Ransomware Threats, Countermeasures and Trends within the Insurance Industry

A CRO Forum White Paper - Synopsis
March 2023

Table of Contents

cro forum

Executive Summary

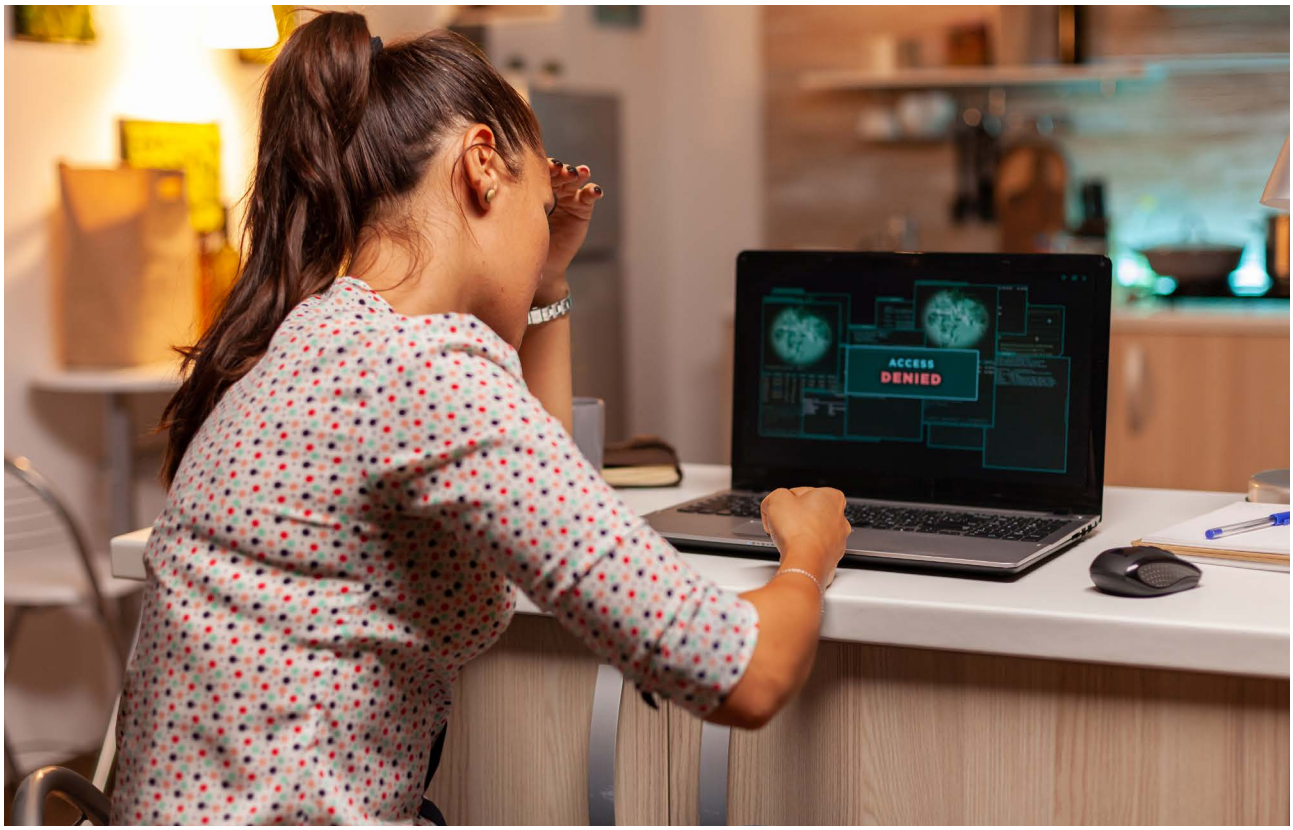
Ransomware cemented its position as the most prominent cybersecurity threat faced by organisations across geographies and sectors, with increased momentum and impact in the last few years. In this report, we shall cover the trends in ransomware and the regulatory development; how the ransomware threat works, and how (re) insurance companies can defend themselves against ransomware attacks.

