Final Assignment

Team Members

Xiaoyang Wei
Gray Li
Michael Huang

Contents

Executive Summary

XYZ Corporation is a supplier of laboratory automation, lab equipment, and chemical supplies to various universities, hospitals, and industrial and clinical labs. MTSTPro relies on a combination of novel molecular testing techniques but then uses advanced analytics and data science to analyze the data. By using machine learning, it can also fine-tune its analytical engine to further improve the speed and accuracy of detection over time. XYZ Corporation has decided to enter the diagnostic testing market and sell its MTSTPro system to its current customers to be used for Covid-19 testing.

To support the development of the new diagnostic system, XYZ Corporation has decided to deploy a Data Management System. This system also contains the results of the lab experiments that were performed, along with the interpretation of the experiment results. It connects to the other system systems using APIs. A Data Management system was already in development at IVDPro when it was acquired by XYZ Corporation. In the interest of speed and time to market, XYZ Corporation wants to use the system that was already developed as it already has the interface built to the analysis engine.

For part one, our team has reviewed all possible risk assessments on the data management platform; and identified twelve all high danger risks. For the top twelve high-danger risks, we have classified them by 4*4 levels of the risk matrix. For each risk, we also provided treatment and response to it. For part two, we briefly introduced what ransomware is. Our team then identified some of the most common ransomware threat vectors. We then provided 19 general practices to protect systems from ransomware. In case the system is attacked by ransomware, we provide a five-step recovery from a ransomware attack. We believe by all the documents provided below, the XYZ corporation can have a powerful means to protect their property and against ransomware.

Part I

The team has reviewed the data management platform and identified the following risks and treatments for those risks:

Category	Name	Description	Impact	Probability	Rating	Treatment/Response	Residual Risk
Supply Chain Risk	The 3rd party has a long response time (1)	The systems are covered by a support contract with a 3rd party support provider with a 4-hour response time; this means if the system is down and needs emerging support, there are at least 4 hours of downtime to the system. If the hardware component needs to be replaced but it is not in stock, it could take 48 hours for a part replacement.	Catastrophic	Remote	Serious-8	To require a shorter response time and ensure all required replacement hardware is in stock. The firms could build their own system support team as a second option.	
Program Risk	System in a dangerous room with another system and no temperature control. (2)	The system is in a high-temperature room with other systems. The room has no temperature control or redundant power supply. High temperatures could cause the system to have bad performance.	Major	Probable	Serious-6	XYZ Corporation has Tier III and Tier II data centers; they could move the system to either room.	
Competition Risk/Business Execution Risk	Slow system speed; customers and users have complaine	The system needs to be optimized to have the ability to handle more users concurrently using the system. This could cause customers to choose other	Negligible	Frequent	Medium-4	To optimal system to handle more users simultaneously, to make the system run faster.	

	d about it (3)	corporations because of the bad user experience.					
Security and Privacy Risk	Third-party access are allowed on the devices from the user (4)	Users can access the system through a web browser on their own laptops or desktops. The user uses the laptop for other activities, such as checking email. The scam email may contain viruses and capture information about accessing the corporation's system. This means the corporation's system has a high risk that accessed by hackers and causing the corporation's property lost.	Critical	Remote	Serious-6	User access to the system outside the company need VPN. Install a more professional anti-virus system on their personal laptop.	
Program Project risk	Testing (5)	All system configuration changes to the system are made manually and generally tested before on the development system before they are made on the production system, although there have been cases where some changes were not thoroughly tested in the development environment and made it to the production system, causing issues. When changes are not thoroughly tested before they are made on the production system. Firstly, it's a highly probable failure	Catastrophic	Probable	High - 12	Mitigation: Form a test team to focus on changes testing Or Transfer: ask for a Third-party assessment and testing	When executors lack experience or professional skills, some bugs may remain after testing (but since the rating decreases, we can accept)

