TABLE OF CONTENTS

Background

Wells Healthcare Hospitals (WHH) is a mid-sized private medical company where 200 medical staffs work. Due to the recent post-Covid-19 recession, the management department made a plan to reduce some management staff. Therefore, WHH brings all their payable invoices under the website and gives a 13% discount to patients hence patients pay their invoices online. Traffic between each patient and the WHH website is encrypted using SSL. As WHH management believes in the "prevention first" strategy, they spent money on an commercial firewall to protect the internal network. WHH has links to several medical suppliers whom they contact over the Internet via a VPN. WHH uses several connections such as cable modem connections, wired connections and wireless 802.11b connections to support remote clinic offices. Usually, during Christmas, the workers expected a hefty bonus but before Christmas in December 2019, WHH's finance department faced a cyber attack, they started collecting complaints instead of money. Also, the company's Apache HTTP 2.0 server was responding slowly and they lost their patient records and could not access some medical devices. In addition, they haven't fixed their bugs in the MySQL database server. In this situation, the company appointed an information security officer to investigate the attack. His report states that perhaps the attacker gained access to the system using social engineering, malicious code, or a locally privileged user. The attacker encrypted the medical devices, making the devices temporarily inaccessible. The Information Security Officer ended up the investigation with a preliminary analysis due to his medical reasons and handed it over to me before he left. So for the purpose of investigation I interviewed several employees and found several problems of these employees. For example, the receptionist spends time watching movies using the company's fast Internet connection, the finance department manager logs on to his workstation in front of his assistant. Moreover, the company faced some natural threats such as floods, earthquakes and fire attacks. Also, the staff is not properly trained.

Depending on the scenario, the report will explore all potential sources of threats and discuss notable threats. Likewise, it will find out the vulnerabilities of the company and discuss the types of vulnerabilities. Next, the report will determine the likelihood of risk and then determine a potential risk impact rating. After analyzing the potential threats, the report provides a recommendation plan and security countermeasures that should be taken against the threats to mitigate the potential risks.

Threats

Factors that have the potential to harm an organization are referred to as threats. According to the scenario some specific threats are discussed below:

Human-Caused Physical Threats (Insider threats): The potential for an insider to harm an organization through their authorized access or understanding of it is known as an insider threat. This harm can be caused by malicious, complacent, or unintentional actions that compromise the organization's integrity, confidentiality, and availability, as well as its personnel, facilities, or data. Customers and external stakeholders of DHS may find this broad definition more appropriate and adaptable for their organization.Insider threat is defined by the Cyber and Infrastructure Security Agency (CISA) as the threat that an insider will use their authorized access to harm the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems, whether they intend to or not.The following insider actions have the potential to cause harm to the Department as a result of this threat:

- Espionage
- Terrorism

- Unauthorized disclosure of information
- Corruption, including participation in transnational organized crime
- Sabotage
- Workplace violence
- Loss or degradation of departmental resources or capabilities, whether intentionally or unintentionally.

The threat posed by an insider can be unintentional or deliberate.

- **Unintentional Threat:**

Negligence: An organization is put at risk by a careless insider of this kind. Negligent insiders are generally familiar with security or IT policies but choose to ignore them, creating risk for the organization. Allowing someone to "piggyback" through a secure entrance point, misplacing or losing a portable storage device that contains sensitive information, and disregarding messages to install new security updates and patches are examples.

Accidental: This kind of insider mistakenly poses a risk to an organization that was not intended for it. Despite the best efforts of organizations, accidents still happen; They cannot be completely avoided, but they can be minimized when they do. Mistyping an email address and sending a confidential business document to a competitor, clicking on a hyperlink without realizing it, opening a virus-laden attachment in a phishing email, or improperly disposing of confidential documents are all examples.

- **Intentional Threats:** An intentional threat is one made with the intention of causing harm to an organization for personal gain or to address a personal grievance. It is common practice to use the terms "intentional insider" and "malicious insider" interchangeably.Motives include personal gain or harm to the organization. For instance, a lot of insiders are motivated to "get even" because they have not been recognized or met their expectations (for example:promotion, bonuses, and travel that you want) or even termination. Leaking sensitive information, harassing associates, sabotaging equipment, or committing violence are some of their actions.In the erroneous hope of advancing their careers, some people have snatched confidential information or intellectual property.

Social Engineering Attacks (Phishing): Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams typically trick unsuspecting users into giving access to restricted systems, exposing data, or spreading malware.Attacks can occur in person, online, or through other interactions.

