MetaCompliance®

Ransomware Resilience:

A CISO's Playbook for Prevention & Recovery

Elevate your **Cybersecurity Training** with **MetaCompliance**

Make it personal.

metacompliance.com

Abstract

Information security is the very definition of a CISO's responsibility, and a ransomware infection is the nemesis of this role. Where once ransomware was relatively rare, now this insidious and harmful malware is a global industry, often sponsored by state actors who use the proceeds to finance criminal activities and even warfare. A recent series of raids by Interpol highlights the significant activities of ransomware gangs. A joint investigation team (JIT) involving Norway, the USA, the United Kingdom, Ukraine, and others, managed to bring to justice a ransomware gang that had targeted organisations in 71 countries, causing hundreds of millions of euros in losses. [1]

Ransomware as a business is now common worldwide and continues to grow as a lucrative way to steal money. Ransomware tactics morph and adjust to market forces, much like a business. One of the reasons for the success of ransomware is the ease with which cybercriminals enter the corporate network. The image of a hacker using super coding skills to break through cyber defences is unrealistic. Instead, ransomware attackers focus on the person in front of the computer: attackers socially engineer employees, issue phishing campaigns, attack vulnerable systems and processes, and brute force passwords to install ransomware.

In the world of ransomware, human-centric attacks are the norm, not the exception.

So, how does the busy CISO prevent (or recover) from a ransomware attack?

MetaCompliance excels in preventing human-centric cyber attacks. Here, we explore how to prevent ransomware, and if the worst happens, how to recover from an attack.

Part One: Ransomware, the facts

Is your industry sector in the sights of ransomware criminals?

Many studies are exploring the type of industries most targeted by ransomware. However, the consensus is that all industries are at risk. Some sectors are targeted more than others, but cybercriminals are great at adapting and changing focus. If your sector is not in the sights of ransomware threat actors now, chances are your industry will soon be the flavour of the month. Research into ransomware is ongoing as the landscape evolves, but some recent statistics show the breadth of this most insidious of cyber security threats.

Assess Current Capabilities and Needs:

- Around one-third of all data breaches involve ransomware [2]
- 59% of organisations were attacked in 2023 [3]
- 70% of attacks resulted in data encryption [3]
- Ransomware attacks increase by 84% in 2023 [4]

Targeted industries

According to NCC Group [4]:

- Most targeted industries: Industrials (32%), Consumer Cyclicals (15%), and Technology (11%).
- Most targeted countries: North America (50%), Europe (28%), and Asia (10%) remain the most targeted regions.
- According to the 2024 Verizon Data breach Investigations Report, Ransomware was a top threat in 92% of industries. [2]

Ransom costs

A 2024 Chainalysis report found that over $1.1 billion USD (£800 million GBP) was paid out in ransoms during 2023. The report describes the situation as a "watershed moment." [5]

Ransomware tactics, techniques, and trends to watch out for

Cybercriminals are nothing if not inventive. It will be found if there is a way for ransomware attackers to slip under an enterprise Radar. Understanding attackers' tactics and techniques to circumvent enterprise security is vital to avoiding ransomware threats. Here, MetaCompliance highlights some of the latest trends to be aware of:

Supply chain attacks

The era of supply chain-initiated ransomware attacks is truly upon us. The supply chain and other third-party suppliers, like consultants, are ideal attack bases. These third parties often require privileged access to corporate apps, devices, and systems. One recent example demonstrates the vulnerability of the supply chain and attackers' move to create mass attacks.

MOVEit ransomware attack
MOVEit is a secure file transfer solution. Cyber attackers exploited a SQL injection vulnerability (CVE-2023-34362) in MOVEit software that allowed it to implant ransomware across 255 supply chain members. The hackers behind the attack were the infamous CLOP ransomware gang. CLOP is renowned for using phishing, Ransomware-as-a-Service (RaaS) and double extortion techniques, as discussed next. [6]

Have any information on CLOP? Send in a tip.

