Security Awareness Program for Ransomware Attack

Pavlo Bokovyi

Table of Contents

Summary.....3
Section 1: Introduction.....3
Section 2: Goals of the Security Awareness Program.....5
Program goals.....5
Audience.....5
Content Modules.....5
Frequency of Training.....6
Section 3: Contextual concept.....6
Ransomware Awareness.....6
Common Delivery Methods for Ransomware Phishing emails.....6
Employee Actions to Avoid Ransomware.....7
Ransomware Detection.....8
Steps to Take if Infected.....9
Section 4: Implementation Strategy.....10
Timeline.....10
Employee Participation.....10
Tracking Success.....10
Section 5: Challenges and Solutions.....10
Common Obstacles.....10
Methods of solving challenges.....10
Chapter 6: The Maturity Model.....12
Conclusion.....13
References.....14

Summary

This report was created to establish a security awareness program, outline its feasibility and necessity. It is intended to familiarise employees with the new threats associated with ransomware and to enhance the cybersecurity culture. This program is important for the company because of the value of the data that is handled within the product. Financial and medical data are particularly valuable to attackers, hence it's quite sensitive.
The Company is implementing this program to ensure that employees can quickly and efficiently recognise and respond to threats posed by ransomware and other attacks, and to appropriately handle risks.
The program meets industry best practices and regulatory requirements. It consists of structured learning steps, including ransomware simulations, phishing awareness exercises, and incident response training.

Section 1: Introduction

Ransomware is a type of malware that blocks access to a device or the data stored on it, mostly by encrypting files. Attackers generally start by demanding a ransom in exchange for decryption (‘What Is Ransomware? How to Prevent Ransomware Attacks?’ 2025a). Attackers may choose a potential target for an attack due to security or other issues. Since the attacks are focused on data access, the logical target is companies where access to data is critical in terms of business processes, such as the Company, as it involves medical data that is highly valuable. Therefore such data must be available at any time at the request of an authorized client. There are several stages of the attack, which are divided into sequential phases, each of which is designed to accomplish certain tasks. For example, first, it is necessary to collect as much information as possible about the target of the attack, its network structure, etc. The sequence of steps in a ransomware attack is shown in Figure 1.

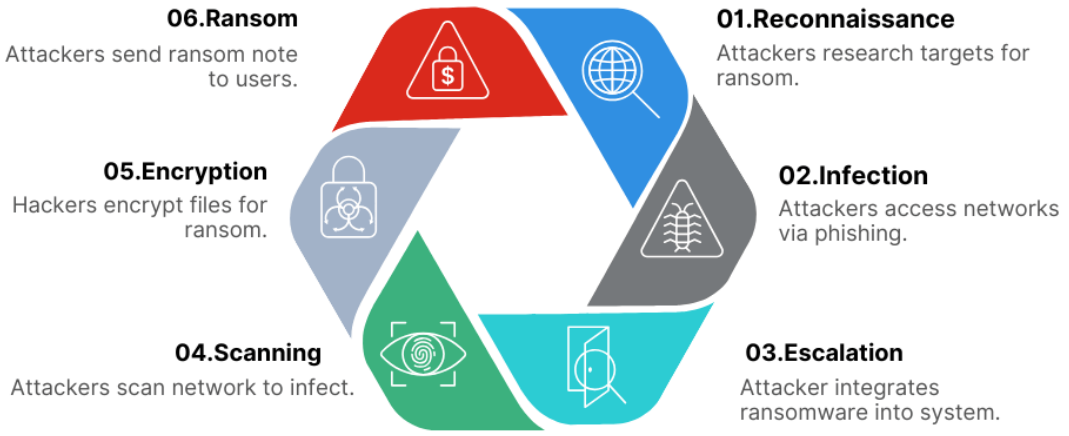

Figure 1 Six stages of ransomware attack (‘What Is Ransomware? How to Prevent Ransomware Attacks?’ 2025b)

As of 2025, ransomware is one of the biggest cybersecurity threats to mid-market and enterprise companies. This is due to the complexity of the attacks, the level of expertise of the attackers, and the potential consequences for the organization. Over the past 10 years, a very

large number of organizations have become victims of ransomware, including the most famous Bad Rabbit in 2017, Petya in 2016, and Wannacry in 2017 (‘What is Bad Rabbit ransomware? | NordVPN’ 2024). With losses estimated in the billions of dollars, preventive measures to ensure a decent level of cyber security are critical to ensuring business continuity.

