2019 from an average of US$282,750 in 2018. Interestingly, the study also highlighted the benefits of automation of these processes, with 80% of the surveyed companies reporting that the use of automation allowed a reduction in the amount of time taken to respond to vulnerabilities.[49]

There are two main methods of undertaking these scans, namely *unauthenticated* where the test is performed from the perspective of a hacker with no network access, and *authenticated* which tests for vulnerabilities accessible to an inside 'trusted' user.[50]

Any vulnerabilities that are flagged should be addressed in order of their criticality to minimise the threat of being exploited, consequently preventing hackers from gaining access to the network.

As for patching, according to the recent Ponemon Institute study:

- 57% of cyber attack victims stated that applying a patch would have prevented the attack
- 34% of victims reported that they knew about the vulnerability before the attack

These statistics illustrate how important effective patch management is in order to maintain effective cyber security.[51]

When a patch is released by a software vendor, the vulnerability that it aims to address inevitably becomes common knowledge. Unfortunately, this provides a short-cut for hackers who can focus their attacks on those publicly disclosed unpatched vulnerabilities, rather than conducting time-consuming scans to identify those still unknown.

Key considerations regarding effective patch management include:

- Having a patch management process in place to ensure that patches are administered in a formalised and efficient manner. Inventories and risk classifications should be used to direct the order in which patch management should be prioritised.
- Patching cadence should be timely to close vulnerabilities as quickly as feasible. However, time should be left to allow for patch testing before deployment and a phased roll-out approach scheduled to allow further testing of patch security.
- Software should be consolidated where possible. Consolidation will ultimately mean fewer patches to apply and a far more efficient patch management process.
- Be prepared for scenarios where vendor patches cannot be applied for functionality reasons, or where patches are not provided for your legacy systems. In these scenarios, ensure that you lock the vulnerable system down as far as possible, isolating it from both the network and internet, with strict access controls, until you are able to ultimately phase these out of the network and upgrade.

Business Continuity Planning (BCP):

Whilst we are discussing all of the tools and processes available to help protect against a ransomware attack, it would be wise, at this stage, to point out that it is not an academic exercise. Sadly, research has shown us that it is not a matter of whether or not a company will be attacked, but a matter of when it will be attacked.

Therefore, it is essential to have a tailor-made and tested BCP plan to ensure that you know exactly what to do in the event of an incident, supplemented perhaps by a ransomware or phishing specific Incidence Response Playbook (IRP) for maximum clarity.

Crucial to this, is the ability to adquately identify which of your critical systems and databases are your "crown jewels". This will create an order for restoration to minimise any impact on business. These plans should be tested annually, at least, to ensure they are fit for purpose.

ISO standard 27031 provides useful guidance on the concepts and principles behind the role of information and communications technology in ensuring business continuity.

TECHNOLOGY

Make the most of the technology available to enhance your lines of defence against ransomware.

Network segmentation and segregation:

The vast majority of malware is written to elevate privileges and move laterally in an environment. Network segmentation and segregation will help contain any incidents and allow other areas of the network to remain uninfected.

Network segmentation means to divide a network into smaller partitions, independent from each other. This way, if a malicious program manages to infect one of the partitions, it will not be able to spread to the whole network, as the infection will not be able to expand outside the single partition (same concept as fire doors or bulkheads).

Network segregation is a complementary measure to segmentation and it regulates the access to the different network segments controlling communications between the different users.

For a more in-depth look, the Australian Cyber Security Centre recently published detailed guidelines on how network segregation and segmentation can successfully be achieved within an organisation.[52]

Back-up / disaster recovery infrastructure:

As already anticipated, a back-up / disaster recovery policy is essential to face a ransomware attack and mitigate possible systems downtime.

Choosing the right infrastructure is a key element for the set-up of an efficient policy and the choice should reflect the peculiarities of each organisation.

To assess a proper disaster recovery structure, two main concepts must be taken into account: Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

RPO is an indicator of the amount of data that can be lost without having a significant impact on the company's operations. Back-up frequency must be set directly based on this variable. For example, if the organisation can only allow itself to lose two hours' worth of data, minimum back-up frequency shall be set at two hours.