Ransomware-as-a-Service (RaaS)

Gone are the days when a cybercriminal had to be an experienced software developer to carry out an attack. The advent of "as-a-Service," off-the-shelf cyber attack packages has made ransomware attacks open to all who are criminally inclined. Cybercriminals using RaaS get all they need to carry out a ransomware attack—payment to the cybercriminal controllers of the RaaS comes in the form of a cut of the ransom.

Phobos RaaS [7]
Phobos ransomware creators have gone out of their way to ensure their RaaS package is easy to use. The ransomware is accessible working with lots of open-source tools, and the wide range of variants makes it harder for email gateways and anti-virus solutions to detect Phobos attacks. Phobos attacks are usually initiated using phishing email campaigns or by scanning for vulnerable Remote Desktop Protocol (RDP) ports.

Double and triple extortion and data theft

In the past, ransomware was used to encrypt critical files and documents and then extort money to release the decryption key. This model has gone out of favour as cybercriminals turn to increasingly devious tactics to ensure the ransom is paid. Modern ransomware attacks typically involve data theft. Today, double and triple-extortion tactics are common. Two examples explain why these attacks are so-called double and triple extortion:

Double-extortion attack
Royal ransomware is typically initiated using phishing. The attackers typically gain access via stolen credentials. Once inside a network, the attackers exfiltrate data before encryption, publishing this data to a leak site to pressure the company to pay the ransom. So far, Royal ransomware ransom payments have exceeded $275 million USD (£225 million GBP). [8]

Triple-extortion
Cybercriminals can leverage chaos and vulnerability by adding other forms of cyber attack to a ransomware infection. Triple-whammy attacks typically include DDoS (Distributed Denial of Service) and involve attacks on the supply chain. Blackcat is an example of a triple-extortion ransomware gang. Blackcat targets many industry sectors; victims include Grupo Estrategas EMM, NextGen Healthcare, and Solar Industries India. The gang exploits vulnerable RDP and compromised credentials obtained via phishing and from previous data breaches. Blackcat also uses DDoS along with ransomware.

Human-centric attacks and vectors

Many of the ransomware tactics mentioned above use human-centric attacks to initiate a ransomware infection. The "human in the machine" approach to cyber attacks is now well-established, with the 2024 DBIR captures this putting it succinctly:

"Regardless of the exact method that attackers use to reach organisations, the core tactic is the same: They seek to exploit our human nature and our willingness to trust and be helpful for their own gain."

Social engineering
Direct manipulation of individuals, like an IT administrator, can provide access into the heart of an organisation. Manipulation of human behaviour is a vital tool for cybercriminals, and ransomware attackers use it to execute a variety of techniques. Behaviour manipulation takes many forms. Egregor ransomware is an example of the length's attackers will go. Once installed, attackers printed ransom notes on organisation's printers for additional pressure. Other ransomware attacks will display countdown timers on computers to pile the pressure on to pay. [9]

"What is Social Engineering"

Phishing
Phishing emails are the main vector to initiate or deliver ransomware attacks. Phishing comes in a variety of forms, from targeted spear phishing to mass phishing campaigns. Spear phishing is extremely common. The UK Cyber Security Breach Survey 2024 found that 84% of businesses were victims of phishing. [10] Phishing tactics regularly change, and a recent phenomenon is the use of QR code phishing. QR codes are embedded in phishing emails to encourage people to click the link. This then leads to a spoof website where credentials are stolen. Once the cybercriminal can access login credentials, they can escalate privilege. This provides privileged network access where they can then install ransomware.

"What is phishing and how to prevent it"

Zero days and exploits

Zero-days are so-called because they are new vulnerabilities that the vendor has yet to fix. Zero-day exploits are increasingly being exploited for ransomware gains. According to research from Akamai, zero-day exploits have led to a 143% increase in ransomware victims. [11] The CLOP ransomware group, which uses RaaS, has increased its victims by nine times by exploiting zero-day vulnerabilities during an attack.