		in the production system. Furthermore, it may change or destroy other implemented systems, which may cause the whole system to collapse.					
Data Breaching/ Business Execution Risk	Backups (6)	The database is backed up to offline storage and those backups are kept on-site. Only one backup is easy to be destroyed or lost, which may cause a data breach or be not able to use when we need it.	Critical	Remote	Serious-6	Recommend using a 3-2-1 backup strategy. It means having at least three copies of your data, two local (on-site) but on different media, and at least one copy off-site.	
Security and privacy risk/Reputational risk	User password (7)	Password aging or uniqueness is not enforced. Password aging or uniqueness can protect users' accounts from data leaks. Without aging and uniqueness, it's easier for other people to guess the password of users. It will also affect our reputation when users find their personal data leaked (although they may expose their passwords by themselves).	Critical	Probable	Serious - 9	Adds rules of aging and uniqueness when the user creates the accounts.	
Security and privacy risk	User authentication (8)	User management is done through the web server and is not linked to the corporate Active Directory, so neither single-sign-on nor multi-factor authentication	Critical	Probable	Serious - 9	Link user management to corporate Active Directory and implement either single-sign-on or multi-factor authentication	

		is available or used. It may let others who are not actual users- to log in the system					
Security and Privacy Risk	System Random Access (9)	Many of those team engineers or developers have root access to the system, and they are also the administrators for the web, application, and database servers. That would improve the risk of data leaks.	Critical	Probable	Serious - 9	The system should allow as few people to have root access to the system as possible. Some of those developers do not need full access to the system for their work responsibility. For those people who have root access, do not give them full access to those systems. In other words, even administrators can only have partial access to the systems, and that will reduce the risk of the leak of sensitive data.	
Security and Privacy Risk	Password Configuration (10)	It is unknown whether default passwords or configurations have been changed or not.	Catastrophic	Remote	Serious - 8	Check the current passwords and configurations. Change the default passwords and document the new passwords and configurations	
Safety Risk	Patching (11)	The systems are periodically patched, but they do not appear to follow a regular patching schedule. Sometimes a few weeks go by before some patches are installed.	Negligible	Probable	Medium - 3	The developers can set a specific time period for patching after talking to project managers and business analysts. Those people can help come up with a reasonable time range for patching. Then developers can develop	

						related algorithms to set up a static time range for system patching. The system can automatically achieve patching in a consistent time period. No one needs to worry about the consistency of the patching anymore, because the system will get patched automatically based on the business needs and requirements.	
Legal Risk	Approval Request (12)	There is a development version of the Data Management system where the developers develop and test their code, and once tested, the code is promoted to the production version. No pre-approval is required. A similar approach is taken with any database change.	Critical	Remote	Medium - 6	All the database changes need to get approved before they are promoted to the production version. Some of the updates might damage sensitive data or create a threat to the whole system. Therefore, database change should be approved by the business analyst and project managers before promoting to the production version.	

Figure 1 - Top Risks

	High	Medium	Low
High	High - 9	High - 6	Medium - 3 ③
Medium	High - 6⑤	Medium -4 ②④⑥⑦⑧⑨⑩(11)(12)	Low - 2
Low	Medium - 3	Low - 2	Low - 1

Figure 2 - Rating (3 * 3 Matrix)

When we analyze the probability and impact, we found that if we use 3*3 matrix, we will get many risks in medium level. In order to make a more clear classification, we decided to use a 4*4 matrix.

	Catastrophic:4	Critical:3	Major:2	Negligible:1
Frequent: 4	High -16	High - 12	Serious - 8	Medium - 4 ③
Probable: 3	High -12 ⑤	Serious - 9 ⑦⑧⑨⑩	Serious - 6 ②	Medium - 3 (11)
Remote: 2	Serious -8 ①	Serious -6 ④⑥(12)	Medium - 4	Low - 2
Improbable: 1	Medium - 4	Medium -3	Low - 2	Low - 1

Figure 3 - Rating (4 * 4 Matrix)

Part II

Introduction: What is Ransomware

Ransomware is a type of malware that encrypts files and information on a system and threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. The attackers can demand a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key, and the costs can range from a few hundred to thousands of dollars. The hallmark of ransomware has been the conspicuous ransom note that appears on victims' computer screens indicating files have been encrypted. Ransomware begins by gaining an initial infection on the system of an individual or employee at work. After gaining access to a system, ransomware can begin encrypting files. There are two common ways for ransomware to infect a device: through malicious emails, containing infected attachments that include intriguing or urgent names that encourage users to open them, or URLs, being used in emails that lure users into clicking to deliver web-based attacks with drive-by downloads or malvertising.

