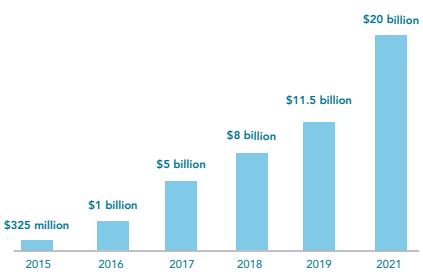
TECHNICAL NEWSLETTER
#51 - July 2020

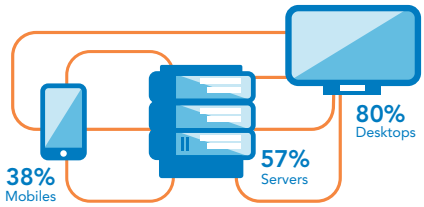
DECRYPTING RANSOMWARE

RANSOMWARE IS GAINING MOMENTUM

Over the past 3 years, ransomware has jumped into the spotlight in the cyber threat landscape. Annual ransomware demands have multiplied by ten. Ransomware is a type of malicious software that allows a hacker to restrict access, through encryption, to an individual's or a company's vital information until some form of payment is made. There is no guarantee that the data will actually be decrypted following this payment.



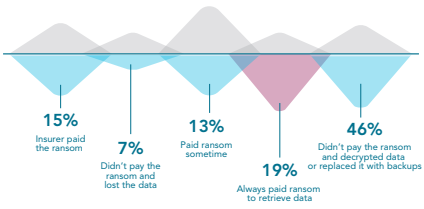
ANNUAL COST OF RANSOMWARE ATTACKS



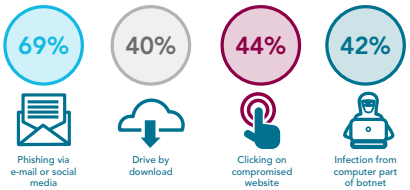
DEVICES AFFECTED IN 2019

Operational impacts in 2016

40h	**Employee working hours** On an average, estimated 40 employee hours were lost in decrypting/replacing files with backup
19%	**Stopped business** Nearly 19% of companies had to stop business immediately after discovering a ransomware attack
3.5%	**Higher stakes** 3.5% said lives were at stake because of ransomware's debilitating effects

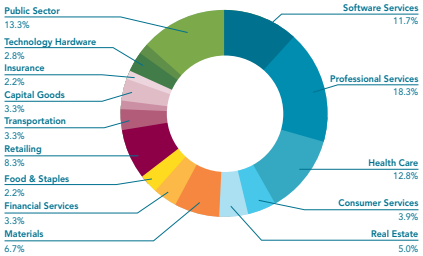


RANDSOM PAYMENT STATISTICS IN 2019



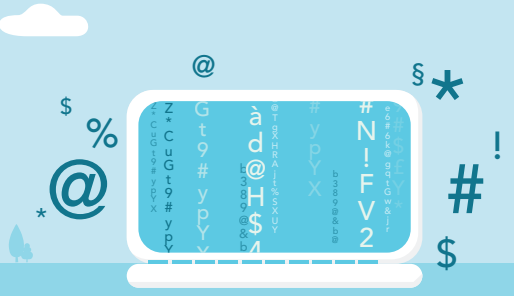
HOW DID ATTACKERS GAIN ACCESS?

The three sectors most impacted by ransomware are professional services, the public sector and healthcare.



COMMON INDUSTRIES TARGETED BY RANSOMWARE IN Q2 2019

Sources: MalwareFox – Ransomware statistics in 2019. Coveware – Q3 2019 ransomware marketplace report. Spin Backup – 24 recent ransomware attacks in 2019. Malwarebytes – The global impact of ransomware on business



THE PURPOSE OF RANSOMWARE

The main goal of this malicious software is the extortion of money from its victims. It blocks victims' access to their data / devices through encryption, demanding a ransom from them to unblock that access. Ransomware can, for example, be spread through malicious links or attachments in emails. When the recipient opens the link or attachment, the malware encrypts data and monetizes access to the decryption key.

Attackers have developed two main ways to monetize the files on a victim's computer – the first is to demand a ransom to decrypt them, and the second is to demand a ransom to avoid publicly releasing them.

THERE ARE TWO MAIN CATEGORIES OF RANSOMWARE

Cryptor or crypto ransomware encrypts data on the victim's machine, rendering it inaccessible. This situation could be compared to locking items away inside the victim's home – the victim has no problem entering his home, but he cannot access the locked items.

Blocker or locker ransomware totally locks a computer or other devices, rendering them unusable. This situation can be compared to a changed lock on the victim's front door: he can no longer even enter his house.