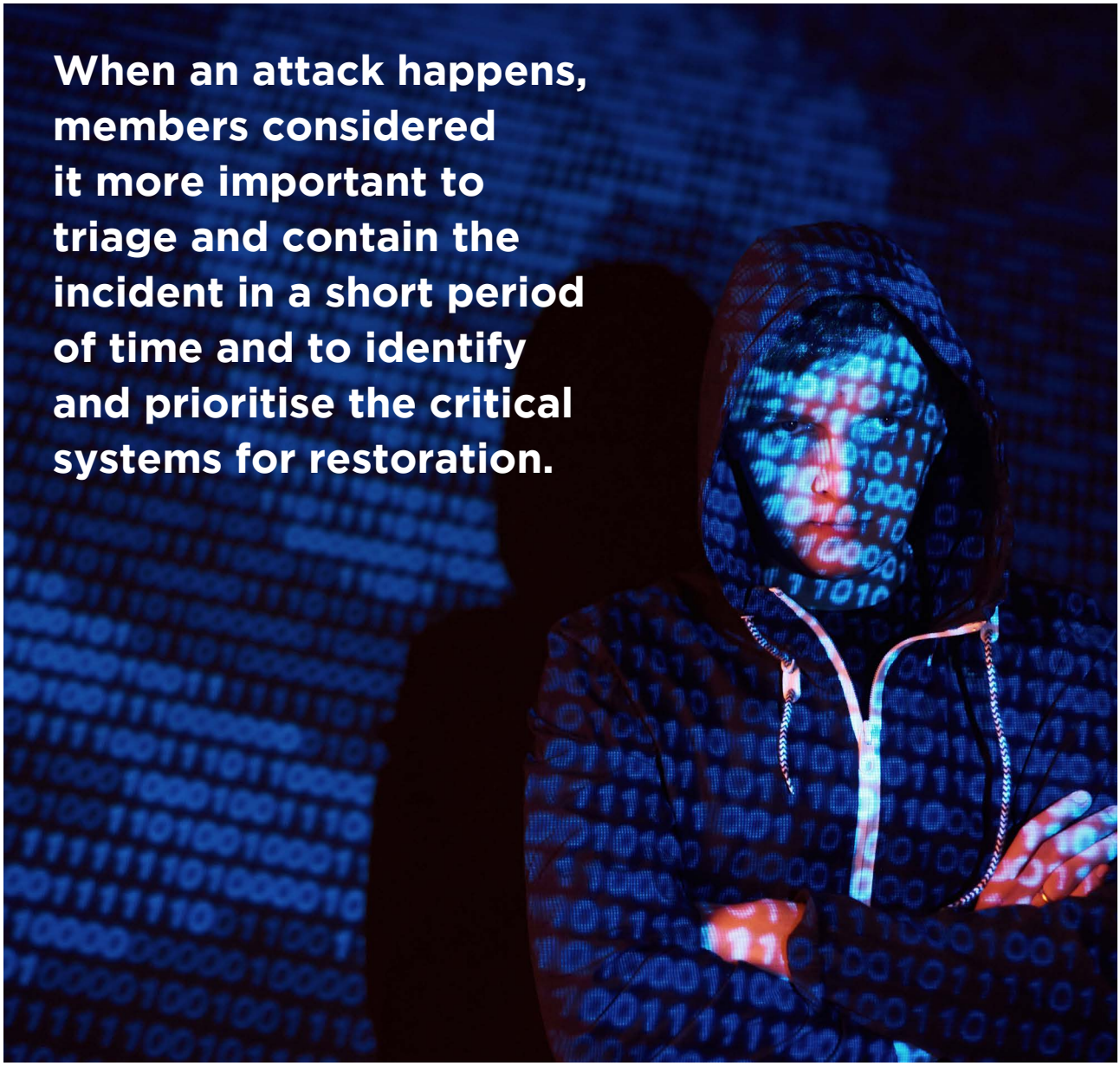
Ransomware attacks have been attracting public attention since the cyberattack by CryptoLocker and WannaCry, due to their broad impact on computer systems globally. The number of attacks keeps on rising, fuelled by the recent Ransomware-as-a-Service (RaaS) trend that allows a larger population of cybercriminals with lower technical capability to also access the tools to launch ransomware attacks.

Although some ransomware attacks have been specifically designed for particular targets and even for use at a particular period of time, it is generally believed that ransomware attackers do not usually have specific targets, but rather opportunistically attempt to attack multiple targets at the same time, mainly through phishing.

Apart from the traditional method of encrypting the victim's data to demand ransom, there is a trend for ransomware attacks to also exfiltrate the data, threatening the victims to disclose or sell their data in order to raise the chance of getting payment from the ransom. Some organisations choose to leverage cyber insurance to reduce the financial impacts from ransomware attacks, where it has been seen that the number of claims made against cyber insurance policies has been increasing, and this changes the risk position of the cyber insurance providers.

Since ransomware attacks request payment of ransomware through cryptocurrencies, it is expected that regulators would enhance the laws to bring cryptocurrencies under the coverage of the existing anti-money laundering and countering financing terrorism laws in order to combat the ransomware crimes. Meanwhile, insurance industry regulators are concerned about the capabilities of the insurance providers in managing the risk exposure from the 'silent cyber' policies as well as the ability of the insurance providers to prevent themselves becoming victims of ransomware attacks.





In order to protect the organisation from ransomware, this paper provides the best practices on the defence measures that insurance companies can adopt, which can be concluded in the five major domains: Prepare, Protect, Detect, Respond and Recover. The CRO Forum conducted a member survey to understand the priority of the measures and activities in these domains. Establishing the inventory of critical data and the cyber incident response plan rated high in preparing for the challenges from ransomware attacks, where timely deployment of patches, 24/7/365 monitoring of security operations and deployment of SIEM tools are considered most critical for protecting and detecting the attacks. When an attack happens, members considered it more important to triage and contain the incident in a short period of time and to identify and prioritise the critical systems for restoration.

In addition to response preparedness and deployment of protection mechanisms, (re)insurers may also consider purchasing cyber insurance policy to mitigate all or part of the financial impacts from the ransomware attacks if they consider the impact could be outside their risk appetite. While the cyber insurance policy may cover the amount of ransomware payment, the organisation still needs to consider whether paying ransom is legal and align with its ethical values. There is also a risk that the data cannot be recovered even if a ransom will be paid and, even with cyber insurance policy, the reputational damage may not be fully covered. Hence, cyber insurance cannot replace investments in information security and the (re)insurers should seek a balance here.

1. Overview of Ransomware Incidents, Trends and Regulatory Development

1.1 Recent incidents, trends with impact on the insurance industry

Ransomware attacks are on the rise. While there are a number of reports showing this, the 2022 SonicWall Cyber Threat Report provided some specific points, including that the number of recorded attacks in 2021 has tripled compared to the number in 2019. This indicates that the risks from ransomware cannot be neglected.

Whilst ransomware has been making headlines for the last five years, its origin can be traced back to 1989. However, it was the release of the CryptoLocker ransomware family in 2013 that raised attention to this threat. Then, the WannaCry ransomware family in mid-2017 became one of the most widely publicised and prolific ransomware, not only within the information security industry, but also among the general public, due to its broad impact on computer systems across the globe.