Among the main potential consequences of ransomware for companies are: loss of money, reputational damage, and regulatory risks from the regulator (‘13 Biggest Ransomware Attacks in History’ 2025) .

The information security awareness program is a set of measures aimed at improving the company's current cybersecurity posture. One of the key objectives of the program is to raise awareness of information security among employees at all levels of the company, as well as to inform them about what to do in the event of an incident and what actions are necessary in daily activities to avoid threats from ransomware as much as possible (‘Information Security Awareness Program | Maynooth University’ 2025).

The relevance of implementing this program is that the threats of ransomware remain with businesses and are likely to remain constant. At the time of writing, a new ransomware program called Medusa is being widely used, with details provided by the Cybersecurity and Infrastructure Security Agency (‘#StopRansomware: Medusa Ransomware | CISA’ 2025).

As noted, more than 300 organizations have already experienced ransomware. The result of the attack is shown in Figure 2 (‘Medusa Ransomware: FBI and CISA Urge Organizations to Act Now to Mitigate Threat | Tripwire’ 2025). Therefore, the actuality of the threats is high, while the first link in most ransomware attacks is the company's employees, so their awareness is a critical factor that affects security.

Figure 2 Medusa Ransomware's example of operation is March 2025 (‘Medusa Ransomware: FBI and CISA Urge Organizations to Act Now to Mitigate Threat | Tripwire’ 2025).

The security awareness program involves cyclical stages as it is rolled out. A visualization of these steps is shown in Figure 3. In particular, the following phases are highlighted:

- Assessment - identifying security risks and vulnerabilities by evaluating and modelling attacks.
- Training - conducting specialized training on threats, including phishing and ransomware.
- Reinforcement - using phishing attack simulations, as well as reminders and rewards to raise awareness.

- Measurement & Optimization - tracking security metrics and continuously improving the program.

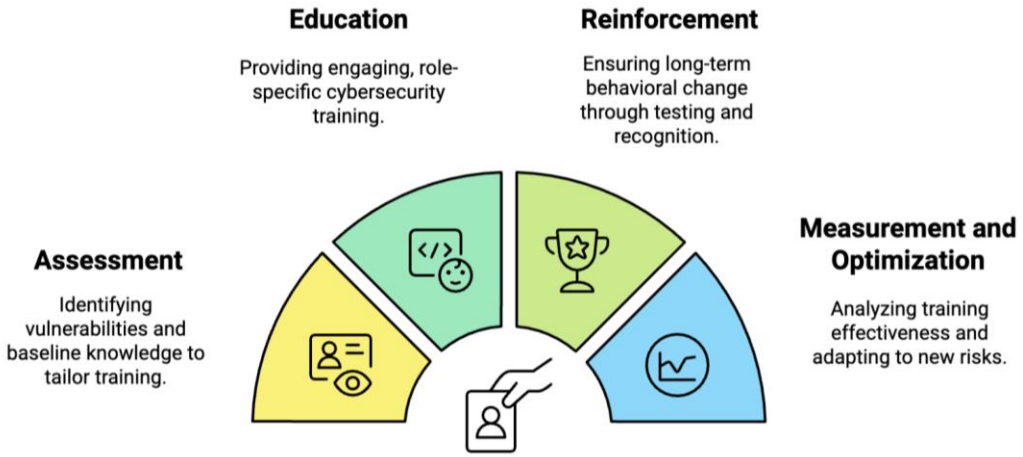

Figure 3 Security awareness cycles (Labs 2025)

Companies can minimize risk while ensuring compliance by proactively reducing human error by implementing quality security awareness programs and building a security culture.

Section 2: Goals of the Security Awareness Program

Program goals

The program is intended to:

- Provide training opportunities for employees to reduce the risk of a successful ransomware attack
- Mitigate the impact of potential attacks by raising awareness.
- Ensure compliance with regulatory security standards.
- Provide instructions for action in the event of an incident
- Ensuring best practices against ransomware - technical and non-technical.