ENCRYPTION, DECRYPTED

Beyond the loss of money, ransomware can have a major operational impact on businesses.

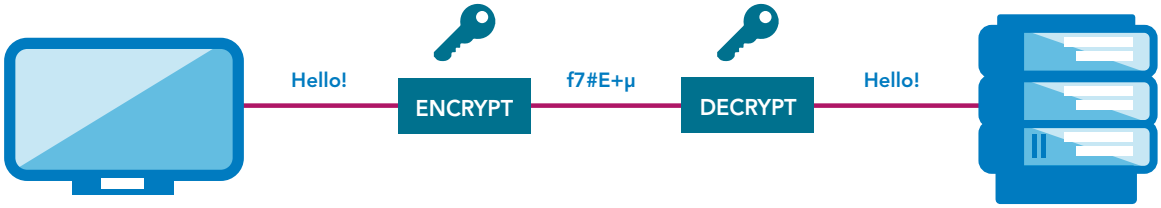
According to the anti-malware company Malwarebytes[1], nearly 19% of companies worldwide had to stop business immediately in 2016[2] after discovering a ransomware attack. Once infected, victims have several options:

- Pay the ransom and hope that the attacker will send the key to recover the encrypted data
- Restore data from backup
- Lose the files
- Try to decrypt the encrypted files, for example using the "brute force" decryption technique, which tries all possible decryption keys until the right one is found.

HOW DOES ENCRYPTION WORK?

Encryption is the conversion of data from a readable format into an encoded format that can only be read once it has been decrypted with a decryption key[3].

There are so many different decryption keys that finding the right one through "brute force" (see above) would require more decryption attempts than there are atoms in universe – on a standard desktop computer, it would take around 6.4 quadrillion years!



1. Malwarebytes, The global impact of ransomware on businesses
2. https://www.malwarebytes.com/pdf/infographics/global-impact-of-ransomware-on-business.pdf
3. https://www.kaspersky.com/resource-center/definitions/encryption

DECRYPTING WITHOUT PAYING THE RANSOM?

Occasionally hackers make mistakes and it is possible to decrypt encrypted files more rapidly than expected. For example, this can happen:

- If the length of the key is smaller than expected, it is possible to find the decryption key by testing all the combinations
- If the decryption key is still present in the computer's memory, it can be retrieved to decrypt files.

Nevertheless, it is extremely unlikely that ransomware victims can will be able to decrypt files by leveraging encryption mistakes.

RANSOMWARE ATTACK ON A MAJOR CONSTRUCTION COMPANY

On January 30, 2020, a ransomware attack was detected at a major construction company. This ransomware, called Maze, encrypted a large amount of data. The company was forced to shut down its IT systems. It is believed that the hackers requested a ransom of USD 10 million (NB: this has not been confirmed by the company). In addition, on their website ("mazenews.top") the hackers published a password-protected 1.2 GB archive file supposedly containing the company's data, but there is no evidence that this archive file actually contains data from the company's systems.

Maze ransomware was first discovered in May 2019. This ransomware is also known as ChaCha ransomware because of its encryption algorithm ChaCha20.

Maze ransomware is managed by – at least – one hacker group specializing in targeted attacks. The ransomware uses sophisticated techniques formerly employed by nation state actors for espionage purposes.

Maze's *modus operandi* is to silently penetrate the victims' network as deeply as possible, stealing data and implanting file encryption capacities along the way. When the ransomware is finally triggered, a vast amount of data has been encrypted, sometimes including back-ups, and a high volume of data has been exfiltrated from the network.

The blackmail is then twofold: pay the ransom to recover encrypted data and to prevent hackers from publicly releasing stolen data.

THE NEW RANSOMWARE ECONOMY

Ransomware, as a form of cyber extortion, is one of the most prolific criminal business models in existence today, mostly due to the multimillion-dollar ransoms criminals demand from individuals and corporations. Since the first ransomware attacks witnessed in 1989, experts have observed a regular expansion of this type of attack. And ever since ransomware began to be created in exchange for rent or commission (otherwise known as Ransomware-as-a-Service), the frequency has drastically increased. Researchers classify the evolution of ransomware in two steps: before and after Ransomware-as-a-Service. The rise of Ransomware-as-a-Service brought new targeted attacks, which are also known as "Big Game Hunting".

BIG GAME HUNTING

Experts have observed a paradigm shift in the evolution of ransomware targets:

- From individuals to corporations
- From random to targeted attacks

From individuals to corporations

In the past, ransomware has predominantly targeted private individuals. At first sight, this may not appear to be lucrative.

The payout for a single attack could be anywhere between USD 100 and USD 1000 (more recently, ransom payments have been made in Bitcoin). But hackers play the numbers game: they can reach several victims using the same phishing campaign, for instance. Moreover, individual computer users remain an "easy target": weak security protection, no recent backups to restore data, etc. Victims are likely to pay a ransom if it is a reasonable amount, rather than risking the loss of personal data.