Research from the Verizon 2024 DBIR sums up the situation regarding the plethora of techniques used by ransomware attackers:

"When prioritising your efforts at protecting yourself, don't neglect addressing malware infections, stolen credentials or unpatched systems as it may lead you to break out in Ransomware."

This leads us neatly onto our next section about how to protect against and recover from ransomware.

Part two: Take action against ransomware

Prevent ransomware

Ransomware attackers may modify tactics, but they also use tried-and-tested techniques. A CISO can use the section on "tactics, techniques, and trends" to develop strategies that prevent a ransomware attack. However, one thing is clear: Ransomware protection requires a defence-in-depth approach. The following strategic methods and techniques should be used together for a comprehensive ransomware prevention strategy.

Patch vulnerabilities

Ensuring that software, firmware, and hardware updates are quickly installed is an important aspect of ransomware prevention. However, the increased use of zero-days and CVEs (Common Vulnerabilities and Exposures) that are not yet patchable, means that this security measure must be shored up with defence-in-depth approach.

Employee awareness

Attackers love to make life easy, and exploiting human behaviour can quickly steal credentials or socially engineer an individual. Regular, role-based Security Awareness Training is a fundamental security layer that helps to protect your organisation. Security Awareness Training covers various topics that impact employee security behaviour. The awareness training package teaches employees how poor security behaviour, such as sharing passwords or clicking on phishing links, can lead to security incidents.

With research indicating that 62% of employees share passwords with colleagues, ensuring employees understand risk is essential to preventing ransomware infections. [12]

Phishing and phishing simulations

Phishing is a common method for stealing credentials that can lead to ransomware infection. Phishing simulation exercises are part of regular and targeted Security Awareness Training. Phishing simulation platforms generate fake phishing emails that are sent out to employees to test their responses. This is done with employee consent and cooperation. The phishing simulations can be tailored to reflect the typical phishing attacks specific employee roles experience. The phishing simulations use interactive training sessions when an employee interacts with the fake phishing emails. The training explains what would happen if this was a real phishing email. Over time, and with regular targeted simulated phishing sessions, employee behaviour changes and phishing becomes less effective.

Secure backup

Ransomware attackers rely on the fear, uncertainty, and doubt of an organisation that does not have access to its data post-ransomware infection. To help alleviate the pressure of an attack, a company should use a back-up solution. However, it is vital to use a back-up system that is designed to be secure and has ransomware-proof features: a report on the State of Ransomware from Sophos found that 94% of organisations hit by ransomware said cybercriminals tried to compromise back-ups during the attack, and 57% were successful. [13]

Email security and DNS security

In Q2 2023, there were around 1.3 million phishing websites, many of which are set up to steal login credentials. [14] DNS filters works by cross-referencing against a URL blocklist. Other email security solutions can help to identify phishing attempts and block phishing emails before they reach the user's inbox. Advanced email security solution use AI and machine learning to identify emerging threats, However, no method is 100% failproof. Instead, using a combination of symbiotic measures creates a defence-in-depth approach.

Monitoring tools

Behaviour-based detection systems can be used to identify anomalies, such a data exfiltration, that could be caused by an ongoing cyber attack. Monitoring tools are a useful first signal to identify a ransomware attack, allowing an organisation time to act.

Enforce least privilege access

Many cyber attacks leverage privileged access rights. For example, spear phishing attacks often attempt to steal a user's login credentials with privileged access rights. The principle of least privilege is used to ensure that access rights reflect the needs of an individual to do their job and no more. Applying least privileged access across the organisation and out into the supply chain helps to minimise the risks associated with login credential theft. Using role-based security awareness combined with least privilege access rights ensures that targeted users can handle the risks associated with their role.