Types of Social Engineering Attacks:

- Attacks by phishing: In an effort to persuade you to reveal personal information and other valuables, phishing attackers pose as reputable organizations or individuals. Attacks using phishing are targeted in many ways:
- Mass phishing, also known as spam phishing, is an attack that targets a large number of users. These attacks, which are not targeted by anyone, aim to nab any unsuspecting target.
- Spear phishing and, by extension, whaling target specific users with personalized information. Attacks by whalers specifically target high-value targets like celebrities, executives, and high-ranking government officials.
- The automated message systems that make voice phishing (vishing) phone calls may be recording all of your inputs. In some cases, a live person may speak to you in order to build trust and urgency.
- Text messages sent by mobile apps or SMS phishing (smishing) may include a link to a fake website or a prompt to contact the sender via a fake email or phone number.
- Email phishing is the most traditional means of phishing, using an email urging you to reply or followup by other means. It is possible to use web links, phone numbers, or malware attachments.

Network Security Threats (Ransomware): Ransomware is the most profitable type of malware

attack in history–and attacks will only get worse in the future, according to Cisco Systems' midyear report on the state of cyber security, released Tuesday. Employees must now be aware of the various stages of an attack and the best ways to avoid them. Ransomware was referred to as "weaponized encryption" by senior fellow James Scott, who was also a co-founder of the Institute for Critical Infrastructure Technology and co-authored the Institute for Critical Infrastructure Technology Ransomware Report in 2016."The method of attack is malware that is distributed via spear phishing emails, encrypts important data assets, and demands a ransom to be released.

Environmental Threats: It is unquestionably a threat to an organization if it does not adapt to changes in the environment. An organization may face different types of environmental threats:

Changing the environment: Numerous factors influence any organization's future growth; adopting climate change or another environmental change is one of them. There is unquestionably a threat to an organization if it does not adapt to changes in the environment.
Pollution: Numerous brand-new mills and manufacturing companies are beginning to produce goods and services for their clients. They gradually harm the natural environment by utilizing chemicals or raw materials. Water, air, and land are permanently polluted and wasted, posing an insurmountable environmental threat to individuals and organizations.
Mismanagement of waterways and land: For any business organization, these are the most crucial aspects. Additionally, the land is one of the four price factors that must be present for any company to begin operations. Organizations will face more threats if land and waterways are not managed properly and unplanned.
Weather extremes: Any area's population density was always important. Because less natural energy and other resources are used, a low population density may always be beneficial to an environment. The risk of harm to people's lives and property rises when there are more people living in vulnerable areas, and this holds true for businesses as well.
Natural disaster: Numerous nations are confronted with a variety of natural disasters as a result of climate shifts. Sometimes, they are extremely disastrous for a country. A natural disaster can be beneficial to some organizations, but only for a short time. The organization can deal with floods, cyclones, and other natural disasters.
According to the scenario, we have got two types of environmental threats (flood and earthquake). Numerous environmental threats to data centers, other information processing facilities, and their staff originate from natural disasters.

- Matrix

Threat Source	Threat Statement
Human-Caused Physical Threats (Insider threats)	Instead of money, WHH began collecting complaints. Angry doctors reported missing and denying access to the patient's records, they can't even to carrying on with normal operations due to inaccessible some medical devices.
Social Engineering Attacks (Phishing)	His report concluded that most likely the attacker got access into the system using social engineering and user interaction to put in the malicious code or using local privileged user.
Network Security Threats (Ransomware)	The attacker managed to encrypt a number of medical devices within the hospital rendering them temporarily inaccessible. He replaced all the current web-apps including those in server/web applications, then installed a web app that included an XML parser which was stored in the web application library.
Environmental Threats	Each winter due to heavy rains, the river down the

(Flood)	road comes dangerously close to overflowing and flooding the nearby neighbourhood, including the company.
Environmental Threats (Earthquake)	Last year, a mild earthquake rattled the main campus and fortunately, no damage was reported to the structure or foundations. Earthquakes in this area occur approximately once every other year.

Vulnerabilities

A security vulnerability is a flaw in a system's design, implementation, operation, or management that can be used by an attacker to violate the security policy of the system. Notes, bugs, glitches, or exploits are frequently used to document security vulnerabilities.

When Facebook (Meta) was hacked and millions of people's data were leaked online, this is a good example.The hacker was able to send targeted advertisements to people based on what they liked on Facebook.