Recently, several factors have driven attackers to shift their focus, targeting larger organizations across a new range of business sectors (big companies, SMEs, police departments, nonprofit organizations, universities, hospitals, etc.)

The main factor involved is money, because businesses are a more lucrative target for extorters than individuals:

- They depend on data for their activities (so they have a greater incentive to pay the ransom)
- They have greater financial capacity with which to pay the ransom (fewer targeted victims can make larger sums of money)
- They are highly vulnerable to ransomware (network distribution, high level of mobility and remote employees)

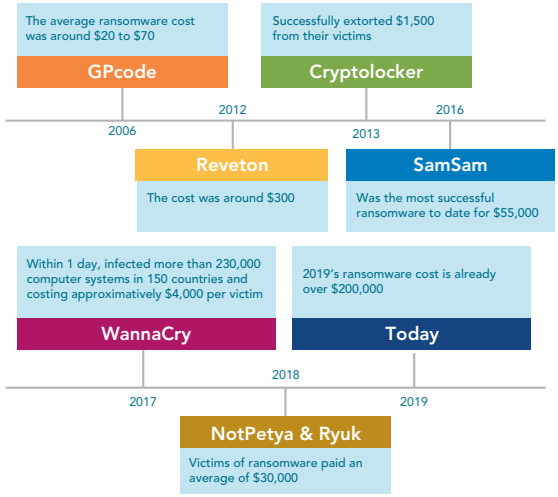
Pressure on companies from ransomware can increase in line with the number of people they employ, the amount of assets they have and the diversity of their locations.

From random to targeted attacks

In the early days of ransomware attacks, hackers targeted one-to-one victims. Once the victim was identified, attackers sent them a "generic ransomware program". The ransomware was not specifically designed for the victim's information system, but the victim was clearly chosen.

Then, ransomware attacks shifted to massive and random campaign mode. The main goal was to target as many victims as possible with generic ransomware: quantity first.

Now, the trend has moved back to targeted attacks, but in both an intentional and a technical way. This means that ransomware is now designed to impact a specific targeted company (based on knowledge of the technologies used, of the network's infrastructure, processes, IAM rules, non-patched vulnerabilities, and so on.).



Source: Ransomware demands skyrocket – Network access

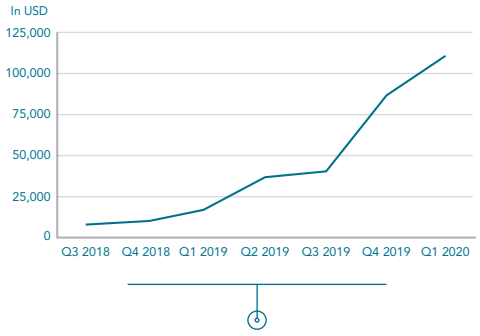
These targeted attacks are also known as Big Game Hunting. Over the past four years, Big Game Hunting attacks have drastically increased. They use methods and techniques previously only employed by state-sponsored hackers for spying operations. All technologies are now vulnerable to ransomware attacks: Windows, Linux/Unix and Mac OS.

Year, name	Description
May 2015, ransomware-as-a-service [1]	Using a TOR website, atackers could create ransomware for free The site handles payment and takes a 20 percent cut of the ransom
2015, Tor sites [1]	As the name implies, it targets Linux systems. It encrypts both data files and files associated with web applications
September 2015, LockerPin [1]	It infects Android systems and changes the PIN
Nov 2015, Linus.Encoder.1 [1]	It was discovered by Dr Web, a Russian computer security firm
November, fourth iteration of CryptoWall [1]	It includes a modified protocol to help avoid detection Additionally, it alters the file names when it encrypts files, making it harder to determine what files were actually encrypted
January, 2016. JavaScript-only [1]	It is a ransonware-as-a-service Multi-platform attack, including Linus and Mac OSX
April, Petya [1]	Makes the whole hard disk inaccessible until the ransom is paid It does this by overwriting the master boot record (MBR) of the infected computer Without the MBR, the operating system cannot reconstruct the unencrypted files
KeRanger, Jan, 2016 [1]	KeRanger is first ransomware attack targeting Apple system It takes three days to activate and is designed to encrypt more than 300 file types
Xbot, Feb, 2016 [1]	To target Android services in Australia and Russia Tries to steal online banking details
Jigsaw, 2016 [8]	Embeds an image of the clown from the Saw movies into a spam email, ransom payment of USD 150, according to Webroot
Locky, July, 2016 [1]	Added a failsafe mechanism that begins encrypting files even if the ransomware cannot request a unique key from the criminals' servers due to the target computer either being offline or blocking the communica-tions (Constantion, 2016c)
NotPeya, 2017 [8]	It comes with a fake software update, harms systems of more than 100 countries
Jeff, 2017 [8]	It attacked in May 2017 with spam mail and collected money in form of bitcoin