Protecting Data Management System from a ransomware attack

Guarding against common ransomware threat vectors

Here are some of the most common ransomware threat vectors that our team identifies:

- ***Credential phishing*** is where hackers attempt to steal credentials by pretending to be a trusted party in an email or other communication channel. Using links, attachments, or both. An email phishing attack seeks to trick users into taking some sort of action. Phishing emails containing link comes from some known contact, asking a user to enter credentials for a bogus purpose. The attacker can include fake attachments that enable ransomware to start downloading automatically. Those credentials then get stolen, and attackers will gain the access to those credentials and enable the installation of ransomware. Attackers might have built-in social engineering tools that trick users into allowing administrative access. Hackers will often sell the data they have collected to the dark web.

  Control: Knowledge is the best solution for credential phishing. Companies should educate employees about the dangers of phishing emails so they can be the first line of defense. The company can create a professional employee security awareness program that includes steps and quizzes to determine comprehension. In addition, companies can add practices for strong password protocol and overall cyber hygiene to avoid this issue.

- ***Remote Desktop Protocols*** is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. It is a protocol, or technical standard, for using a desktop computer remotely. RDP provides remote access through a dedicated network channel. An RDP-enabled application or service packages the data to be transmitted, and the Microsoft Communications Service directs the data to an RDP channel. From there, the OS encrypts the RDP data and adds it to a frame so that it can be transmitted. RDP ports are often poorly secured and easily compromised. In addition, RDP security relies heavily on proper password protocol, which can be ignored by users. Without a strong password for protection, attackers can easily infiltrate weakly protected RDPs to harvest credentials.

Control: To solve this issue, companies should focus on strengthening RDP, such as putting RDP behind a firewall, requiring strong passwords, employing two-factor authentication, and limiting IP access. The solutions above can help secure the RDP and prevent ransomware.

- ***Patches*** are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features. Unpatched software not only opens the door to malware intrusions but lays out a welcome mat as well. Without being properly updated and patched, attackers can access networks without having to harvest credentials. When they are in the systems, they begin attacking key programs and viewing or exfiltrating sensitive data. Many types of ransomware have evolved to forms that are difficult to detect, therefore extending their dwell time for maximum destruction.

  Control: The solution is to keep computer programs up-to-date and patch software in time. That will fix potential problems or bugs inside the system and prevent ransomware from hacking into the system.

- A ***Denial of Service (DoS)*** attack is an attempt to overload an IT infrastructure to cause systems and applications to become slow or unusable by customers. An attacker uses scripts to send an overwhelming number of complex requests to a system in an attempt to exhaust all of its resources (CPU, RAM, Storage, Network, etc.).

  Control: Improve our network security and strengthen our overall security posture by installing antivirus and anti-malware software and setting up a firewall that monitors and manages incoming traffic.

- ***Baiting*** is like the real-world *Trojan horse*. Therefore, it uses physical media such as a USB flash drive and prays on people's curiosity. An attacker may leave malware on a USB flash drive where it is expected that someone will find it. The person finding it may plug in the flash drive to research the contents out of curiosity or with the intent to identify the owner. Software is often "spring-loaded" to install as soon as the drive is connected, or as soon as any file is opened. The difference between baiting and other social engineering techniques is the promise of a good or gift that hackers use to Venice victims.

Control: The strongest defense against baiting is educating the team. Each one of the team should have a strong security culture within their surroundings. Every individual must consider *company security* as an essential part of their individual responsibilities.