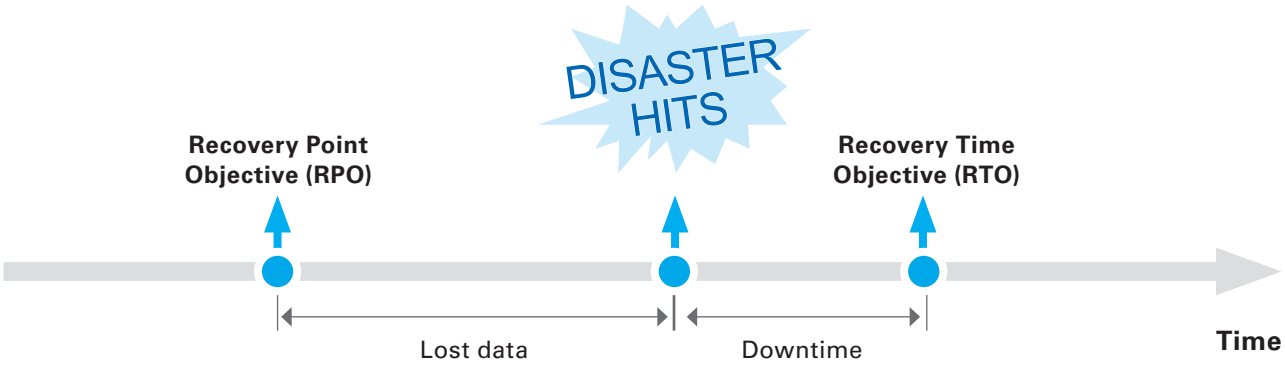
RTO is the maximum amount of downtime that a company can afford in case of system shutdown. The kind of back-up structure should be elected taking into account this figure.[53]

Ideally, both RTO and RPO should be minimised as much as possible, due to the high costs involved. However, having to reach a compromise in terms of back-up architecture and to choose a solution that fits both the risk profile identified and the budget allocated to the matter is inevitable.

There are two main recovery architecture structures: active-active and active-passive.

- **Active-active architecture:** data is synched almost instantaneously on off-site servers, making it a particularly uptime-driven solution. One of the downsides is that, in case of an attack, the active-active layout could fail in preventing a malware from spreading to the off-site servers. This option is also by far the most expensive and complex.
- **Active-passive architecture:** the off-site server stays inactive between back-up intervals. This solution will involve more downtime and data loss to occur, so it is essential that the back-up frequency is equal to or higher than the targeted RPO.[54]

Back-ups need to be tested regularly to make sure that the procedure is in line with the RPO/RTO goals. Companies with more sophisticated needs will use automated monitoring systems in order to be notified immediately in case of malfunctioning.



Data protection:

Depending on the amount and type of data held, proper security measures should be in place in order to mitigate data breach risk. This concept is also clearly underlined in the GDPR guidelines that instruct the controller and the processor of personal data to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Ideally, both data at rest and data in transit should be encrypted or protected in other ways, as well as networks and endpoint devices.

There are different methods that can be used to protect sensitive data:

Encryption: This is the most common method for protecting sensitive data. It disrupts readable data into an unreadable format using an algorithm. To revert the process and make data readable again, a secret key, held only by authorised individuals, is needed.[55]

There are different encryption levels: the more complex the algorithm, the less likely it is that someone could successfully guess and decrypt the data without the decryption key.[56]

Choosing a secure encryption method is also a key factor in guaranteeing a proper level of security. One of the most common and secure systems is the AES (Advanced Encryption Standard). It is a symmetric encryption algorithm (meaning that the same key is used to encrypt and decrypt the file) and it is the algorithm of choice for the US government when it comes to classified information.

A symmetric algorithm, however, can pose some challenges when an institution must manage a large quantity of keys, as each specific key is shared with the recipient. A possible solution is to switch to an asymmetric encryption method that is based on the combined use of two different keys, one public and one private, hence eliminating the need of sharing a specific single key.[57]

Apart from encryption, data can be protected in a number of other ways, for example, through masking techniques such as anonymisation and pseudonymisation.