Source: Ransomware: Evolution, Target and Safety Measures – International Journal of Computer Sciences and Engineering

Soaring ransoms

Since 2019, experts have observed an increase in the average ransom payments made by large companies.
Targeted attacks mostly involve blackmail, to force the victims to pay the ransom.
There are various blackmailing techniques, including threatening to shut down systems and operations and to publicly disclose data - personal data, sensitive data, credit card data, and so on.



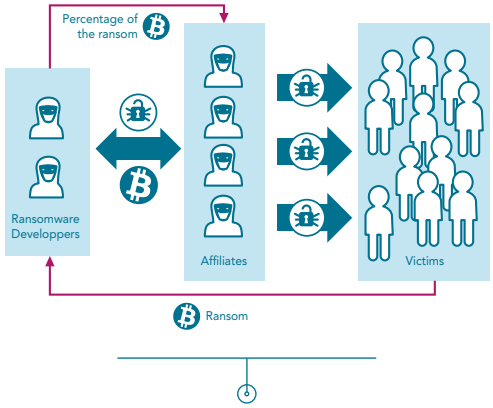
AVERAGE RANSOM PAYMENT BY QUARTER

Source: Coveware

RANSOMWARE-AS-A-SERVICE (RaaS)

In the Ransomware-as-a-Service (RaaS) "business model", ransomware can be sold to other criminals to enable them to attack IT systems. As part of a targeted cyber-attack, hackers buy all or part of the malicious resources they need to perform the attack. For example, on the black market they can buy the network accesses previously compromised by another hacker group.

At the beginning of the chain, the developers create the malware. Then they delegate the job of infecting systems to affiliates, who are responsible for spreading the ransomware and generating infections. If payment is made, part of it goes to the ransomware developers and the rest is paid to the affiliates. This model is based on task sharing. Sophisticated ransomware developers focus on developing the malware while their affiliates are in charge of finding and infecting targets. The affiliates, who focus purely on this part of the process, run the greater risk of detection.



RANSOMWARE-AS-A-SERVICE (RaaS) MODEL

Source: McAfee, GandCrab RaaS model

BLURRY STATISTICS BUT CLEAR TREND CONSENSUS

Until now, there has been no consolidated vision of ransomware attacks, only partial views based on a variety of tools and methodologies. As cyber risk is a recent phenomenon, there is not a great deal of hindsight in terms of the frequency and the severity of cyber incidents. Statistics are provided by cyber threat analysis tools, which give a subjective vision depending on the software publishers concerned. These points may explain why there are differences in market reports about the main countries impacted by ransomware attacks. Nevertheless, existing reports do seem to identify four major target regions for ransomware attacks: the USA, Asia, Western Europe, and the Middle East (in no particular order). Free tools showing real-time attacks and daily geographical statistics are increasingly becoming publicly available. For example, the SonicWall Live Cyber Attacks page shows worldwide attacks in real time[4], the top three attack origins and targets, security news in specific ransomware categories, and so on.

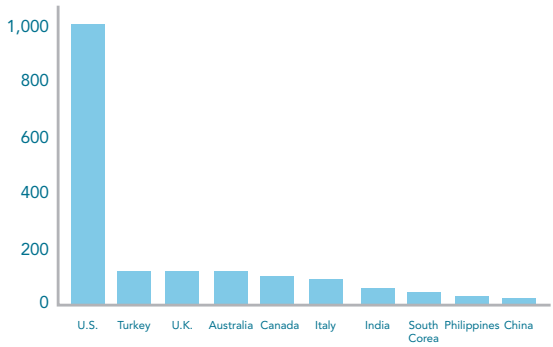
Although experts disagree on the top locations for ransomware attacks, they all agree that 2019 was a boom year for ransomware.