Although some victims of ransomware attacks were specifically targeted (where the attacks happen to a specific industry in a specific point of time when the data and systems are critical for the business operations), a cybersecurity advisory published jointly among cybersecurity authorities in the United States, the United Kingdom and Australia shows that the companies and industries of the ransomware victims were broadly diversified.

Phishing continues to be the primary method for the ransomware attacks where it can be used opportunistically in an attempt to attack multiple targets at the same time. Other than that, some attacks could be conducted through exploiting internet-facing systems of the targets, e.g. exploiting application vulnerabilities or using password brute-force attacks to gain the credentials for accessing a target system.

Compared to the past, there has been an increasing trend in not just encrypting files for ransom, but also exfiltrating the data and threatening to post it online; this is often known as the double ransom. The attackers use this to secure payment should the victims manage to recover the encrypted data (e.g. through restoring the data from the backup). When the data is exfiltrated, it will be used by the attackers to demand payment in exchange for the attacker not to publish the data, sell to other malicious parties, harass the victim's customers, and/or attack the business partners through the victim, which would threaten the reputation of the organisation, and in many cases will have a regulatory impact.

Another increasing trend is Ransomware as a Service (RaaS), where the developers of ransomware pass on their tools and expertise with a rental fee to other perpetrators (affiliates), who can carry out ransomware attacks without much know-how of their own. This allows a wider cybercriminal community with lower technical capability to access the ransomware attack tools.

Research from ISC(2) provided the companies' view of how they would respond to ransomware attacks; 70% of respondents said they discussed whether they would pay a ransom or not, with 64% of executives saying they would consider paying if it proved to be the quickest way to restore operations. By industry, healthcare executives are the most willing to pay, followed by financial services. However, paying the ransom doesn't mean getting back all of the organisation's data in a usable format. It was reported that, on average, organisations that paid got back only around 60% of their data.

Data plays an essential role in today's business world. If access to IT systems and/or to information is denied, this almost immediately means a business disruption. If production facilities come to a standstill, or online stores cannot be accessed anymore, or the IT in a hospital fails, this not only results in financial damage but can also lead to personal injury with fatal consequences. Some companies may purchase cyber insurance policy to reduce the financial impact and associated risk from ransomware. In the last five years, the number of claims made against cyber insurance policies have been increasing, with a reported doubling in the UK between 2019 and 2020. Similar results are seen in the US, with claims having doubled over a slightly longer period of three years. The risk position of a cyber insurance provider is changing, and it is observed that there has been a general increase in the premiums of such insurance products.

1.2 Latest regulatory developments

So far, the percentage of nation states passing legislation to regulate ransomware payments, fines and negotiations is low – estimated by around 1%. Gartner predicts that this number will rise to around 30% by the end of 2025.

It can be expected that much of this regulation will focus on ransom payment; some countries are considering or already restricting ransom payments. On the other hand, since most ransom payments were paid through cryptocurrencies, it is also expected that countries will be more focused on enhancing the laws and regulations in bringing cryptocurrencies under the scope of laws like anti-money laundering and countering financing terrorism laws.

From the insurance industry regulators' perspective, more focus on both threats posed by ransomware attacks against the insurance industry and the stability of underwriting portfolios has been observed. For instance, German regulator BaFin was keen to figure out and assess the so-called 'silent cyber' exposures that insurance carriers may have in traditional policies that do not address cyber risks at all or in an adequate way. Prudential Regulation Authority (PRA) in the UK will include a cyber component with regard to a systemic ransomware attack in the Insurance Stress Test (IST). Insurance industry regulators in China, Hong Kong, Singapore, Japan and Australia also enhance the requirements for the protection and security controls of the systems, data, and operational capabilities of the insurance companies.

1.3 Threat profile of insurers

Most ransomware attacks are not that targeted but are a result of successful phishing attacks performed at a high scale; hence, any company is a potential target if its security controls and awareness are not sufficient. Research results from a ransomware negotiation company show that insurers currently are not exceptional targets. In fact, among the sixteen industry categories in the research, the insurance industry is considered to be one of the industries that are less likely to be targeted, together with Automobile and Media.

2. Ransomware Threat Landscape

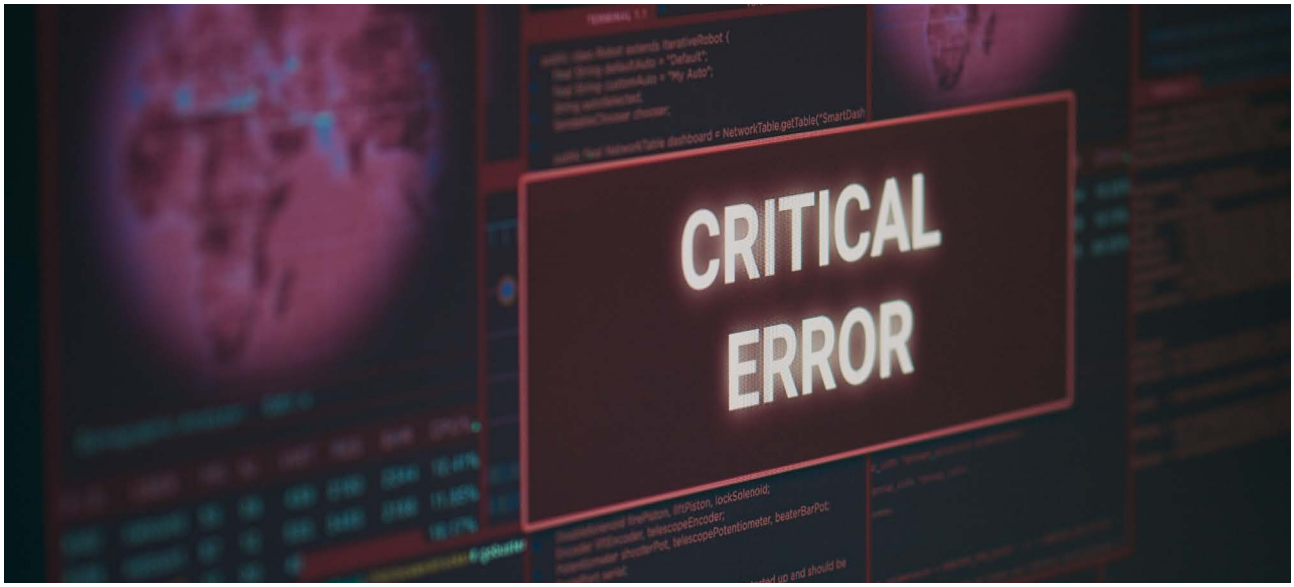
2.1 How do the ransomware groups operate and who are they?