Pseudonymisation: Through pseudonymisation, personal data is treated in a way that, unless matched with additional pieces of information, it cannot be tracked down to a single individual.

Anonymisation: This is similar to pseudonymisation, but differs in the fact that, while pseudonymisation can be reversed using information that is held separately, it should not be possible to reverse the process with anonymised data.

Multi-factor authentication: A popular tactic used by cyber criminals is to leverage stolen employee credentials to enter networks and distribute ransomware once inside. Credential compromise has recorded a 280% increase since 2016, with credentials often collected via phishing or harvested from past breaches.[58]

An efficient way to prevent such fraudulent access is to adopt multi-factor authentication (MFA) across all technology solutions, focusing on access to critical systems and data, and for all remote working access. Multi-factor authentication simply increases the number of authentication factors that are required to prove a user's identity.

These factors can fit within different categories, of which Security Boulevard identifies five:[59]

- **Knowledge:** Something known only to the user (password, PIN, username, security question)
- **Possession:** Something that the user owns (badge, token, ID)
- **Inherence:** Something the user is (meaning biometrics, such as fingerprints or facial recognition)
- **Location:** Where the user is
- **Time:** When the user accesses the network, a specific timeframe within which the user can authenticate

Artificial Intelligence (AI): The use of AI has become increasingly embedded as a method to improve a company's cyber immune system and facilitate the early detection of even the most sophisticated cyber attacks. Spending on AI-based cyber security systems is predicted to reach US$30.9 billion in 2025.[60]

AI tools have the advantage of going beyond pre-determined rules and assumptions to decide with artificial human intelligence what should be deemed 'normal' and what should be treated as suspicious or malicious behaviour.

Using billions of sources of data, these self-learning tools can complete analysis and react in a matter of seconds, allowing security analysts to respond to threats up to 60 times faster, without needing an extensive headcount.[61] As the cyber threat landscape continues to evolve and the attack surface area continues to grow, use of AI will be critical for cyber security functions to keep pace.

To apply this specifically to the threat of ransomware…

With the shift towards big-game hunting, hackers are apparently aware that their intrusions must become increasingly sophisticated to avoid early detection. Many hacker communities now prefer to use legitimate credentials to gain access to the network, to 'live off the land' and lay dormant within the network for a period of time. As a result, the hacker can reside within the victim's network unflagged until the optimum opportunity arises for them to execute their attack. This shift in approach has made it harder for traditional intrusion detection methods - previously identified from red flags such as: illegitimate email addresses, corrupt attachments, or noisy internal lateral movement and elevation of privileges - to be effective.

The use of an AI monitoring tool could help flag unusual yet discrete behaviour by generating an understanding of the typical behavioural patterns of roles or specific employees. This monitoring takes into account a huge range of sources and processes them quickly. Analysed factors include log-in hours, email contacts, file and application use or even trackpad patterns to determine if curser behaviour is human or bot-controlled.

Conclusion

We sincerely hope that this white paper has helped you better understand both the reality and gravity of the ransomware threat our society and businesses are facing.

Over a relatively short period of time, this cyber threat has come an incredibly long way. Its fast evolution is both fascinating and frightening, and shows little sign of slowing. As ransomware continues to evolve and adapt, we turn our hopes for survival towards awareness and pro-activity.

When typing these final words (April 2020), we have just been made aware of a new significant ransomware attack made against a Power & Utility (P&U) company. This Portuguese company has been victim to the RagnarLocker malware, which illegally gained access to 10 terabytes of confidential data (billing info, contracts, transactions, clients and partners...) and attempted to extort 1.580 Bitcoins (EUR 10 million).

Ransomware creativity continues to break boundaries as criminals strive to stay one step ahead of the available defensive tools. Combine this creativity with the ever-increasing volume and value of data driving our modern world, and we see that the attack landscape is broadening, providing even more territory for ransomware to roam. As long as there are cyber vulnerabilities, ransomware is sure to lurk around.