General Best Practices

Here is a general list of best practices our team identifies which will develop a Defense in depth to protect or limit the risk of ransomware. Defense in depth is an information assurance strategy in which multiple layers of defense are placed throughout an IT system. Defense in depth addresses security vulnerabilities in personnel, technology, and operations for the duration of the system's life cycle. The idea behind this approach is to defend a system against any particular attack using several varying methods.

1. Awareness and training program – End users are top targets. Everyone in the organization must be aware of the threat of ransomware and how it is delivered. The training content may include
   - malvertisements, phishing emails
   - Never click on unverified links
   - Only download from trusted sites
   - Use a VPN when using public Wi-Fi
   - Do not Use unfamiliar USB devices
   - Avoid giving out personal data
2. Email scanning – Content scanning and email filtering should be used to detect threats before they reach end users.
3. Spam filters – These prevent phishing emails from reaching end users. Also, spam filters authenticate inbound emails using technologies such as Sender Policy Framework and DomainKeys Identified Mail.
4. Block ads – Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads can reduce that risk.
5. Whitelist applications - Add acceptable software to the whitelist and block unauthorized programs from running.
6. Firewalls – These software or hardware appliances control network traffic through access or denying policies or rules. These rules include denying listing or allowing listing IP addresses, MAC addresses, and ports. There are also application-specific firewalls, such as web application firewalls (WAFs) and secure email gateways, that focus on detecting malicious activity directed at a particular application.

7. Intrusion detection or prevention systems (IDS/IPS) – An IDS sends an alert when malicious network traffic is detected, whereas an IPS attempts to prevent and alert on identified malicious activity on the network or a user's workstation. These solutions are based on the recognition of attacks on signatures of known malicious network activity.
8. Endpoint detection and response (EDR) – This is software or agents that reside on the client system (e.g., a user's laptop or mobile phone) and provide antivirus protection, alert, detection, analysis, threat triage, and threat intelligence capabilities. These solutions run on rulesets (i.e., signatures or firewall rules) or heuristics (i.e., detection of anomalous or malicious behaviors).
9. Network segmentation – This is the practice of splitting a network into multiple subnetworks designed around business needs and technology requirements. This might include different sub-networks for executives, finance, operations, and human resources. Depending on the level of security required, these networks may not be able to communicate directly. Segmentation is often accomplished through the use of network switches or firewall rules.
10. Inspect east-west internal traffic – This provides anomaly detection of certificates when traffic is encrypted.
11. Inspect north-south traffic – This detects command and control (C&C) traffic by using threat intelligence to identify malicious IPs, domains, and more.
12. Scan network artifacts – This dynamically analyzes file behaviors for threats by using AI to detect malicious code.
13. Log aggregation – This collects logs from all critical devices, security controls, and endpoints in a central location for correlation and analysis.
14. The principle of least privilege – This requires policy and technical controls to only assign users, systems, and processes access to resources (networks, systems, and files) that are absolutely necessary to perform their assigned function.
15. Strong passwords – These are critical authentication mechanisms in information security. Modern password guidance involves using multifactor authentication for any account of value, using a phrase with multiple words, and not reusing passwords.

16. Patch management – This is the process of applying updates to an operating system, software, hardware, or plug-in. Often, these patches address identified vulnerabilities that could allow cyber threat actors unauthorized access to information systems or networks.
17. Back up data regularly – This verifies the integrity of backups and tests the restoration process to ensure it's working.
18. Secure your offline backups – This ensures backups are not permanently connected to the computers and networks they are backing up.
19. Conduct an annual penetration test and vulnerability assessment.

Recovering from a ransomware attack

Here are some of the steps our team believes that organizations can take to limit the scope of the attack and remove from it:

Step 1 - Isolate and shut down critical systems:

The first important step is to isolate and shut down business-critical systems. There is a chance the ransomware has not affected all accessible data and systems. If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.

If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.