Threat actors can mainly be classified in two different groups: i) initial intruder, who commits the network intrusion and prepares the scenario for the ransomware deployment; and ii) the ransomware operator, who deploys the ransomware and manages the negotiation with the victim.

The network intruders tend to be more technically proficient and they focus on preparing all the necessary steps and high-privilege credentials for the ransomware deployment. Ransomware operators do not necessarily need to be as technically proficient as the network intruders. In many cases, ransomware operators do not develop the ransomware themselves but obtain the tools through RaaS.

Usually, ransomware groups take their names from the ransomware software they have developed. Some well-known names are Conti, Lockbit, Ragna Locker, BlackCat, etc. There are some well-known ransomware groups that do not operate nowadays; some were taken down by law enforcement, such as REvil, and some may just shut down their operation by themselves, such as Maze.

Even though there is no direct link between the ransomware groups and Commonwealth of Independent States (CIS) countries, especially as some of them have declared that they are apolitical, there are some conspiracy theories about the linkage since most of the ransomware software turns inoperative if the ransomware detects that the victim's keyboard language is among any of the CIS countries.



2.2 Latest attack tactics and techniques

The common approach of attackers towards ransomware can be summarised into five key stages: (i) Initial Access, (ii) Reconnaissance and further expansion, (iii) Exfiltration, (iv) Deployment and (v) Extorsion.

In the Initial Access stage, the attackers may simply purchase credentials for accessing the target's system through Initial Access Brokers or Credential Markets. The attackers may also use phishing techniques to obtain credentials or even execute payload scripts if the receiver is not careful. Alternatively, the attackers may also try accessing the victim's system through Remote Desktop Protocol (RDP), which is a method for remote accessing or remote working. Although security-matured companies no longer use RDP as the remote working solution, smaller and medium-sized companies may still rely on RDP, this was observed particularly during the height of the COVID-19 pandemic. Sophisticated attackers may gain access through exploitation of the vulnerabilities in the victim's systems, especially between the time that the vulnerabilities were known and the patches were deployed.

After gaining access to the network or systems, the Reconnaissance stage follows, where the attackers will try to understand the structure of the victim's environment, specifically the antivirus vendor that victims are running on their servers and workstations. This allows the ransomware groups to develop a specific ransomware software that is undetectable for this specific antivirus vendor. The attackers may also try further expanding their access to the privileged user or admin level by searching the information available to them or by deploying some tools like Cobalt Strike, which is also being used in cybersecurity testing activity.

Before the attackers will deploy the ransomware, it is becoming more common that the attackers will try performing data exfiltration as another option to threaten the victim for ransom. Data exfiltration is a high-risk operation since it can be detected by the victim's security systems. Therefore, ransomware groups usually try to use covert ways to silently exfiltrate data and will likely select a destination of where the data will be transferring to that is not known to be malicious or blacklisted, including public or corporate file-sharing sites.

When the attackers further proceed in deploying the ransomware, they will use the privilege user and password gathered in the earlier stage and, apart from deploying the ransomware, if possible, they will remove the attack trails from logs. In addition, there is an upward trend of the attackers deactivating the backup processes and triggering an erasure or alteration of data backup files so as to reduce the possibility that the victim can restore the data and operations from backup.

After the ransomware has been deployed, a ransomware notification will be shown to the victim revealing which ransomware group is responsible for the attack and an anonymised and secure channel will be provided to communicate with them for negotiation and payment. The attackers may also threaten to disclose the data, publishing a portion of the data they obtained during the data exfiltration stage to demonstrate their ability to the victims. Regardless of the payment being made, there is a chance that the attackers could sell the data on dedicated darknet marketplaces.

3. Defence Measures and Best Practice Recommendations

A 'one-size-fits-all' approach is not applicable, as each (re)insurance company has a different risk profile and threat landscape. Risk assessments tailored to a company's individual circumstances are essential to develop and embed an effective risk management process against ransomware. A plan for response, and resuming the systems and services is critical in reducing the impact of the attack.

3.1 Defence measures – prepare and detect

In the risk assessment, the (re)insurance company needs to define the individual risk profile by compiling a threat catalogue, mapping existing risk mitigation measures to these threats and comparing the remaining risk with management's risk appetite statement, in which ransomware threats should be included. The (re)insurance company should also identify and register the information assets and define the sensitivity levels based on the protection requirements of confidentiality, integrity and availability of those assets.