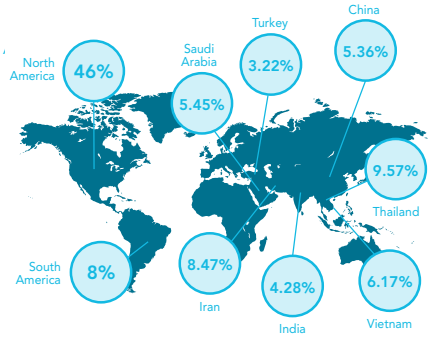
4. https://securitycenter.sonicwall.com/m/page/worldwide-attacks

A few 2019 geographical ransomware statistics:

Top 10 countries attacked by encryptors

	Country	%
1	Bangladesh	13.78
2	Uzbekistan	7.20
3	Mozambique	6.08
4	Turkmenistan	4.23
5	Ethiopia	3.97
6	Nepal	3.86
7	Afghanistan	2.45
8	Vietnam	2.34
9	China	1.94
10	India	1.91





EXTRACTS FROM 2019 RANSOMWARE GEOGRAPHIC STATISTICS

Source: Number of ransomware attacks by country, November 2018 to October 2019, Kapersky Security Bulletin 2019

Source: Number of organizations affected by targeted ransomware attacks by country, January 2017 to May 2019, Symantec report: Target Ransomware

Source: Distribution of ransomware attacks, 2019 - Malwarefox: Ransomware Statistics 2019

As several indicators show, 2019 certainly seems to have been the top year for ransomware damage worldwide:

Ransomware posed the most serious threat to IT, with 80% of desktops, 57% of servers and 38% of mobile devices infected.

There were more targeted ransomware attacks, causing more damage to victims and earning far greater sums for their perpetrators (costs amounting to ~11.5 billion in 2019)

Much of the ransom paid has flowed into the new cyber extortion economy (99% of ransoms are paid in Bitcoin)

TO PAY OR NOT TO PAY?

When looking at the issue of ransom payment, there are three areas to consider: legal, technical and ethical.

LEGAL

The legality of ransom payment is still open to debate. In the French market, some recommend that such ransoms be uninsurable for public law and order reasons. In fact, there is a possibility that the money sent to attackers could be used to finance an act of terrorism, which is a breach of public law (Article 6 of the French Civil Code and Articles 421-2-2 of the Penal Code). Authorities advise reconstructing the network, better protecting it and filing complaints as soon as possible.

According to the French legal association Le Club des Juristes, this position seems to be shared by most countries of the European Union except, notably, The Netherlands, the United Kingdom (from 1981 since the "Ransom Act of 1782" was repealed) or Switzerland, where criminal risk can be insured[5].

5. https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_rapport_cyber-risk_janvier-2018_uk_web.pdf

To sum up, there is a grey area around the legality of ransom payment and no consensus.

SEVERAL LEGAL INITIATIVES AGAINST RANSOM PAYMENT HAVE BEGUN TO EMERGE, ESPECIALLY IN THE USA

- **In New York City:** two bills (S7246 and S7289) have been introduced into the New York State Senate. The first bill would make it illegal for local governments to use taxpayer dollars to pay a ransom, while the second bill bans all ransom payments entirely.
- **In the USA:** there are bills similar to a resolution passed in July 2019 by the U.S. Conference of Mayors[6] which stated that it stands against paying ransoms in the event of an IT security breach, as such an act merely encourages further attacks.

TECHNICAL

There is real and tangible pressure to make a choice that could save, for example, an organization from weeks of downtime from a critical service. There is no guarantee the hacker will actually decrypt the data, give the right decryption key to the company or not publicly release exfiltrated data.

According to research by Kaspersky[7], 20% of ransomware victims who have paid up have not got their files back.

An increasing number of companies are proposing cyber extortion negotiation and recovery services to support the victims of ransomware attacks.

ETHICAL

Most ransoms are still being paid in Bitcoin. As this is a virtual currency, it is difficult to trace where or what it is being paid to. Some experts offer ethical arguments against making ransom payments. For example:

- They encourage further attacks
- They mark the company concerned as an organization willing to pay ransoms
- They fund criminal activity

Some argue that the best way to solve the ransomware epidemic would be to make it illegal for organizations to pay ransoms.

To summarize, some companies are in favor of ransom payment, hoping quick for a recovery, limitation of losses due to business interruption and reimbursement by their insurance policy. Others are against ransom payment because of uncertainty in terms of legality, ethical matters and the possibility that the data involved may ultimately not be decrypted in any case.

Source: Cyentia Institute

6. The official non-partisan organization of cities with populations of 30000 or more.
7. https://www.kaspersky.com/blog/no-no-ransom/13364/

FROM RANSOMWARE ATTACK TO CYBER CRISIS

Ransomware attacks involve short-, medium- and long-term IT and operational impacts.

Business operations
Due to encrypted PCs and servers, in offices and industrial sites

Sales
E.g. interruption to the sales process and inability to process billing

Compliance
Contractual, legal fines due to data loss, etc.

Organization
E.g. no access to emails, temporary layoffs, etc.

