RISCS Ransomware Workshop: Industry Perspectives

RISCS held an online workshop on 26th May 2022 as part of the Cybercrime theme led by Dr Maria Bada, with 10 participants mainly from the private sector.

Context

Our work to date on this topic has found that three main factors can increase vulnerability to ransomware attacks such as: a) organisational factors and decision-making processes within organisations; b) the human factor (the individual); and c) the lack of resources.

Workshop aim

This workshop sought to understand what the private sector considers to be 'best practice' in defending against ransomware. It also aimed to better understand the challenges organisations face in decision making and the steps they should take after an attack happens. The primary objectives were to identify:

- The decisions that need to be made and by who
- The factors which should be considered when responding to a ransomware attack
- The impact of such an attack

After the workshop we analysed the results of all scenarios and we produced a Best Practice Guide to defend against ransomware.

Summary of recommendations

Preventative measures

Steps to prevent a ransomware attack:

1. Follow best practices on security hygiene
2. Conduct table-top exercises
3. Deploy endpoint detection and response
4. Implement multi-layer prevention capabilities

Incident Handling

How to respond to a ransomware attack:

1. Ensure clear decision making after an attack
2. Identify who to contact after an attack
3. Identify the crisis team
4. Isolate the infected computer
5. Prepare a governance plan
6. Plan a communications response
7. Report the attack

The Activity

Participants analysed three scenarios based on organisations in different sectors who have experienced a ransomware attack.

The first scenario described the case of a manufacturing company which suffered a ransomware attack after the use of an unsecure USB to transfer files.

The second scenario described the case of an SME in the retail sector which suffered a ransomware attack due to the owner's son using his computer to play video games when visiting the office.

The third scenario focused on the health sector and specifically an organisation which conducts COVID-19 research and provides vaccinations in central Europe. For each scenario, participants explored the following:

- The amount of ransom requested
- The value of assets compromised
- The type of data affected
- The level of risk the company is willing to take; and
- The cyber maturity of the organisation on review

Participants discussed the following for each scenario:

- Time available to decide on paying the ransom or not
- The critical importance of affected data and systems
- The availability and integrity of data backups
- The cost of the ransom vs the estimated cost of production and restoration
- The likelihood of successful restoration (whether the ransom is paid or not)
- Any regulatory implications

Best Practice Guide to Defend Against Ransomware

After the workshop we analysed the results of all scenarios and we produced a Best Practice Guide to defend against ransomware. The Best Practice Guide is practice-inspired and industry-validated by participants. The Guide provides organisations with both a set of preventative measures to reduce attack vulnerabilities as well as a set of guidelines for actively dealing with an attack.

Preventative measures

1. Follow best practices on security hygiene

This is one of the most important recommendations since it includes different steps which can be taken in order to prevent an attack:

1. Back-up data regularly and test the restoration process.
2. Secure offline backups by ensuring that they are not connected permanently to the computers and networks they are backing up.
3. Implement an awareness and training programme: ransomware attacks can stem from a phishing attack. End users are top targets, therefore all employees need to be aware of the possible risk of a ransomware attack and how it is delivered. Training on cybersecurity basics and best practice is essential to help end-users identify phishing emails and other common cyber scams that threaten the network's security.

2. Conduct table-top exercises

A ransomware table-top exercise begins with a specific ransomware attack scenario, describing the details of the attack, and how the organisation reacts, step by step. Every company's approach to ransomware will vary based on numerous factors, such as size, network and infrastructure resources and existing software.

3. Deploy endpoint detection and response

Every device connected to a network is a potential entry point for hackers. All of these entry points, known as "endpoints," need to be included in an organisation's cybersecurity plan. The purpose of an endpoint protection platform (EPP) is to stop threats before they can be installed on devices. The purpose of an endpoint detention and response (EDR), on the other hand, is to detect threats that have installed and started to run on a device in the network and automatically respond to them. Larger companies are more likely to have response plans in place, but these plans can be subverted by panic during an attack.

4. Implement multi-layer prevention capabilities

Implementing multi-layered security is crucial to protect the network, users, and business-critical data. The main security layers which should be in place are as follows:

- Firewall: A firewall acts as a barrier between a trusted network and an untrusted network, only allowing into your network traffic that has been defined in the security policy.
- Patch Management: Patching is the process of distributing and applying updates to software and firmware. Patches are important to address functionality errors or bugs, boost performance, and close the security gaps that would otherwise leave your systems, software, and applications vulnerable to cyberattacks.
- Multi-Factor Authentication (MFA): Enabling MFA is one of the most important steps to reduce the risk of a cyberattack. These additional forms of authentication prevent hackers from exploiting weak or compromised end-user credentials to access a network.
- Email Filtering: Filtering emails at the gateway reduces the risk of phishing and helps to protect users and businesses from cyber threats such as phishing attacks, ransomware, viruses and malware, and business email compromise.
- Sophisticated Password Policy: Password policies set organization-wide rules about password strength and complexity (e.g., irregular capitalization and special characters) to prevent password re-use, prohibit weak passwords, and improve network security.
- Physical Security of IT infrastructure: Physical security measures restrict access to and protect infrastructure and spaces in which data is stored. These can be access control systems, security cameras and surveillance, and security personnel.
- Business Continuity and Disaster Recovery (BCDR): BCDR solutions can mitigate the downtime and damage associated with a cyberattack, allowing to restore data and operations from a backup. Two important measures are: 1) Isolate backups to ensure that if the network is breached, backups can't also be accessed and encrypted; and 2) Ensure the business continuity plan is documented, tested, and regularly updated.
- Managed Detection and Response (MDR): MDR isolates suspicious behaviour on the network and detains confirmed threats to prevent spread.