It is as difficult to anticipate the shape that ransomware will assume in the future, as it is to detect a zero-day vulnerability. However, board directors, risk managers and CISOs alike might start reconsidering their business model, their dependence on data and how they could reinforce their business with greater redundancy and resiliency features.

Ransomware is the type of threat that pushes you to rethink your business model.

From North America to Asia via Continental Europe, from SMEs to large corporations, whether a retailer, transportation company, financial institution, or other, every single business is at risk.

If we can leave you with one key message, it is to not underestimate this threat any longer. The threat is real, the threat is here!

However, as light is able to enter the darkest and scariest places in this world, education and awareness are the keys to defeating the expansion of the ransomware threat.

As we have repeatedly stressed, the human paradox is a key element of any relevant cyber security strategy. People within your organisation or those interacting with it (service providers, suppliers, clients…) are likely to be the biggest weakness in your cyber security. Indeed, it is well known that around 90% of any cyber incident can be traced back to human error.

Yet there is no firewall as strong or resilient as the human firewall itself. It is very unfortunate that the Achilles heel of so many ransomware victims could have been so easily converted into their greatest strength had it been addressed through investing in people, education and awareness.

So, to all those who believe that education is expensive, please do not wait to see how much ignorance can cost.

Interesting reading for Risk Managers:

NIST Framework

Developed by the United States National Institute of Security and Technology, the NIST Framework provides guidance based on existing standards, guidelines, and practices for organisations to better manage and reduce cyber security risk within an organisation.

This flexible model aims to simplify complex cyber practises to help an organisation tailor their cyber security processes, considering:

The Tiers: determining the appropriate level of rigour for the cyber security programme. This is where risk appetite, mission priority and budget are taken into consideration.

The Core: managing and reducing cyber security risks in a way that complements the existing cyber security and risk management processes. The Core is divided into 5 key functions: Identify, Protect, Detect, Respond & Recover.

Profiles: unique alignment of a company's requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core.

NIST framework pdf:
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST overview video:
https://www.nist.gov/video/cybersecurity-framework-version-11-overview

ISO/IEC 27031 standard Information technology. Security techniques. Guidelines for information and communication technology (ICT) readiness for business continuity.

ISO 27031 leverages both information security and business continuity expertise to provide a framework to guide ICT-related readiness for business continuity.

The standard identifies all relevant aspects, including performance criteria, design, and implementation details, for improving ICT readiness as part of the organisation's ISMS, with the ultimate aim of ensuring business continuity through effective use of a disaster recovery program, focussed on six key principles:

1. **Protecting** the ICT environment from incidents, failures and disruptions
2. **Detecting** incidents at the earliest possible time
3. **Reacting** to incidents as efficiently as possible
4. **Recovering** by identifying and implementing appropriate recovery strategies
5. **Operating** in disaster recovery mode
6. **Returning** to normal operations

By adopting this framework, an organisation will be able to better measure its ICT continuity, security and readiness to survive a disaster in a consistent and recognised manner.

ISO/IEC 27031:
https://www.iso.org/standard/44374.html

About us

About Tokio Marine HCC

Tokio Marine HCC is a leading specialty insurance group conducting business in approximately 180 countries and underwriting more than 100 classes of specialty insurance. Headquartered in Houston, Texas, the company is comprised of highly entrepreneurial teams equipped to underwrite special situations, companies and individuals, acting independently to deliver effective solutions. Our products and capabilities set the standard for the industry, as many of our approximately 3,000 employees are industry-leading experts.

Tokio Marine HCC's major domestic insurance companies have financial strength ratings of "A+ (Strong)" from Standard & Poor's Financial Services LLC, "A++ (Superior)" from A.M. Best Company, Inc., and "AA- (Very Strong)" from Fitch Ratings; its major international insurance companies have financial strength ratings of "A+ (Strong)" from Standard & Poor's Financial Services LLC.*

Tokio Marine HCC is part of Tokio Marine, a premier global company with a market cap of approximately US$38 billion.**

*At the time of printing
**Market cap as of 31/12/2019

About Tokio Marine Group

Founded in 1879, the Tokio Marine Group consists of Tokio Marine Holdings, including 249 subsidiaries and 22 affiliates, and is engaged in the domestic non-life insurance, domestic life insurance, international insurance, and financial and general businesses.