Then, the (re)insurance company needs to identify the possible entries of the attackers and implement appropriate controls to protect the assets. In general, the common entries are phishing, brute-force attack (password guessing), exploiting system vulnerabilities, accessing through unsecured Remote Desktop Protocol (RDP) or through the weakness in the third-party system hosted by an outsourcing partner. So, it is important to ensure security controls are deployed, e.g. proper security awareness and culture in the company, encryption on the data is deployed, identity and access management controls are in place, regular vulnerability scanning and timely patch deployment and adequate and continuous third-party due diligence, etc.

Other than the protection controls, an effective detection mechanism is also critical to protect the system and data. A 24/7 Security Operations Centre (SOC) for monitoring system activities could help in identifying attacks in a timely manner, and a Threat Intelligence team can help in continuously monitoring and analysing the development of threats from new techniques or procedures used by cybergroups.

3.2 Respond and resume

In case a ransomware attack is successful, before diving into the responding action, it is important to step back to review and consider all the facts that will help focus the scope of the investigation. The (re)insurance company should identify the objective and scope of the responding actions, listing the tools available that can help in the responding actions and investigation, and reviewing the environment on whether additional professionals (e.g. legal or IT forensics) are required to be involved.

When it comes to the actions, the infected zone should be isolated, and a trusted zone should be created based on available sanitised backups parallel to the impacted zone and separate from the regular production areas. Once the minimum critical services have been restored in the trusted zone, verified and confirmed as secured, the structured migration of the trusted zone to the regular production can take place. Attention is needed for the network monitoring, vulnerability scanning and completeness in the patching of all assets.

After the systems have been restored, it is also important for a secure destruction (e.g. secure whipped) or archiving (if required for legal purposes) of infected or impacted assets.

3.3 Cyber insurance

Besides their own risk management activities, (re)insurers can choose to mitigate all or part of the financial impact of a ransomware attack by purchasing a cyber insurance policy. The use of cyber insurance as a mechanism for risk transfer to minimise the loss in the event of a ransomware breach is suitable where the economic impact from a successful ransomware attack is outside the company's risk appetite.

Any insurance product would require due care from the insured to implement appropriate IT controls to prevent ransomware, as the entire risk cannot be transferred. The insurance coverage and the residual risk should be determined by the senior management of the company since, in the end, the impact of a ransomware attack can carry a significant reputational risk that exposes the directors and officers of the company.

In considering the coverage of the cyber insurance, different aspects should be included, like the litigation costs associated with the breach of data, costs for crisis management (e.g. IT forensics, legal advice and communications), cost for restoring the data and system, the loss of profit attributable to the ransomware event, and also the coverage of the ransom payment.

When deciding whether the cyber insurance coverage includes ransomware payment, the (re)insurance company should also consider whether it is legal to pay the ransom or whether such a payment is ethical based on the organisation's value. In addition, the (re)insurance company should consider the risk that the attackers may not decrypt the data, and the logistic challenge in arranging the cryptocurrencies to be paid, where a (re)insurance company should not have such assets readily available.

Even though cyber insurance may help in transferring part of the risk, companies need to be aware that the purchasing of insurance to mitigate the ransomware event should not cultivate inappropriate corporate behaviour or compromise the security investment, since the result of the attack could far exceed the cover bought, and then the company has exposed itself to a greater risk than intended. In addition, cyber insurance may not be able to help fully mitigate the reputational risk.

4. CRO Forum Member Survey Analysis

An anonymised member survey was conducted as part of the research and development of this ransomware paper. The survey was structured with reference to the NIST Cybersecurity Framework, with the key analysis summarised.

4.1 Identify domain analysis

Members were asked to rate in order of priority the importance of nine measures to aid in the preparation of a ransomware attack. The results are shown in table 4.1-A.

Table 4.1-A: Most critical ransomware measures as voted by CRO Forum member insurance companies

Domain	Ref	Key ransomware security measures and activities	**Identify: Top 3 most critical ransomware measures** (by percentage)
Identify	ID-M1	Cyber Incident response plan(s) and playbooks specifically for ransomware are available and up to date	82%
Identify	ID-M2	Understanding / inventory of most critical data and systems (e.g. registered in a CMDB). Supporting infrastructure and application dependencies are also captured and updated	82%
Identify	ID-M3	Business impact is known when IT assets and data are unavailable. Business impact assessments (BIA) are regularly performed and updated	53%
Identify	ID-M4	Comprehensive network diagram(s) describing systems and data flows within your organization's network (including external connections)	35%
Identify	ID-M5	Dependencies and cyber risks in the supply chain are known	18%
Identify	ID-M6	A strategy towards the (potential) payment of ransomware have been defined, internally discussed and agreed upon	12%
Identify	ID-M7	Regular tabletop exercises are performed with management	12%
Identify	ID-M8	Strategy, policies, and governance regarding the payment of ransomware has been defined and approved by management	6%
Identify	ID-M9	Board is periodically informed of the current security posture and ransomware readiness activities	0%

4.2 Protect domain analysis

Members were asked to rate in order of priority the importance of fourteen measures to aid in the preparation of a ransomware attack. The results are shown in table 4.2-A.