Supply chain risk management

As cyber attackers increasingly target third parties, having governance over your suppliers is essential. Supply chain risk management (SCRM) must become integral to your defence-in-depth approach to ransomware prevention. SCRM can be challenging as it covers all potential risks that impact supply chains, including cyber security risks. However, all of the defence-in-depth measures used in an enterprise to prevent ransomware should be repeatable by a supply chain member.

Recover from ransomware

Ransomware prevention will significantly reduce the risk of an infection. However, it will not be 100% failsafe. If your organisation becomes infected with ransomware, there are best practices that can minimise the impact. The fact is that 98% of organisations with data encrypted by ransomware got the data back either by restoring from back-ups (68%) or paying the ransom to get the decryption key (56%). [15]

However, restoring data is only part of the recovery process. Ransomware infections have far-reaching effects, especially those with additional security implications, such as associated DDoS attacks. Ransomware attacks also result in downtime, reputation damage, and compliance fines. Recovery times, for example, can vary from a week (28% fully recover) to up to three months (27% recover). Recovery in 2024 cost, on average, $2.3 million (£1.8 million GBP).

Three-step recovery plan

MetaCompliance suggests a three-point recovery plan to prepare if your business becomes infected with ransomware. These steps to recovery will help to mitigate the impact of the ransomware infection:

Step One: Create an incident recovery plan (IRP)

Effective incident response plans that cover ransomware attacks are well-documented, CISA [16] provides guidelines for responding to a cyber attack. Examples of the type of best practices to include in an IRP include the following:

Prepare: Understand the risk and create cyber security policies, that reflect these risks. Use the right tools and team to handle potential incidents.

Identify: Detect the ransomware attack as quickly as possible by using appropriate monitoring tools.

Contain: An attack must be contained to prevent further damage. This includes isolating infected systems and securing network segments.

Remove: Remove the ransomware from all affected systems.

Recover: Restore data from back-ups and repair affected systems.

Post-Incident Analysis: Analyse the incident to understand what happened, how it was handled, and how to prevent future attacks.

Communication: Clear communication with all stakeholders, including employees, management, and customers, is essential for containment and reputation.

Documentation: Keep detailed records of the incident, response actions, and lessons learned. This is also essential for regulatory compliance.

Step Two: Restore from secure backup

As outlined in your IRP, the restoration step is the next essential step in recovery from ransomware. A business runs on its data and must quickly gain access to critical documents and files. Restoring data stored in a secure, ransomware-proof back-up will get your company back into production. However, this can only be done by initiating the previous steps of the incident response plan, which include removing the ransomware and securing all systems.

Step Three: Communicate and collaborate

Communication and collaboration may seem like the last thing you want to do after a ransomware attack; however, these are essential elements in protecting your company. Being open and transparent about the attack can help to stop it from propagating across supply chain members. Transparency with customers can mitigate the fallout from the attack that could affect your reputation. Collaboration with law enforcement, supply chain members, consultants, and any national body for ransomware incident sharing prevents future attacks and reduces the power of cybercriminals to continue attacks unabated.

Future trends in ransomware

Prevention and recovery from ransomware are essential aspects of a CISO's role in the modern enterprise. Effective ransomware attack and incident management also require that a CISO keeps on top of the trends in ransomware. Maintaining knowledge of cyber security is an ongoing exercise.

However, one key area to watch in coming years is the use of AI by ransomware attackers. According to GCHQ's National Cyber Security Centre, GenAI will be increasingly used to compose believable phishing emails and develop ransomware code. [17] Along with RaaS, AI-enabled ransomware will lower the bar to entry for potential attackers. This is likely to result in increased threat volumes. The speed of innovation in ransomware variants that AI could offer will also make tools, such as email security gateways, less effective. This leads back to the use of a defence-in-depth approach to ransomware prevention. Using a mix of measures, including human-centric protection from simulated phishing and Security Awareness Training, will provide the layers of protection needed to mitigate AI-enabled ransomware.