Tokio Marine Group operates a worldwide network that spans 45 countries and regions with over 40,848 employees and has built a structure that can respond to the diverse needs of customers in each country. Through stable business expansion, profit growth and high capital efficiency, the company has a market cap of ¥3.8 trillion.**

The insurance business is based upon the commitment to be there for our clients in their moment of need. It is a people's business, therefore our people and the trust they engender is everything. We will continue to build a workforce that has been empowered and enabled to think and act from the customer's point of view and to live up to our corporate vision to *Be a Good Company*.

*Market cap as of 31/12/2019

Our cyber capabilities

At Tokio Marine HCC, we understand that cyber risks are constantly evolving and the attack surface is ever-broadening. Coverage, therefore, needs to contemplate today's threats and anticipate tomorrow's. Our offer has been devised by our dedicated cyber underwriting, claims and product development teams and designed so that coverage can be seen at a glance. A wide range of cyber events are considered and clients can extend and adapt further coverage to best suit their set-up and needs.

Our key differentiators:
- Clear, straight-forward language used in our wording makes it is easy to follow and understand
- Tailor-made cyber incident panel
- Fully developed menu of preventative consulting services

Our cyber response solution:
- Dedicated team with a wealth of experience and expertise in cyber incident management
- Simple notification process including localised emergency numbers
- Comprehensive panel of incident response partners and first-in-class local language service via our strategic partnership with Crawford & Company
- On-hand global expert assistance (IT forensic, lawyers, PR firms)
- Fully trained in-house claims handlers with local language capabilities

Our reach:
- UK, Continental Europe, Asia, Pacific, Middle East, Latin America and Africa
- Sectors include Financial Institutions, Manufacturers, Communication Media & Technology, Retailers, Power & Utilities, Transportation, amongst others
- Our clients are companies with US$250 million to multi-billion dollar annual revenues

We have a financial capacity of up to EUR 25 million (US$25 million or GBP 15 million) per Cyber policy on primary or excess coverage.

Meet the authors

Xavier Marguinaud

Head of Cyber - International Financial Lines

Tel: +34 93 530 7439
Email: xmarguinaud@tmhcc.com

Xavier Marguinaud is Head of Cyber, overseeing and coordinating Tokio Marine HCC's Cyber strategy for EMEA, APAC and LATAM. Previously, Xavier worked at Marsh occupying positions such as New Zealand Cyber Risk Specialty Head, Financial Lines Senior Risk Advisor, and Cyber Product Champion - France. He launched his career in the Risk and Insurance department of Publicis Groupe.

Today, Xavier is a well-known figure in the cyber insurance industry. He often imparts his knowledge hosting cyber conferences for Tokio Marine HCC, or as a guest speaker at major cyber conferences hosted worldwide. He has also been interviewed for insurance publications both on screen and in print, and has written a number of articles on the topic of cyber risk and insurance.

Xavier holds two master's degrees, one in Risk Management from Kedge Business School (IMR) and another in Crisis Communication and Management from ESG Paris Management School.

Xavier obtained his certificate in Cyber Resilience and Security by Axelos in 2015, and is a Certified Information Security Manager (CISM) by ISACA since 2018.

Christie Jones

Assistant Underwriter - Cyber Financial Lines

Tel: +44 (0)7545 942 763
Email: cjones1@tmhcc.com

Christie joined Tokio Marine HCC in 2019 as an Assistant Underwriter to the Cyber team, based out of the London office. As the cyber relay for the UK, she reviews most of the cyber opportunities for this market and is involved in several projects related to TMHCC's Cyber offer (wording, services, underwriting tools) as well as auditing cyber opportunities from other regions.

Previously, she completed an underwriting graduate scheme at Aspen Insurance where she worked within a range of business classes including; Professional Indemnity, Crisis Management and Cyber and Technology. Christie holds a bachelor's degree from Exeter University in French and International Management.