Audience

The program applies to all employees of the company from all departments. An individual approach is provided depending on the level of authorization and responsibilities. The program involves interaction with:

- Strategic level - senior level (CISO, CTO, CEO, CFO) and management.
- IT and information security personnel involved
- Employees at the operational level - sales, marketing, development, etc.

Content Modules

The content of each section of the program provides the necessary depth for the appropriate operational level.

It includes the consideration of the next modules:

- The nature of ransomware, stages of attack, types of challenges, and possible risks.
- Phishing as the first step to a successful attack. Definition of phishing emails and the threats they pose.
- The sequence of actions in case of an attack - reporting, procedures and steps depending on the role.
- Common best practices for data protection (requirements for passwords, software updates, interaction with company policies)
- Working from your own devices and or from home or other non-corporate networks.
- Simulation exercises to rehearse actions in the event of an attack.

Frequency of Training

The following training frequency is provided for employees:

- Quarterly sessions for all employees.
- Twice-yearly advanced training courses for IT and security teams.
- Demand-based training on new threats related to ransomware.
- In the event of an incident, mandatory training is provided after the incident is successfully resolved to analyze the causes and consequences of the incident.
- Mandatory individual training for new employees as part of onboarding

Section 3: Contextual concept

Ransomware Awareness

As outlined in the previous sections of this report, the impact of ransomware can affect any employee in a company, so every department has to be well aware of the dangers and how to avoid them.

Locker ransomware. The ransomware tries to restrict access to the basic system functions of the computer, which makes the system practically unusable. In particular, you can lose access to the desktop, and the mouse and keyboard functions can be partially disabled - exclusively for interaction with the ransomware window. Ransomware usually does not encrypt important files, but only blocks access to the system. Therefore, the probability of complete data loss is relatively low.

Crypto ransomware. The second type of attack involves cryptographic ransomware that encrypts important files, such as documents and customer data, without disrupting the operating system. This causes panic as users see their files but cannot open them. Attackers often add a timer to the ransom demand, threatening to delete all files after the deadline if payment is not made.

Due to the lack of backups in cloud storage or on external media, many users suffer significant losses. As a result, many victims agree to pay the ransom in the hope of recovering their data.

Both outcomes lead to significant financial losses or can even lead to the collapse of the company (‘Ransomware Attacks and Types | How do Locky, Petya and other ransomware differ?’ 2021).

Common Delivery Methods for Ransomware

Phishing emails. The most popular first step in compromising a company is phishing emails. A phishing email is an email that contains malicious links, file attachments, etc. and is designed to make the employee perform an action that the attackers expect. Such ransomware attacks often start with a seemingly harmless action - an employee clicks on a link in a phishing email or downloads a malicious attachment. After that, the employee may not notice any other changes, but they are actually there. The links may redirect victims to malicious websites that secretly download ransomware, and the attachments may contain executables or documents with dangerous macros disguised as invoices or reports. Once opened, the ransomware quietly installs encryption files and blocking systems until they demand payment.

Social engineering increases the danger. An employee may receive an email claiming to be from a current colleague, manager, etc. The main task is to look as similar as possible to a legitimate email.

Phishing emails are a highly effective delivery channel for ransomware that looks like it's legitimate, mimicking trusted organizations such as banks, healthcare providers, or social media platforms. The persuasiveness of such emails, combined with tactics such as urgency or authority, manipulates users into clicking on malicious links or opening infected files. Such emails frequently avoid major spam filters and reach inboxes directly (‘How Ransomware Is Delivered and How to Prevent Attacks’ 2025).

Compromised Websites

Often, malicious actors carry out drive-by attacks by exploiting known vulnerabilities in the software of legitimate websites. When the victim visits an infected website, the ransomware is downloaded unnoticed and executed without their knowledge.Therefore, any non-work Internet surfing from work devices is not desirable and should be covered in the company's information security policy.

Infected Removable Media

USB devices and other removable media are an easy and convenient way to spread ransomware between computers that are not directly connected to each other or to the Internet. Connecting an infected external device can trigger an attack on the local system and potentially spread across the network. Therefore, employees should pay attention to unfamiliar media that they may find inside or outside the office. It is unacceptable to connect these types of storage media to work computers, especially those with valuable data or whose owners hold managerial or other important positions.