Table 4.2-A: Most critical ransomware measures as voted by CRO Forum member insurance companies

Domain	Ref	Key ransomware security measures and activities	**Protect: Top 3 most critical ransomware measures** (by percentage)
Protect	PR-M1	Critical patches are timely deployed (=>95% compliant with own standards)	65%
Protect	PR-M2	Implementation of Multifactor Authentication (MFA) for critical systems and privileged accounts	59%
Protect	PR-M3	Identity and Access Management is based on the principles of least privilege, high-quality password rules, Multifactor Authentication and a specific focus on privileged accounts	35%
Protect	PR-M4	System hardening is based on published industry standards and best practices	29%
Protect	PR-M5	Endpoint security tools are used with behavioral detection and exploit mitigation capabilities	29%
Protect	PR-M6	External access with Remote Desktop Protocol (RDP) is protected with Multifactor Authentication (MFA)	18%
Protect	PR-M7	Employee's awareness and training includes regular phishing simulations and training on social engineering	18%
Protect	PR-M8	Administrators have a unique, privileged credential for administrative tasks	18%
Protect	PR-M9	Backups are immutable	12%
Protect	PR-M10	Network segmentation of critical resources	12%
Protect	PR-M11	Offline backups of data are used	6%
Protect	PR-M12	Backups are subject to Multifactor Authentication	0%
Protect	PR-M13	Regular updated 'gold images' of critical systems are created. Gold images are automatically rotated into production as they come online	0%
Protect	PR-M14	Compliance with the agreed control requirements are monitored on a regular basis via third-party due diligence	0%

4.3 Detect domain analysis

Members were asked to rate in order of priority the importance of thirteen measures to aid in the preparation of a ransomware attack. The results are shown in table 4.3-A.

Table 4.3-A: Most critical ransomware measures as voted by CRO Forum member insurance companies

Domain	Ref	Key ransomware security measures and activities	**Detect: Top 3 most critical ransomware measures** (by percentage)
Detect	DE-M1	24/7/365 monitoring of security operations	71%
Detect	DE-M2	Critical IT systems are connected and logging to security and event monitoring (SIEM) tool	71%
Detect	DE-M3	The security and event monitoring (SIEM) tool is sufficiently tuned in order to detect ransomware in a timely manner	53%
Detect	DE-M4	Regular vulnerability scanning to identify and address vulnerabilities on internet-facing systems	35%
Detect	DE-M5	Incoming mail is filtered for phishing messages	29%
Detect	DE-M6	Penetration tests are executed to assess security of internal and externally facing systems	12%
Detect	DE-M7	Network traffic is monitored for potentially suspicious data transfer	12%
Detect	DE-M8	Security operations have processes to detect when logging from security tools and IT systems has stopped	6%
Detect	DE-M9	Maintain backup logs for critical systems for a minimum of one year	6%
Detect	DE-M10	Threat intelligence services are used to continuously assess operational cyber threats	6%
Detect	DE-M11	Business transaction logging used for correlation	0%
Detect	DE-M12	Internal red team tests are performed to test security level of critical systems / crown jewels	0%
Detect	DE-M13	Tools to monitor data loss (DLP) are implemented	0%

4.4 Response domain analysis

Members were asked to rate in order of priority the importance of six measures to aid in the preparation of a ransomware attack. The results are shown in table 4.4-A.

Table 4.4-A: Most critical ransomware measures as voted by CRO Forum member insurance companies

Domain	Ref	Key ransomware security measures and activities	**Respond: Top 3 most critical ransomware measures** (by percentage)
Respond	RP-M1	Average time to triage and contain security incidents of workstations is <30 minutes	94%
Respond	RP-M2	SOC is mandated and able to (quickly) block / isolate part of the IT if a major (cyber) risk is identified	82%
Respond	RP-M3	Ransomware playbook is exercised with crisis management teams	59%
Respond	RP-M4	Systems and accounts involved and quickly identified in an initial breach	59%
Respond	RP-M5	Out-of-band communication options are available in case of a major ransomware incident	6%
Respond	RP-M6	Communication strategy / plans executed to (proactively) inform management and key stakeholders in case of a security incident	0%

4.5 Recover domain analysis

Members were asked to rate in order of priority the importance of three measures to aid in the preparation of a ransomware attack. The results are shown in table 4.5-A.

Table 4.5-A: Most critical ransomware measures as voted by CRO Forum member insurance companies

Domain	Ref	Key ransomware security measures and activities	**Recover: Top 3 most critical ransomware measures** (by percentage)
Recover	RE-M1	Critical systems are identified and prioritised for restoration	82%
Recover	RE-M2	Critical systems are part of practice recoveries at least once a year with a focus on ransomware	18%
Recover	RE-M3	Lessons learned are discussed, documented and shared with all key stakeholders	0%

4.6 Survey analysis

The following key observations can be derived from the survey that was conducted.

No.	Framework	Observation
1	Identify	Cyber incident response plans are an essential security measure in the preparedness of handling a ransomware incident.
2	Identify	82% of respondents stated that an understanding of critical data and systems, typically through registration in a CMDB, is a top 3 security measure.
3	Protect	Patch management was identified as the most critical measure with regards to defending against potential ransomware attacks.
4	Protect	Implementation of Multifactor Authentication (MFA) on critical systems was considered to be the second most important after patch management for defending against ransomware attacks.
5	Detect	From the 13 security measures in the Detect domain, the top 3 most critical measures identified by member organisations all relate to threat detection with 24x7x365 security monitoring capabilities and ensure that critical systems are correctly onboarded to security information and event management (SIEM) tools that have appropriate ransomware use cases in place.
6	Respond	The top two prioritised security measures based on member responses relate to the speed at which an organisation can respond to a threat. 94% of members prioritised average response and containment time to take place within 30 minutes, followed by 82% of members prioritising the Security Operations Centre (SOC) being able to quickly neutralise a detected threat.
7	Recover	Member responses placed recovery measures that prioritised identification and prioritisation of critical service recovery as well as testing of recovery above lessons learned activities.

5. Final Words

A ransomware attack is a real threat to any organisation, and there is an upward trend for the number of ransomware attacks. This trend could be contributed to by two main factors.