Best practice guidelines for incident handling

1. Decision making after a ransomware attack

Most organisations will need to know what data and what percentage of the data they could retrieve in order to decide whether to pay the ransom or not. The decision depends specifically on the type of data impacted, systems used and the malware used for the attack. It is a trade-off between what will be lost if the business is down by a day, compared with the amount being asked in ransom.

Most organisations would only need around 10% of business-critical data back. In addition, individuals and organisations can get a sense of the level of damaged data within the first 5-10 days. SMEs tend to panic more as there is minimal preparedness for business continuity. It is advisable to get negotiators to prolong the period given before a pay-out to use the prolonged time to recover data from relevant backups. Participants also suggested it is important to determine:

- If there is a free decryption tool
- The entry point to the attack and close it to minimise further victimisation and contain the attack

if the threat is to disclose personal data rather than just denial of service, this information will help inform the ransom payment decision.

2. Identifying who to contact after a ransomware attack

- Step 1: Reach out to your Managed service provider.
- Step 2: Contact the IT/service desk raising an incident. However, this could be challenging if all computers are affected by ransomware.
- Step 3: The IT/service desk investigating the scope of the attack. Closing the entry point to the attack is critical to avoid repeat victimisation.
- Step 4: Contact your Law Firm or relevant Legal Council, before reaching out to externals. It is recommended that companies notify the Information Commissioner's Office (ICO) and insurer (if relevant).
- Step 5: Third parties and suppliers might need to be contacted via other means such as by phone instead of email, as malware can propagate via email.
- Step 6: Lastly, consider engaging with Cyber Incident Response (CIR) partners and ransomware negotiators to try and extend the ransom payment deadline set by the attackers.

3. Identify the crisis team

Identify key employees who will become members of a ransomware crisis team and put measures in place to ensure they can be easily reached after a ransomware attack. The crisis team will be making decisions about handling the attack. Ideally, the crisis team should include members of the leadership team, the Director of IT, Department Chiefs, PR, Sales and Comms.

4. Isolate the infected computer

Irrespective of the sector, isolating the infected computer/system and contacting the IT personnel is the most effective first response to an attack. If IT and other networks are interdependent, the computer should be isolated and production or services stopped. In the manufacturing scenario, all participants agreed to isolate the computer by disconnecting it from the network and stop production. The IT team can then revert to back ups. If computers and systems are up to date, then the ransomware attack should not spread easily. In addition, If IT and production line networks are separated work may continue despite the attack.

5. Prepare a governance plan

This will depend on the size of an organisation. A governance plan would include defining:

- Roles and responsibilities of each member of the ransomware crisis team need to be defined and explained to ensure clear chain of command and efficient response.

- Response at a technical level, communication level but also response level, making a decision to pay ransom or not. Note: The NCSC and law enforcement do not encourage, endorse nor condone the payment of ransom demands.

6. Plan a communications response

- Document audiences that will require immediate notification (customers, employees, attorneys, other stakeholders).
- Identify who will communicate the message and how (who will be the spokesperson, how will communication take place if means of communication are disrupted).
- Create an internal communication plan that will enable sharing information swiftly with employees.
- All businesses should plan communications with the following stakeholders:
  - IT Manager: Might have an incidence response plan as per company policy. The challenge however, is the ability to utilise the plan. This is dependent on the company's business continuity maturity. Correlation between size of company and incident response plan – the smaller the company the lower the likelihood of this being in place.
  - Leadership: If personal records are impacted, all leadership levels should be informed.
  - Employees: Carefully consider the communication plan and timings for sharing information about the attack with employees.
  - Legal: When does legal come in? Legal to be informed before external stakeholders.
  - Insurance: Informing insurance companies can be done after the stakeholder groups above.

7. Reporting

Under the GDPR (General Data Protection Regulation) organisations are required to notify their relevant supervisory authority within 72 hours of discovering certain types of data breach.

The NCSC is supporting reporting by the use of a newly developed web tool which will guide reporting processes.

Ransomware and the Impact to Business

Participants also discussed the different types of harms and impact stemming from a ransomware attack, based on the three scenarios. These can be:

Financial:

- Production line disruption.
- Payroll impact on employees.
- Supply chain issues.
- Potential fine from the Information Commissioner's Office (ICO) depending on the nature of the breach.

Social:

- Impact on the security culture of the organisation.
- Lower morale for employees.
- General user worry about the breached data.

Physical:

- If the malware has spread, equipment might not work, putting lives in danger.
- Impact such as health outcomes or loss of life.

Psychological:

- For employees fighting the hackers.
- Customer Impact.

Political:

- Loss of trust in the government generally and healthcare as a result of the attack on the health sector organisation conducting COVID-19 research and providing vaccinations in Europe.

Reputational impacts:

- Impact on the organisation's reputation, depending on the type of the attack and if the hackers are threatening to disclose data.

Participants list by organisation

- AwareGo
- Cyber Smart
- Kivu
- KPMG UK
- NCSC
- Skales
- University of Kent

Contributors

This workshop and report were produced with support from the RISCS team and with Dr Esther Edun as part of the Research Institute for Sociotechnical Cybersecurity (RISCS) Fellowship on Cybercrime led by Dr Maria Bada, QMUL.

Contact us

Dr Maria Bada, Lecturer in Psychology, Queen Mary University of London and RISCS Fellow for Cybercrime: M.Bada@qmul.ac.uk.