Davide Donna

Underwriter Financial Lines

Tel: +34 93 530 7412
Email: ddonna@tmhcc.com

Davide Donna joined Tokio Marine HCC in 2015 and is a financial lines underwriter focusing on the Italian, Turkish and Israeli territories. He recently became cyber relay for his team, coordinating the cyber book and developing specific knowledge on the line of business.

Davide holds a bachelor's degree in Business Administration and Management from Bocconi University and a master's degree in Finance from ESADE Business School.

Endnotes

[1] Information Security Group. Ransomware Costs May Have Hit $170bn in 2019. 2020. Retrieved 8 July 2020, from https://www.infosecurity-magazine.com/news/ransomware-costs-may-have-hit-170/

[2] Coveware. Q1 2020 Ransomware marketplace report. (2020) Retrieved 18 June 2020, from https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

[3] Kaspersky.com. What is Wannacry Ransomware? (2020). Retrieved 18 June, from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[4] CrowdStrike. Big Game Hunting with Ryuk: Another lucrative targeted ransomware. (2019). Retrieved 18 June 2020, from https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

[5] Coveware. Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate. (2020). Retrieved 18 June 2020, from https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

[6] Locky was a ransomware released in 2016 and had the ability to encrypt over 160 file types. This ransomware was spread via fake emails with an infected attachment (phishing) and targeted designers, developers, engineers and testers.

[7] WannaCry was designed to exploit a vulnerability in Windows, released in 2017, spread across 150+ countries and infected around 230.000 computers. Created originally by the US National Security Agency (NSA), it was leaked by the Shadow Brokers group and caused an estimated $4bn in financial losses worldwide.

[8] CryptoLocker was first seen in 2007. With the ability to search for valuable files and encrypt them.

[9] Resurgence of Petya ransomware, GoldenEye is known as the sibling of WannaCry and, in 2017, hit over 2.000 high profile targets (e.g. oil producers and bank).

[10] DigitalHealth.net. Government puts costs of Wannacry to NHS at GBP 92m. (2018). Retrieved 18 June 2020, from https://www.digitalhealth.net/2018/10/dhsc-puts-cost-wannacry-nhs-92m

[11] ZeroDay.net. Tick, tock: Jigsaw ransomware deletes your files as you wait. (2016). Retrieved 18 June 2020, from https://www.zdnet.com/article/tick-tock-jigsaw-ransomware-deletes-your-files-as-you-wait/

[12] KnowBe4, Bad Rabbit Ransomware. (2020). Retrieved 13 July 2020, from https://www.knowbe4.com/bad-rabbit-ransomware

[13] TrendMicro. Ryuk Ransomware Information. (2019). Retrieved 18 June 2020, from https://success.trendmicro.com/solution/1123892-ryuk-ransomware-information

[14] Coveware. Q1 2020 Ransomware marketplace report. (2020). Retrieved 18 June 2020, from https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

[15] CrowdStrike, 2020 Global Threat Report. (2020). Retrieved 20 May 2020, from https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/

[16] FireEye. (2016). Effective Ransomware Responses (pp. 1-13). Retrieved 01 May 2020, from https://www.fireeye.com/solutions/ransomware/wp-effective-ransomware-reseponses.html

[17] Sjouwerman, Stu. Ransomware on the rise: The evolution of a cyberattack. TechBeacon.com. Retrieved 18 June 2020, from https://techbeacon.com/security/ransomware-rise-evolution-cyberattack

[18] Knowbe4. AIDS Trojan or PC Cyborg Ransomware. (2020). Retrieved 18 June, from https://www.knowbe4.com/aids-trojan

[19] RSA named after the three creators of the algorithm: Ron Rivest, Adi Shamir and Leonard Adleman.