Firstly, the transformation of the 'business model' of ransomware; some threat actors with technical know-how may rent the ransomware to other criminal groups (i.e. Ransomware-as-a-Service model), which allows a wider population of malicious groups to have access to the techniques.

Secondly, the popularity of cryptocurrencies also provides a safer channel for the threat actors to obtain the ransom payment without disclosing their true identities.

Most of the ransomware attacks are committed through phishing, which means companies and industries are having more or less equal chances of being attacked, as the threat actors tend to send the phishing emails to a large population of email addresses, anticipating some of them will be successful.

In order to minimise the ransomware risks, the working group recommends the following:

1. To be aware of and understand the ransomware threat actor's motivation, which affects the specific threat profiles of the insurers.

2. To design the appropriate level of security controls and risk mitigation measures in accordance with its own risk profile and appetite specifically for the ransomware threat.

3. While cyber insurance coverage could be one of the mechanisms in managing the financial impact, it is important to be aware that cyber insurance cannot replace all security investments; instead, the insurers should seek a balance between the security investment and the insurance coverage in order to minimise the potential impact from ransomware.

Companies can also consider leveraging on the checklist in appendix 1 as a tool to assess their internal controls, evaluating their preparedness to ransomware attacks.

Appendix
Defence Measures Library

Domain	Defence measures library main topics to take into account	Description	Reference NIST SP 800-53 Rev. 5 ISO 27001:2013
Identify	**Define your individual risk profile and risk appetite statement**	Identify the individual risk profile by compiling a threat catalogue, mapping existing risk mitigation measures to counter these threats and comparing the remaining risk with management's risk appetite statement. A best as possible mitigation of threats to an acceptable level aligned to management's risk appetite statement is to be aimed for and should be endorsed at board level.	**NIST SP 800-53 Rev. 5** PM-8, PM-11, RA-1, RA-3, RA-9 **ISO 27001:2013** Clause 4.1
	Classify and register your assets	Understanding / inventory of most critical data and systems (e.g. registered in a CMDB). Supporting infrastructure and application dependencies are also captured and updated. Business impact is known when IT assets and data are unavailable. Business impact assessments (BIA) are regularly performed and updated. Comprehensive network diagram(s) describing systems and data flows within your organisation's network (including external connections).	**NIST SP 800-53 Rev. 5** AC-4, AC-20, CA-2, CA-3, CA-9, CM, CP-2, PL-8, PM-5, PM-7, PM-9, PM-11, RA-2, RA-3, RA-8, RA-9, SA-5, SA-9, SA-10, SA-11, SA-20, SC-6 **ISO 27001:2013** A.8.1.1, A.8.1.2, A.8.2.1A.11.2.6, A.12.6.1, A.13.2.1, A.13.2.2, A.16.1.6, Clause 6.1.2, A.18.2.3
	Supply chain and (sub) contractor impact	Dependencies and cyber risks in the supply chain are known and documented. Response and recovery planning and testing are conducted with suppliers and third-party providers.	**NIST SP 800-53 Rev. 5** SR all controls, CP-2, CP-4, CP-8, , IR-3, IR-4, IR-6, IR-8, IR-9, PE-9, PE-11, PM-8, SA-20 **ISO 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3, A.17.1.3, SA-4, SA-9
	Governance and documentation	Establishing and implement policies needed to prevent the impact of ransomware events. These policies should be reviewed periodically to reflect the dynamic nature of risk and the reality of needed ongoing adjustments. Some examples are: • Management Board is periodically informed of the current security posture and ransomware readiness activities • Cyber Incident responds plan(s) and playbooks • Regular tabletop exercises are performed with management	**NIST SP 800-53 Rev. 5** CA-7, PM-4, PM-9, SA-3, SA-8, SA-15 **ISO 27001:2013** Clause 6.1.3

Domain	Defence measures library main topics to take into account	Description	Reference NIST SP 800-53 Rev. 5 ISO 27001:2013
Protect	**Protect threat actor's entries**	Implement appropriate controls to ensure protection of assets. Examples are: • Implementation of Multifactor Authentication (MFA) for critical systems and privileged accounts • Backups are immutable • Backups are subject to Multifactor Authentication • Maintain backup logs for critical systems for a minimum of one year • External access with Remote Desktop Protocol (RDP) is protected with Multifactor Authentication (MFA) Offline backups of data are used Employee's awareness and training includes regular phishing simulations and training on social engineering System hardening is based on published industry standards and best practices	**NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, PE-2, PS-3, SC-5 **ISO 27001:2013** A.7.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3
	Ongoing awareness and Training	Most ransomware attacks are made possible by staff who engage in unsafe practices. Like administrators who implement insecure configurations or developers who program unsafe code. Ongoing increase in awareness and training is necessary.	**NIST SP 800-53 Rev. 5** SA-16, AT-1, AT-2, AT-3, AT-4, AT-5, PM-13 **ISO 27001:2013** A.7.2.2, A.12.2.1
	Monitor deviations of baseline protection	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality). Ongoing monitoring of (unauthorised) changes to the configuration will be used as an indicator of a potential malicious attack. Examples of monitoring relate to the following: • Identity and Access Management is based on the principles of least privilege, high-quality password rules, Multifactor Authentication and a specific focus on privileged accounts • Network segmentation of critical resources • Critical patches are timely deployed (=>95% compliant with own standards) • Administrators have a unique, privileged credential for administrative tasks • Endpoint security tools are used with behavioral detection and exploit mitigation capabilities	**NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-10, AC-14, AC-16, AC-24, CA-9, CM-2, CM-3, CM-4, CM-6, CM-7, CM-9, SA-10, SC-7 **ISO 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.12.1.2, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.5.1, A.12.6.2, A.12.7.1, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3, A.14.2.2, A.14.2.3, A.14.2.4