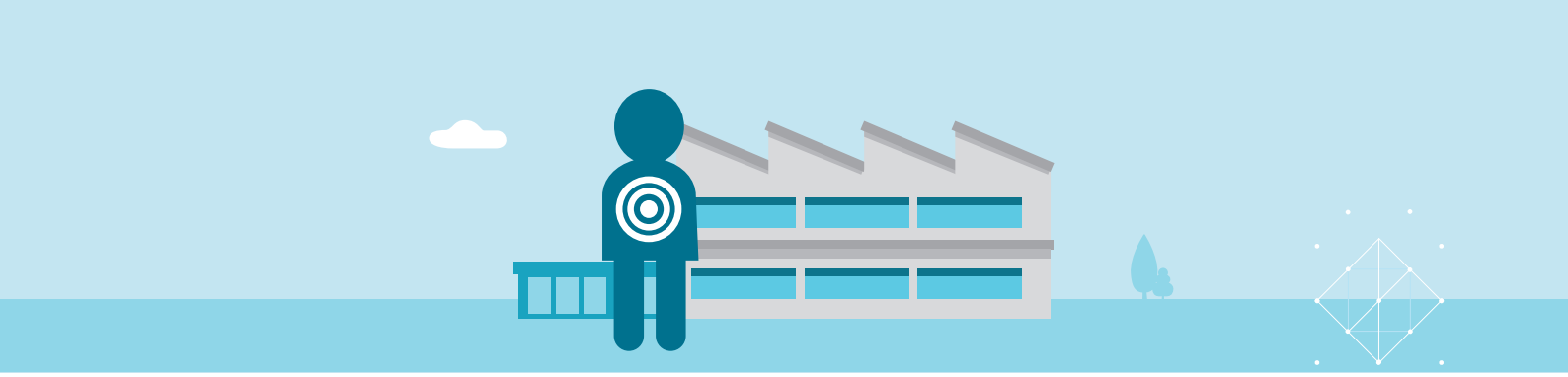
Corporate brand
Loss of confidence from customers and other third parties

Strategy
Impacts on the strategic plan timeline and goals

CYBER KILL CHAIN: BEHIND THE SCENE

A ransomware attack involves various steps from reconnaissance to encryption, also known as "kill chain":

1. Reconnaissance & weaponization	2. Delivery & exploitation	3. Installation & ransom demand
Collecting information about the target company and tailoring ransomware based this information	Delivering the tailored ransomware to the target company and exploiting the company's vulnerabilities to gain access	Installing ransomware to encrypt the target company's data / devices and establishing contact to demand a ransom
IT resources targeted		
Resources exposed directly to the Internet	Internet facing servers User endpoint devices Any IT resources connected to the network	Any IT resources connected to the company's network



CRISIS MANAGEMENT: GETTING THE SHOW ON THE ROAD

A successful kill chain will have a major impact on the supply chain of the targeted company, and could generate a crisis situation. Nevertheless, a crisis response cannot be activated each time a cyber incident occurs, because such responses require considerable resources (board meetings, crisis team, periodic penalty payments, financial resources, etc.). Companies therefore need to objectively identify their crisis triggers, which can vary from one company to another, to decide whether or not they actually need to activate a full-blown crisis response – this may include internal and external ransom negotiation experts, cyber-security experts, and so on.

When confronted with a major ransomware attack, the first reaction of most companies is to activate their business continuity plan (BCP), in order to restore confidence in their information systems and prepare their recovery.

WHEN A CYBER INCIDENT BECOMES A CYBER CRISIS

According to the Israeli National Cyber Directorate (INCD), a cyber crisis is a "situation posing a real threat of damage, or actual damage[8], to a vital cyber asset, which is liable to cause critical damage to routine operations, reputational damage, economic damage and endanger human lives.

A cyber crisis has varying degrees of gravity and, in an extreme situation, substantial damage is caused to core processes and to the functional continuity of an organization/the economy, which is liable to escalate to the point of a national state of emergency"

Cyber crisis management, step by step:

	CYBER WATCH	INCIDENT REPORTING	MASSIVE WARNING	COORDINATION
1. ALERT Mobilize crisis response team	✖	✖	✖	✖
2. CRISIS MANAGEMENT Investigation to understand the attack Build defense & recovery plan Trigger defense & recovery plan	✖		✖	✖
3. CRISIS RECOVERY 24/7 surveillance during the recovery			✖	✖

CYBER CRISIS MANAGEMENT STEP BY STEP:

Cybersecurity provides the foundation for good cyber resilience. The cybersecurity framework published by the U.S. National Institute of Standards and Technology (NIST) specifies five pillars for good cyber resilience: protect, detect, respond, remediate and rebuild. This resilience can be achieved if the Business Continuity Manager (BCM), the Risk Manager (RM) and the Chief Information Security Officer (CISO) work together to combine their full range of capabilities.