Unauthorised Remote Desktop Protocol (RDP) Access

Threat actors can gain access to the network by using RDP (Remote Desktop Protocol), so any equipment that potentially has access to important elements of the company's system must be functionally isolated from unauthorized access (‘Internet Accessible Remote Desktop Protocol (RDP)’ 2025).

Supply Chain Attack

Attackers can access the systems of many organizations through the use of third-party trusted vendors. By exploiting vulnerabilities in interconnected supply chain systems, they can organize a ransomware attack. Therefore it's important to pay attention to the interaction in the context of third-party vendor access to company resources and mechanisms such as SSO.

Exploit Security Vulnerabilities

All equipment used by the company is a potential surface for attacks from the hardware and software point of view. Therefore, it is important to update devices to the latest recommended firmware and OS versions in a timely manner, and to track potentially vulnerable devices based on key metrics and indicators. In particular, it is worth considering such data as the end of service and the life of the product.

Employee Actions to Avoid Ransomware

There is no single solution that can provide complete protection against ransomware attacks. Instead, a proactive, multi-layered approach that combines state-of-the-art security measures with effective cybersecurity practices is required. The following are recommendations for all employees of the company (‘Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches’ n.d.).

- Use VPN services when connecting to public Wi-Fi networks.
- Avoid clicking on unfamiliar or questionable links.
- Update your software and operating system regularly.
- Avoid using unreliable USB drives.
- Download only from trusted sources Do not open emails or attachments from unknown sources.
- Keep your personal information private.

Particular attention should be given to social engineering and phishing emails, as shown in Figure 4, which contains several points to look for when reading an email. Likewise, a similar focus should be placed on social media messages, messengers, and any other communication channels.

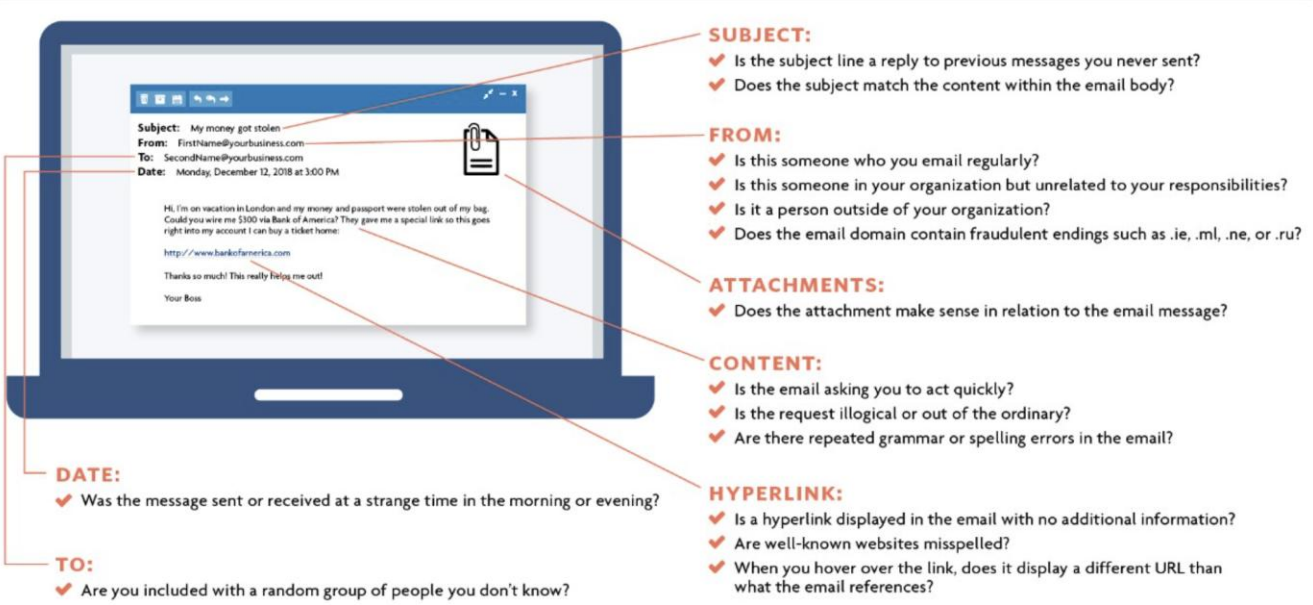

Figure 4 Red flags to pay attention to (‘Phishing Scams’ 2025)

The following proactive actions are important for the security team and IT to take to protect against the ransomware risk.