Domain	Defence measures library main topics to take into account	Description	Reference NIST SP 800-53 Rev. 5 ISO 27001:2013
Protect	**Remote Maintenance**	Most ransomware attacks are conducted remotely. Managing privileges associated with remote access will limit the risks. In addition, the remote maintenance of organisational assets is approved, logged, and monitored.	**NIST SP 800-53 Rev. 5** AC-1, AC-17, AC-19, AC-20, MA-4, SC-15 **ISO 27001:2013** A.6.2.1, A.6.2.2, A.11.2.4, A.11.2.6, A.13.1.1,A.13.2.1, A.15.1.1, A.15.2.1
	Third party due diligence	Compliance with the agreed control requirements is monitored on a regular basis via third party due diligence	**NIST SP 800-53 Rev. 5** SR all controls **ISO 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3, A.17.1.3
Detect	**Continuous Security Monitoring**	Implement appropriate monitoring mechanisms to identify the occurrence of attacks. among other things important to take in account: • 24/7/365 monitoring of security operations • Critical IT systems are connected and logging to security information and event monitoring (SIEM) tool • The SIEM tool is sufficiently tuned in order to detect ransomware in a timely manner • Security operations have processes to detect when logging from security tools and IT systems have stopped • Business transactional logging used for correlation • Network traffic is monitored for potentially suspicious data transfer • Personnel activity is monitored to detect potential cybersecurity events	**NIST SP 800-53 Rev. 5** AC-2, AU-6, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, CP-2, IR-4, IR-5, IR-8, RA-3, PE-3, PE-6, PE-20, SC-5, SC-7, SI-4 **ISO 27001:2013** A.12.4.1, A.12.4.3, A.14.2.7, A.15.2.1, A.16.1.4, A.16.1.7
	Threat detection processes	In addition to the monitoring, detection activities will be conducted in adherence to organisation policy and procedures. Examples are: • Threat intelligence services are used to continuously assess operational cyber threats • Penetration tests are executed to assess security of internal and externally facing systems • Internal red team test are performed tot test security level of critical systems / crown jewels • Regular vulnerability scanning to identify and address vulnerabilities on internet-facing systems • Tools to monitor data loss (Data Loss Prevention (DLP)) are implemented • Incoming mail is filtered for phishing messages	**NIST SP 800-53 Rev. 5** AT-3, AU-6, CA-8, RA-5, SI-2 **ISO 27001:2013** A.12.6.1

Domain	Defence measures library main topics to take into account	Description	Reference NIST SP 800-53 Rev. 5 ISO 27001:2013
Respond	**Response Planning**	Develop techniques to understand the impact and respond appropriately after a detected cybersecurity incident. • Endorsement of the average time to triage and contain security incidents of work stations (e.g. <30 minutes). • Ransomware playbook is validated and exercised with crisis management teams • Out-of-band communication options are available in case of a major ransomware incident • SOC is mandated and able to (quickly) block / isolate part of the IT if a major (cyber) risk is identified	**NIST SP 800-53 Rev. 5** CP-2, CP-3, IR-3, IR-8 **ISO 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1, A.16.1.6
	Response after incident	Ransomware playbook is executed with crisis management team after a detected cyber security breach. To take in account: • Communication strategy/ plans executed to (proactively) inform management and key stakeholders (e.g. regulators, customers, employees) in case of a security incident • Systems and accounts involved and quickly identified in an initial breach. Delimit / isolate the Infected IT assets • Forensics is used to identify the root cause and to and eradicate the attack, including things like resetting passwords of credentials stolen by the attacker, deleting malware used by the attacker, and removing persistence mechanisms used by the attacker.	**NIST SP 800-53 Rev. 5** AU-5, AU-6, AU-7 , CP-2, IR-4, IR-6, IR-8, PM-15, SI-5 **ISO 27001:2013** Clause 7.4, A.6.1.4, A.12.2.1, A.16.1.2, A.6.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
Recover	**Recovery execution**	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. Critical systems are identified and prioritised for restoration. Reputation impact is limited by good communication with all stakeholders after an incident.	**NIST SP 800-53 Rev. 5** CP-10, IR-4, IR-8 **ISO 27001:2013** A.16.1.4, A.16.1.5, Clause 7.4
	Improvements	Lessons learned are being discussed, documented and shared with all key stakeholders. Adjust the Ransomware playbook to increase the effectiveness for future ransomware attacks.	**NIST SP 800-53 Rev. 5** CA-2, CA-7, CP-2, IR-4, IR-8, PL-2, PM-14, RA-5, SI-4 **ISO 27001:2013** A.16.1.6, Clause 10

Domain	Defence measures library main topics to take into account	Description	Reference NIST SP 800-53 Rev. 5 ISO 27001:2013
Risk Transfer	**Cyber Insurance**	Decision to mitigate all or part of the financial impact of a ransomware attack by purchasing a cyber insurance policy. The use of cyber insurance as a mechanism for risk transfer to minimise the loss in the event of a ransomware breach is suitable where the economic impact from a successful ransomware attack is not within the company's risk appetite. • Cyber risks are quantified to assess the impact of a ransomware event • Cyber insurance includes assistance services such as IT forensic supports, legal consulting, customer notification, credit monitoring, etc. • Cyber insurance includes third-party coverage.	

Disclaimer

The CRO Forum is supported by a Secretariat
that is run by KPMG Advisory N.V.
Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands

www.thecroforum.org

cro forum