Prevention is better than the cure

The accessibility of ransomware and the human-centric nature of ransomware attacks have provided the perfect playground for cybercriminals to make money. Ransomware is lucrative, with ransoms bringing in over $1 billion USD (£800 million GBP) in 2023. This cash-rich crime will only attract more cybercriminals to the scene, and Ransomware-as-a-Service, along with AI-enabled ransomware, will open the floodgates.

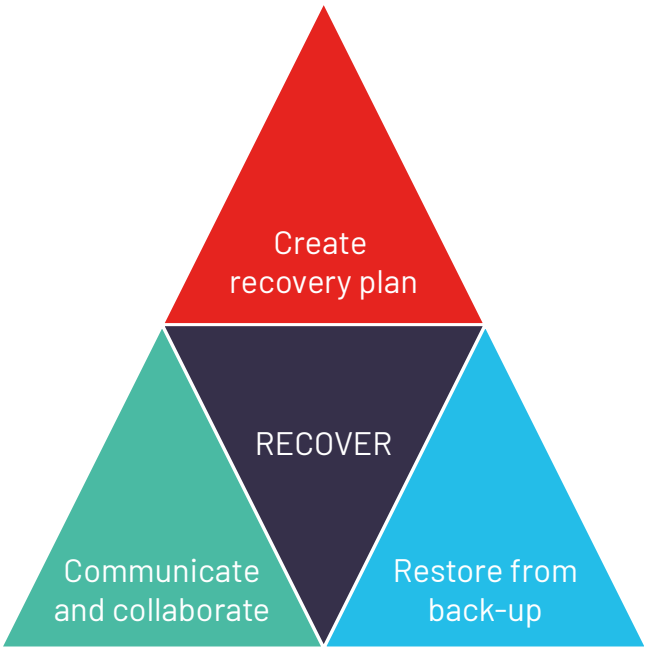
A CISO has their work cut out to mitigate the risks to their organisation. In the case of ransomware, however, prevention is better than the cure. Contingency plans are essential, as there is no failsafe against ransomware. However, a defence-in-depth approach using symbiotic measures will help prevent even emerging ransomware threats.

Ransomware prevent and recover at-a-glance

Prevent

- Stop web access
- Encrypt
- Patch
- Least priviledge
- Supply chain risk
- Phishing simulations
- Security awareness

Recover



References

[1] https://www.europol.europa.eu/media-press/newsroom/news/international-collaboration-leads-to-dismantlement-of-ransomware-group-in-ukraine-amidst-ongoing-war

[2] Verizon 2024 Data Breach Investigation Report (DBIR) https://www.verizon.com/business/en-gb/resources/reports/dbir/

[3] Sophos State of Ransomware 2024 report: https://www.sophos.com/en-us/content/state-of-ransomware

[4] NCC Group Releases Annual Cyber Threat Monitor Report 2023 https://www.nccgroup.com/uk/newsroom/annual-ransomware-attacks-increased-by-84-in-2023/

[5] Chainalysis 2024 report https://www.chainalysis.com/blog/ransomware-2024/

[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

[7] https://www.cisa.gov/sites/default/files/2024-02/aa24-060a-stopransomware-phobos-ransomware_1.pdf

[8] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

[9] https://www.ic3.gov/Media/News/2021/210108.pdf

[10] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

[11] https://www.akamai.com/newsroom/press-release/akamai-research-rampant-abuse-of-zero-day-and-one-day-vulnerabilities-leads-to-143-increase-in-victims-of-ransomware

[12] https://www.keepersecurity.com/en_GB/resources/workplace-password-habits.html

[13] https://www.sophos.com/en-us/content/state-of-ransomware

[14] https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/

[15] https://www.sophos.com/en-us/content/state-of-ransomware

[16] https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

[17] https://www.ncsc.gov.uk/news/global-ransomware-threat-expected-to-rise-with-ai