- Apply additional security, such as enabling multi-factor authentication and login notifications, if available.
- Use the principle of least privilege and re-authentication controls to ensure that users have only the minimum access needed, with the ability to increase privileges as needed.
- Restrict access to any unknown devices, such as USB drives, and implement a zero-trust environment that requires all network actors to prove their security before gaining access.
- Protect both online and offline data backups to prevent them from being overwritten by files encrypted with ransomware.
- Systematically conduct security risk assessments and audits in accordance with the organization's information security policy.
- Create, maintain, and implement incident response, backup, and disaster recovery plans to ensure critical systems are available and business continuity during emergencies.
- Regularly back up important files and check that they can be restored when needed. Backups should be offline and in a separate location - ideally offsite or in a cloud service. Don't use just one backup solution. Disconnect backup devices, such as external disks or USB drives, from the network. Connect backups to trusted and clean devices before starting a restore, and always scan them for malware. Use mechanisms such as privileged access workstations (PAW), multifactor authentication (MFA), and privileged access management (PAM) to protect your backup systems from unauthorized access.

Ransomware Detection

Continuous monitoring of the company's network can detect intrusions in a timely manner, recognize unusual activity, and prevent a complete incident or its further escalation into a disaster.

Particular attention should be paid to important systems and computers where backups are stored, regardless of whether it is part of the company's network or access to third-party services where backups are stored, such as cloud services. For this task, it is recommended to use such systems as ISD and IPS.

It is worth remembering that in the case of sophisticated attackers, they may try not only to encrypt company data but also to destroy or encrypt backups. This technique is described as

Inhibit System Recovery according to Mitre (‘Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®’ 2025).

The reporting of all employees to the cybersecurity department has to be agreed and coordinated. In the event of characteristic signs of a ransomware attack, such as ransomware windows, the responsible person from the security department should be immediately notified, and if that person is not available, the CISO should be informed.

Steps to Take if Infected

Apart from the obvious demands of ransomware, the intrusion and the incident itself can be detected by attack and compromise indicators.

If an attack is confirmed or is highly likely, it is important to take steps to eliminate and recover from it. Any employee should immediately notify the security team or the person in charge (cybersecurity analyst or CISO).

The team should take the following steps:

- First of all, it is necessary to isolate the systems. Disconnect the infected devices from the network to avoid infection to other parts of the network.
- If necessary, turn off the device and, if needed, power down the compromised equipment, while preserving the data of the current workflow as much as possible.
- When the incident has been stopped and localized, it is essential to assess the state of protection and the network. It is necessary to keep in mind the continuation of business processes if it is possible to do so without the guaranteed influence of the attackers on the equipment involved.
- Prioritize recovery efforts: Focus on restoring critical systems first, rather than those that are not affected.
- Business continuity is a priority.
- Document all actions and steps taken for further analysis and to ensure that the system does not remain compromised.
- Collect system images, logs, and artifacts for further investigations. Analyze detection tools: Examine the antivirus, EDR, and logs for indications of a predecessor malware. It is also necessary to detect earlier infections, such as TrickBot or Emotet, before recovery.
- Recovery. Use clean images, make sure that the attackers will not be re-introduced, fix vulnerabilities, and reset passwords.
- After the incident is over, making sure the systems are secure and the environment is clean (‘CISA_MS-ISAC_Ransomware Guide_S508C_.pdf’ n.d.).

It is important that all employees have clear instructions on what to do and who to contact in case of an attack. It is emphasized that it is critical to report not only the presence of ransomware but also phishing emails, especially if they are received regularly, as this may indicate an attempted attack. An example of information that all employees should have is the table shown in Figure 5.

State and Local Response Contacts:		
Contact	24x7 Contact Information	Roles and Responsibilities
IT/IT Security Team - Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

Figure 5 Information for all employees in case of an attack (‘CISA_MS-ISAC_Ransomware Guide_S508C_.pdf’ n.d.)

Section 4: Implementation Strategy

Timeline

This program will be rolled out in several successive stages.