[20] Knowbe4. Archiveus Trojen. (2020). Retrieved 18 June, from https://www.knowbe4.com/archiveus-trojan

[21] Varonis, CryptoLocker, everything you need to know. (2020). Retrieved 18 June from, https://www.varonis.com/blog/cryptolocker/

[22] Dell SecureWorks. CryptoLocker Ransomware. (2013). Retrieved 1 July 2020, from https://www.secureworks.com/research/cryptolocker-ransomware

[23] DigitalGuardian.com. A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time. (2019). Retrieved 18 June, from https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

[24] KnowBe4. Symantec: Crypto Ransomware Phishing Up 700 Percent in 2014. (2014). Retrieved 15 June 2020, from https://blog.knowbe4.com/bid/396484/symantec-crypto-ransomware-phishing-up-700-percent-in-2014

[25] Advisen, Brew, O, Cookson L, Kriesel, T, Sauter, A. Ransomware-as-a-Service (Webinar). (2020, 29 April). CyberCube. Retrieved 01 July 2020, from https://www.advisenltd.com/ransomware-as-a-service-an-evolving-business-model

[26] Kaspersky.com. What is Wannacry Ransomware? (2020). Retrieved 18 June, from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[26] National Cyber Security Centre. "Russian military 'almost certainly' responsible for destructive 2017 cyber attack". (2018). Retrieved 18 June, from https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

[28] CrowdStrike. Big Game Hunting with Ryuk: Another lucrative targeted ransomware. (2019). Retrieved 18 June 2020, from https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

[29] SynergySoftware.com. Ryuk nasty and expensive ransomware (2019). Retrieved 19 June, from http://www.synergy-software.com/blog/?p=6651

[30] Advisen, Brew, O, Cookson L, Kriesel, T, Sauter, A. Ransomware-as-a-Service (Webinar). (2020, 29 April). CyberCube. Retrieved 01 July 2020, from https://www.advisenltd.com/ransomware-as-a-service-an-evolving-business-model

[31] Centre for Internet Security. Security Primer – Ransomware. (2020). Retrieved 01 July 2020, from https://www.cisecurity.org/white-papers/security-primer-ransomware/

[32] Coveware. Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate. (2020). Retrieved 18 June 2020, from https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

[33] Advisen, Brew, O, Cookson L, Kriesel, T, Sauter, A. Ransomware-as-a-Service (Webinar). (2020, 29 April). CyberCube. Retrieved 01 July 2020, from https://www.advisenltd.com/ransomware-as-a-service-an-evolving-business-model

[34] Coveware. Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate. (2020). Retrieved 18 June 2020, from https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

[35] BleepingComputer. Sodinokibi Ransomware to stop taking Bitcoin to hide money trail. (2020) Retrieved 13 July 2020, from https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-to-stop-taking-bitcoin-to-hide-money-trail/

[36] Malawarebytes. Understanding the Depth of the Global Ransomware Problem. (2017). Retrieved 13 July, from https://go.malwarebytes.com/OstermanRansomwareSurvey.html

[37] Coveware. Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate. (2020). Retrieved 18 June 2020, from https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

[38] Coveware. The Marriage of Data Exfiltration and Ransomware. (2020) Retrieved 13 July 2020, from https://www.coveware.com/blog/marriage-ransomware-data-breach

[39] Panda Security. Ransomware has a new trick: pay up or suffer a data breach. (2020). Retrieved 13 July 2020, from https://www.pandasecurity.com/mediacenter/security/ransomware-data-breach-blackmail/

[40] Linn Foster Freedman. ExecuPharm Data Stolen in Ransomware Attack Published on Internet. (2020, 30 April). Retrieved 01 July, from https://www.dataprivacyandsecurityinsider.com/2020/04/execupharm-data-stolen-in-ransomware-attack-published-on-internet/

[41] Kaspersky. Story of the year 2019: Cities under ransomware siege. (2019). Retrieved 13 July 2020, from https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

[42] SecureWorld. Baltimore, $18 Million Later: 'This Is Why We Didn't Pay the Ransom'. (2019). Retrieved 13 July 2020, from https://www.secureworldexpo.com/industry-news/baltimore-ransomware-attack-2019

[43] Kaspersky. Story of the year 2019: Cities under ransomware siege. (2019). Retrieved 13 July 2020, from https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