8. National Cyber Concept For Crisis Preparedness And Management - Israeli National Cyber Directorate (INCD)

CYBER ESSENTIALS FOR RANSOMWARE

Ransomware attacks experienced a shift of mindset with the arrival of Big Game Hunting. More and more ransomware attacks are now human-operated campaigns that pose major challenges in terms of risk mitigation.

To mitigate the impacts of these new types of attacks and make their networks more resilient, companies need to combine three things: cyber security measures, risk management and cyber insurance.

CYBER WORKOUT: BE PREPARED!

Below are the top security and risk measures that both large companies and SMEs can take to build better and more resistant security against ransomware. Some are basic measures that should really already be in place.

CYBER SECURITY

BASICS

Ensure that security basics are in place for critical data/ assets, such as privileged access management, Multi Factor Authentication (MFA), Active Directory (AD) management, etc.

SPECIFIC TO RANSOMWARE

Endpoints are the preferred entry points for hackers to spread ransomware:

- Implement endpoint protection tools (EDR)
- Increase anti-phishing capability
- Improve USB port security to prevent an infected USB key from being plugged into a PC

Backups are critical to ensure effective business continuity:

- Keep backups offline in a secure room, otherwise the online backups could also be infected by the ransomware and become useless
- Implement regular backups for critical and non-critical assets
- Protect backups with encryption / strong passwords

An efficient ransomware detection system ensures better reactivity in the event of attack.

- Implement a detection perimeter adapted to the threat to include endpoints, in order to detect new contamination as soon as possible
- Reshape alerts to make them relevant to the detection perimeter

RISK MANAGEMENT

BASICS

Ensure that the incident response plan includes the threat of cyber extortion (scenarios, reactions, critical assets and data that can be saved, external resources, etc.).

Map the company's vital cyber assets and data and rank them for assessment according to their criticality.

Map and identify the risks contained in suppliers' systems and services and protect vital cyber assets from these risks.

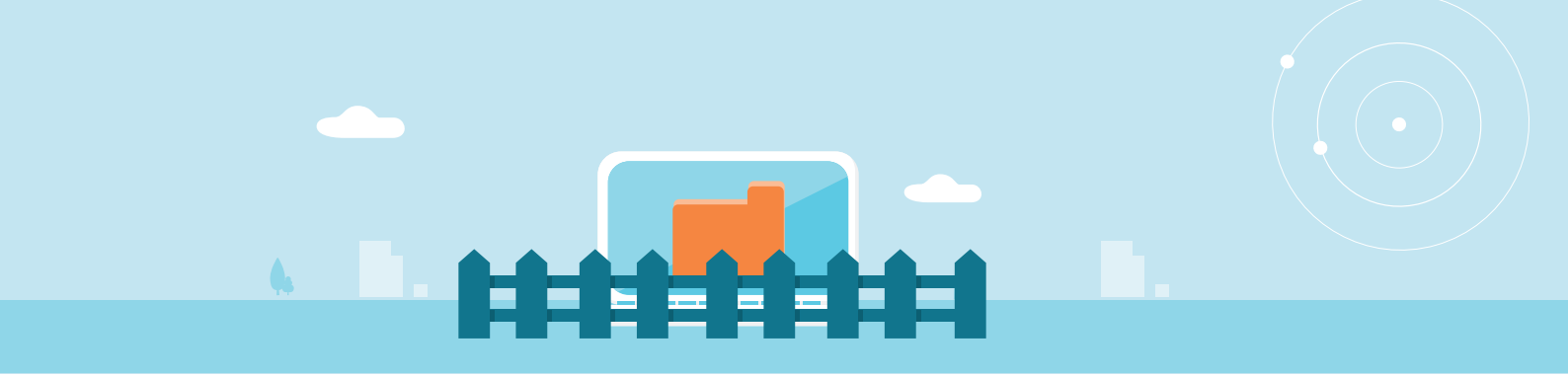
SPECIFIC TO RANSOMWARE

A multi-disciplinary team deals more efficiently with cyber extortion risk, in terms of both prevention and cure:

- The team should include finance, information technology, security, legal, human resources, operations, compliance, and communications.

Cyber insurance coverage is key for risk transfer and possible financial remedies:

- Conduct a policy assessment of the ransomware protection
- Determine if and how the coverage will respond to a ransomware attack, with the help of brokers, claims experts and legal advisors



CYBER INSURANCE: AN ALLY IN THE FIGHT AGAINST RANSOMWARE

If the worst does happen, cyber policies and insurers are well equipped to deal with ransomware events. The frequency and severity of ransomware-related losses has been on the rise for the last two years. While it is not easy to determine the exact loss numbers attributable to ransomware, many insurers feel that such losses contributed to approximately 60% of their overall loss ratio in 2019.

Cyber Insurance policies provide the following cover, designed to help companies respond and recover effectively in the event of a crisis.