- The first stage is the launch of the campaign, correcting all possible nuances and issues that may arise. It lasts for one month.
- The second stage is to conduct online training every week. The second stage also lasts one month.
- The third stage involves simulating real attacks and replaying the steps to inform the relevant personnel, checking documentation and procedures for localization and recovery from ransomware.
- This stage lasts 3 weeks. The results are recorded and documented, and in case of problems, they are all marked for further processing. An attack on staff computers can be simulated without interrupting business processes and its results documented.
- Ongoing: Performance tracking and adjustments.

Employee Participation

The training is held online every Saturday on the corporate platform. Classes are recorded, and in case of absence, the employee can view the recording. After each lesson, the employee has to pass a 30-question test and get at least 75%. Information about the test is recorded in the training log. Training and tests are mandatory, and a number of motivating factors can be used, such as bonuses, compensation for working outside of working hours, or, conversely, a reduction in bonuses in case of refusal to attend training. These aspects should be agreed with the CISO, HR department and relevant authorized persons (CEO).

Tracking Success

The results of successful program implementation can be tracked by KPIs. These include the number of reports of phishing emails, the number of incidents involving the opening of phishing attachments and links.

Section 5: Challenges and Solutions

Common Obstacles

Potential problems include:

- Lack of interest among employees to attend training
- Employees may forget information about the ransomware after a certain amount of time after the training
- Lack of time to complete the training

Methods of solving challenges

- Gamification - learning can be made interesting and interactive. Using short reminder brochures that can be placed in the main areas and or at workplaces. An example is shown in Figures 6 and 7.