After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

From the first evidence of ransomware on the network, containment should be a priority. Containment and isolation can include isolating systems from a network perspective or powering them down altogether.

Step 2 - Enact your business continuity plan:
The business continuity plan and its disaster recovery component are essential to maintaining some level of business operations.

The business continuity plan is a step-by-step playbook that helps all departments understand how the business operates in times of disaster or other business-altering scenarios. The disaster recovery component details how critical data and systems can be restored and brought back online.

Step 3 - Report the cyberattack:
Many businesses may hesitate to do so, but reporting the attack to customers, stakeholders, and law enforcement is essential. Law enforcement agencies can provide access to resources that may not be available otherwise.

You will also need to consider compliance regulations. The GDPR, for example, provides businesses with a 72-hour window to disclose a data breach involving customers' personal information.

Step 4 - Restore from backup:
The best protective measure you have for your data is backups. However, restoring large quantities of data can be time-consuming, forcing the business to be offline for an extended period of time.

Identify and prioritize critical systems for restoration and confirm the nature of data housed on impacted systems.

Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.

Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

This situation highlights the need to discover and contain ransomware infections as quickly as possible to reduce the amount of data that needs recovering.

Step 5 - Remediate, patch, and monitor:

In the final phase of recovering from a ransomware attack, companies remediate the ransomware infection, patch systems that may have led to the initial ransomware compromise, and monitor the environment closely for further malicious activity.

It is not unheard of for malicious activity to continue, even if the ransom is paid, or if infected systems were restored. If the same vulnerability exists that led to the initial attack, the environment can become compromised once again.

Contributors

Identify the team members and each individual's contribution to the paper:

Guorui Li: Top Risks (4), Common Ransomware Attack Vectors, General Best Practices

Xiaoyang Wei: Top Risks (4), What is ransomware, Common Ransomware Attack Vectors

Michael Huang: Four top risks, Executive summary, recovering from ransomware attack

Reference

“9 Tips to Prevent Ransomware Attacks.” Fortinet, https://www.fortinet.com/resources/cyberglossary/how-to-prevent-ransomware#:~:text=9%20Tips%20To%20Reduce%20Ransomware%20Risk%201%201.,Do%20Not%20Use%20Unfamiliar%20USB%20Devices%20...%20%E6%9B%B4%E5%A4%9A%E9%A1%B9%E7%9B%AE.

Madhan, Shwetha. “Ransomware Defense in Depth Strategy - Best Practices for Building a Strong Prevention: Vmware.” Carbon Black Tech Zone, https://carbonblack.vmware.com/resource/ransomware-defense-depth-strategy-best-practices-building-strong-prevention#section5.

ManageEngine, communications@manageengine.com. “Data Visibility and Security Solution by ManageEngine DataSecurity Plus.” ManageEngine DataSecurity Plus, https://www.manageengine.com/data-security/best-practices/8-best-practices-to-prevent-ransomware.html#:~:text=8%20best%20practices%20to%20prevent%20ransomware%201%20Back,privilege%20possible%20...%208%20Logically%20separate%20networks%20.

“Ransomware Guide.” CISA, https://www.cisa.gov/stopransomware/ransomware-guide.

Solutions, Vector. “Levels of a Risk Matrix.” *Vector Solutions*, 28 June 2022, https://www.vectorsolutions.com/resources/blogs/levels-of-a-risk-matrix/.

News Hacker. “5 Critical Steps to Recover from a Ransomware Attack.” *The Hacker News*, 31 Oct. 2021, https://thehackernews.com/2021/06/5-critical-steps-to-recovering-from.html.

Inc., Digital Defense. “Top 3 Attack Vectors Ransomware Exploit.” *Digital Defense*, 29 Nov. 2022, https://www.digitaldefense.com/blog/top-3-attack-vectors-ransomware-loves-to-exploit/.

Fruhlinger, Josh. “Ransomware Explained: How It Works and How to Remove It.” *CSO Online*, CSO, 19 June 2020, https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.