[44] KPMG. The rise of ransomware during COVID-19 (2020). Retrieved 13 July 2020, from https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html

[45] Darktrace. Phishing emails sneak into office 365. (2020). Retrieved 29 June 2020, from https://www.darkreading.com/cloud/25--of-phishing-emails-sneak-into-office-365-report/d/d-id/1334397

[46] Darktrace. Phishing emails sneak into office 365. (2020). Retrieved 29 June 2020, from https://www.darkreading.com/cloud/25--of-phishing-emails-sneak-into-office-365-report/d/d-id/1334397

[47] KnowBe4. 2020 phishing benchmark report. (2020). Retrieved 29 June 2020, from https://www.knowbe4.com/phishing

[48] Kaspersky. Kaspersky finds ransomware now targeting back-up data. (2019). Retrieved 29 June 2020, from https://usa.kaspersky.com/about/press-releases/2019_kaspersky-finds-ransomware-now-targeting-back-up-data

[49] The Ponemon Institute. Costs and Consequences of Gaps in Vulnerability Response. (2019). Retrieved 29 June 2020, from https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

[50] Tech Target. Vulnerability Scanning. (2020). Retrieved 29 June 2020, from https://searchsecurity.techtarget.com/definition/vulnerability-scanning

[51] The Ponemon Institute. Costs and Consequences of Gaps in Vulnerability Response. (2019). Retrieved 29 June 2020, from https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

[52] Australian Cyber Security Centre. Implementing Network Segmentation and Segregation. (2020). Retrieved 01 July 2020, from https://www.cyber.gov.au/publications/implementing-network-segmentation-and-segregation

[53] MSP360. RTO vs. RPO: Two Means Toward the Same End. (2020). Retrieved 01 July 2020, from https://www.msp360.com/resources/blog/rto-vs-rpo-difference/

[54] Atlantic Metro. Active-Active vs Active-Passive Configurations for BCDR. (2020). Retrieved 30 June 2020, from https://www.atlanticmetro.net/active-active-vs-active-passive/

[55] Norton. What is encryption and how does it protect your data? (2020). Retrieved 30 June 2020, from https://us.norton.com/internetsecurity-privacy-what-is-encryption.html

[56] Cloudfare. What is Encryption? (2020). Retrieved 30 June 2020, from https://www.cloudflare.com/learning/ssl/what-is-encryption/

[57] Norton. What is encryption and how does it protect your data? (2020). Retrieved 30 June 2020, from https://us.norton.com/internetsecurity-privacy-what-is-encryption.html

[58] SecureWorld. 2019 State of the Phish: Credential Compromise and Data Loss Have Soared Since 2016. (2019). Retrieved 30 June 2020, from https://www.secureworldexpo.com/industry-news/2019-sotp-credentials-and-data-loss

[59] Security Boulevard. What is Multi-Factor Authentication (MFA)? (2019). Retrieved 30 June 2020, from https://securityboulevard.com/2019/10/what-is-multi-factor-authentication-mfa/

[60] Forbes. 10 ways AI and Machine Learning are improving endpoint security. (2019). Retrieved 29 June 2020, from www.forbes.com/sites/louiscolumbus/2019/09/25/10-ways-ai-and-machine-learning-are-improving-endpoint-security/#104b7b272db0

[61] IBM. Artificial intelligence for a smarter kind of cybersecurity. (2019). Retrieved 29 June 2020, from www.ibm.com/uk-en/security/artificial-intelligence

TOKIO MARINE HCC

Contact Us

Barcelona

Tokio Marine Europe - Spanish Branch
Torre Diagonal Mar
Josep Pla 2, Planta 10
08019 Barcelona, Spain
Tel: +34 93 530 7300

London

HCC International
Fitzwilliam House, 10 St. Mary Axe
London EC3A 8BF, United Kingdom
Tel: +44 (0)20 7648 1300
Lloyd's Box 252, Second Floor

Munich

Tokio Marine Europe - German Branch
Rindermarkt, 16
80331 Munich, Germany
Tel: +49 89 3803 4640

A member of the Tokio Marine HCC group of companies