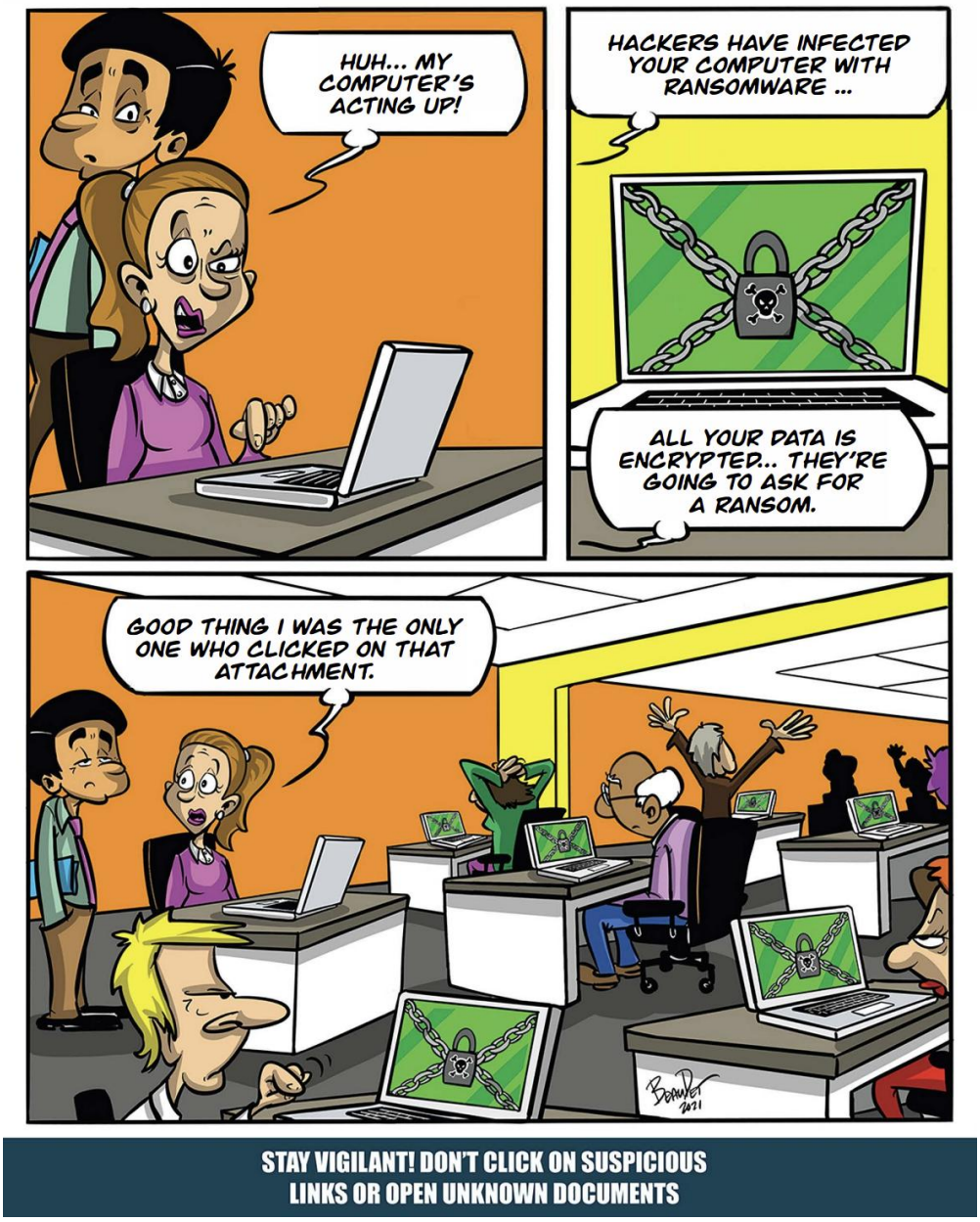

Figure 6 A gamified threat reminder ('fta-tn-ransomware-in.pdf' n.d.)

Figure 7 Short key points for employees ('fta-tn-how-to-protect-your-data-from-ransomware-attacks-in.pdf' n.d.)

- Management involvement - not only operational but also controlling staff should participate in the training, as this can build trust and encourage all segments of the company.
- Practical cases - demonstration of actual incidents related to the requirements. Visualisation of lost financial assets and reputations of other companies. Creating a logical connection that ransomware can lead to business closure and, consequently, to the loss of jobs by employees, therefore creating responsibility for their actions on the part of employees.

Chapter 6: The Maturity Model

The security culture maturity model assumes a gradual development to a higher level of information security in a company. There are many variations in describing progress and assessing the current state of maturity. It is worthwhile to identify the most effective solutions on the market, in particular, the proposed model from NIST - CSF Maturity Model. The model visualisation is shown in Figure 8.

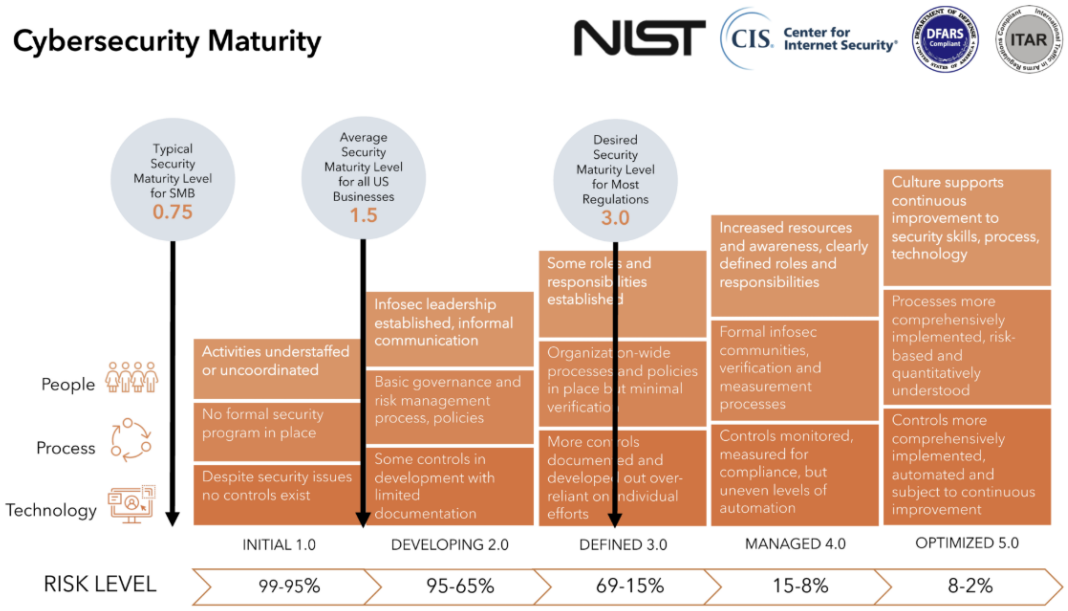

Figure 8 Maturity assessment levels according to the NIST framework

This infographic shows the security maturity score from 0 to 5, the higher the maturity level, the lower the potential risks for the company. As can be seen, the desired maturity level for most regulations is 3. Since the company is developing a product that interacts with patients' medical data, the company's security maturity goal should be level 3 or higher (cinchws 2022).