Cyber Extortion covers the cost of ransom negotiations and payment of the ransom demand (should the insured choose to pay this) and provides access to specialist providers who can access cryptocurrency for payment.

Data Liability, notification and credit monitoring costs are covered if the data lost is classified as Personally Identifiable Information. This provides support to the individuals affected and can help to protect the insured's reputation. Cover includes legal defense costs for any litigation.

Specialized support in IT Forensics, Crisis Management and Legal Advice is available to the insured. Policies include panels of experts available to work along-side the insured to help them recover and resume operations in a secure manner.

Data Restoration Costs are paid by insurers to retrieve any encrypted data. This can involve the cost of recovery from available back-ups, or in the worst-case scenario can include the replacement of hardware if back-ups are not available.

Business Interruption and Extra Expense losses can be commonplace, depending on the industry concerned and the severity of the loss of data or access to the network. Policies provide cover for the loss of profit attributable to the ransomware event. In some instances, policies provide cover to assist the insured with loss preparation when presenting a Business Interruption loss.

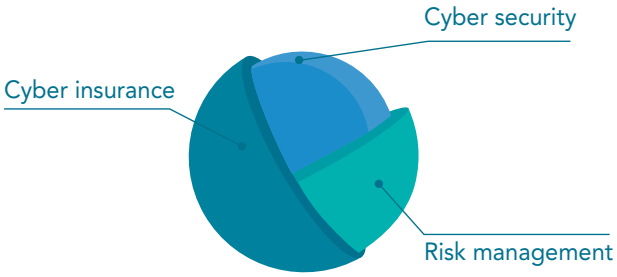
COVID-19 MAKES CYBER RESILIENCE EVEN MORE RELEVANT

The global COVID-19 pandemic has highlighted the need for organizations to dynamically review their cyber exposure because the rapid evolutions of their business environment may strongly impact their cyber posture. During the COVID-19 crisis, threat actors have taken advantage of work disorganization to intensify their malicious activities. The healthcare sector, for example, has faced increased threat activity while under the immense pressure of managing the pandemic. Conversely some organizations have slowed down, if not temporarily stopped their activities, resulting in reduced opportunities for threat actors.

Our growing dependency on IT infrastructures and the agility needed to deploy new IT solutions make Ransomware risk management even more topical. In most cases, IT departments have successfully implemented IT solutions to adapt to the "new normal" situation, while maintaining an adequate cyber security level. This unprecedent situation marks the start of a new era for IT approaches and related cyber security best practices, supported by updated guidelines from cyber security agencies.

CONCLUSION

By working closely with their IT and cybersecurity teams, risk managers can identify worst-case cyber scenarios, implement efficient risk mitigation measures and actively manage any residual risk through cyber insurance.



This article is written by:

ALEXIA MOROT
Cyber Underwriting Analyst
Cyber Solutions
amorot@scor.com

GILLIAN ANDERSON
Global Head Cyber
Specialty Insurance
ganderson@scor.com

For more information feel free to contact:

Cyber Solutions team
Didier Parsoire - Chief Underwriting Officer Cyber Solutions dparsoire@scor.com
Sébastien Héon - Deputy Chief Underwriting Officer Cyber Solutions sheon@scor.com
Teodore Iazykoff - Cyber Risk Modeller - tiazykoff@scor.com
Alexia Morot - Cyber Underwriting Analyst - amorot@scor.com
Olga Zeydina - Cyber Business Analyst - ozeydina@scor.com

Specialty Insurance team
London
Gillian Anderson - Global Head Cyber team - ganderson@scor.com
Simone Hardy - Underwriter - shardy@scor.com
Daniel Stewart - Underwriter - dstewart@scor.com

Paris
Béatrix de Boysson - Senior Underwriter - bdeboisson@scor.com
Edith Roche - Senior Underwriter - eroche@scor.com

New York
Cassandra Nettles - AVP, Senior Underwriter - cnettles@scor.com
Margaret Rose - VP, Financial Lines Manager - Americas - mrose@scor.com

PLEASE FEEL FREE TO VISIT US AT SCOR.COM

SCOR P&C
5, avenue Kléber - 75795 Paris Cedex 16
France
scorglobalpc@scor.com

SCOR The Art & Science of Risk | P&C

TO GET THE FULL RANGE OF TECHNICAL NEWSLETTERS, PLEASE CONTACT SCORGLOBALPC@SCOR.COM

Editor: SCOR P&C Strategy & Development
ISSN: 1967-2136

No part of this publication may be reproduced in any form without the prior permission of the publisher. SCOR has made all reasonable efforts to ensure that information provided through its publications is accurate at the time of inclusion and accepts no liability for inaccuracies or omissions.

© July 2020 - Design and production: Periscope