Conclusion

To conclude, it can be emphasised that ransomware is a growing threat, so employee training is a critical factor in protection. Comprehensive security awareness measures provide employees with the necessary knowledge to detect, prevent, and respond to attacks, increasing the overall resilience of the organization. By integrating structured training, detection tools, and proactive defence strategies, the business reduces the risks associated with the threat of ransomware attacks.

Adopting a maturity model ensures continuous improvement, helping the organization stay ahead of new threats, given the regulatory and organizational context, level 3 or higher should be achieved.

Activities for different levels of the company's personnel were described, as well as details of training, potential challenges and proposed solutions for them.

References

13 Biggest Ransomware Attacks in History [online] (2025) available: https://www.cobalt.io/blog/11-biggest-ransomware-attacks-in-history [accessed 22 Mar 2025].

cinchws (2022) 'Are you prepared to defend your law firm against cyberthreats?', *Strategic Technology Solutions*, available: https://stspartner.com/are-you-prepared-to-defend-your-law-firm-against-cyberthreats/ [accessed 23 Mar 2025].

'CISA_MS-ISAC_Ransomware Guide_S508C_.pdf' (n.d.) available: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf [accessed 22 Mar 2025].

'fta-tn-ransomware-in.pdf' (n.d.) available: https://static.fortra.com/terranova-security/pdfs/infographic/fta-tn-ransomware-in.pdf [accessed 23 Mar 2025].

How Ransomware Is Delivered and How to Prevent Attacks [online] (2025) *Akamai*, available: https://www.akamai.com/blog/security/how-ransomware-is-delivered-prevent-attacks [accessed 22 Mar 2025].

Information Security Awareness Program | Maynooth University [online] (2025) available: https://www.maynoothuniversity.ie/information-security/information-security-awareness-program [accessed 22 Mar 2025].

Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK® [online] (2025) available: https://attack.mitre.org/techniques/T1490/ [accessed 22 Mar 2025].

Internet Accessible Remote Desktop Protocol (RDP) [online] (2025) available: https://www.ncsc.gov.ie/emailsfrom/reports/vp/rdp/ [accessed 22 Mar 2025].

Labs, K. (2025) What Is the Security Awareness Cycle? - Keepnet [online], *Keepnet Labs*, available: https://keepnetlabs.com/blog/what-is-the-security-awareness-cycle [accessed 22 Mar 2025].

Medusa Ransomware: FBI and CISA Urge Organizations to Act Now to Mitigate Threat | Tripwire [online] (2025) available: https://www.tripwire.com/state-of-security/medusa-ransomware-fbi-and-cisa-urge-organizations-act-now-mitigate-threat [accessed 22 Mar 2025].

Phishing Scams [online] (2025) available: https://www.palatinebank.com/personal/resources/security/phishing-email-scams/phishing-scams.html [accessed 22 Mar 2025].

'Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches' (n.d.).

Ransomware Attacks and Types | How Do Locky, Petya and Other Ransomware Differ? [online] (2021) /, available: https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types [accessed 22 Mar 2025].

#StopRansomware: Medusa Ransomware | CISA [online] (2025) available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a [accessed 22 Mar 2025].

What Is Bad Rabbit Ransomware? | NordVPN [online] (2024) available: https://nordvpn.com/blog/bad-rabbit-ransomware/ [accessed 22 Mar 2025].

What Is Ransomware? How to Prevent Ransomware Attacks? [online] (2025a) *Fortinet*, available: https://www.fortinet.com/resources/cyberglossary/ransomware [accessed 21 Mar 2025].

What Is Ransomware? How to Prevent Ransomware Attacks? [online] (2025b) *Fortinet*, available: https://www.fortinet.com/resources/cyberglossary/ransomware [accessed 21 Mar 2025].