Types of Security Vulnerabilities: The following are some of the most common types of security vulnerabilities:

Software vulnerabilities
Typically, software vulnerabilities are discovered in the software's coding or design. These might make it possible for intruders to gain remote control of computers, carry out unauthorized activities, or gain access to sensitive data like credit card numbers and passwords.

Hardware vulnerabilities
Typically, hardware vulnerabilities are design flaws that enable adversaries to circumvent security measures and gain access to sensitive resources or data on mobile devices like laptops and smartphones.

Network vulnerabilities
The weaknesses in network protocols that make it possible for an attacker to eavesdrop on email conversations or intercept data as it is being sent over the internet are examples of network vulnerabilities.

The identified vulnerabilities in the above scenario is mentioned in the following matrix:

- Matrix

vulnerability	vulnerabilities Statement
Perhaps the terminated employee's ID has not been removed from the system.	WHH management decided to reduce the number of managerial staff.
Using internet via VPNs decrease the internet speed.	WHH links to several smaller partners that supply medical supplies. These partners contact through the internet via VPNs.
Use of cable modem connection making a computer more vulnerable to hackers.	WHH also supports several remote clinics offices that rely on cable modems for connectivity.
Unfixed bugs is a big chance for hacker to hack the server.	They did not relish the thought of looking for bugs in the MySQL database server, which also ran on the same platform as the Web server.

Careless/Uninformed Employees (Malware may be installed while downloading movies).	Clare, the receptionist takes advantage of the company's fast Internet connection by movies from time to time.
The Assistant may steal and change the data and sell it for financial gain as he can access client records and reply to emails on behalf of Adam.	Adam, the Finance department manager, often leaves his workstation logged on so his assistant can enter data and reply to some emails on his behalf, and access client records.
Improper maintenance of fire fighting equipment.	A small fire occurred 3 years ago in the patient waiting area that triggered the water sprinkler system. The fire was extinguished, however water from the sprinkler system damaged furniture and computer equipment. Building records show 4 fires have occurred in the past 20 years.
Lack of security training to staff.	The last training conducted for the staff was 6 years ago and the staff manuals and orientation materials are updated once every three years.

Likelihood

Risk	Likelihood Rating (High, Medium, or Low)
Unauthorized disclosure of sensitive business information due to inability to remove terminated employee IDs from the system.	High
Using internet via VPNs decrease the internet speed.	Low
Use of cable modem connection making a computer more vulnerable to hackers.	High
Due to unfixed bugs, hackers may easily hack the server.	High
Careless employees may install Malware while downloading.	Medium
Insider may change the data.	High
Fires occurred due to improper maintenance of fire fighting equipment and damaged furniture and computer equipment.	Low
Lack of security training to staff.	High

Impact Rating

Risk	Impact Rating (High, Medium, or Low)

Risk of access by staff	High
Risk of slow speed due to VPN usage	Low
Risk of attack by hacker	High
Risk of attack by hacker	High
Risk of encrypted files and devices	High
Risk of change of content	Medium
Risk of temporary loss	Low
Risk of lack knowledge of staff	High

Recommendation

Recommended plans and security countermeasures for the following threats are discussed:

1. Human-Caused Physical Threats (Insider threats)
2. Social Engineering Attacks (Phishing)
3. Network Security Threats (Ransomware)
4. Environmental Threats

Human-Caused Physical Threats (Insider threats):

Some ways to prevent Insider Threats:

- **Security Policy:** A comprehensive security policy ought to at the very least include provisions for the prevention of security threats. Include procedures in your security policy to prevent and detect misuse as one of the best ways to prevent insider threats. Additionally, your policy ought to include guidelines for investigating insider misuse. Additionally, ensure that your security policy outlines any potential negative effects of misuse.
- **Physical Security:** Keeping employees away from your critical infrastructure physically is one of the best ways to prevent insider theft. Companies can greatly reduce insider threats by providing employees with a safe place to store sensitive information and isolating high-value systems that require restricted, verified access. Biometric or two-factor authentication systems can also be used to make sure that employees are not using the keys of other employees.
- **Screen New Hires:** A few organizations might consider historical verification to be excessively tedious or costly. However, background checks can save your business a lot of trouble and prevent theft in the future and only cost between $50 and $200.When conducting a background check on a new hire, it is also beneficial to use advanced systems that can verify the entire story. A lot of background checks won't tell you if your new hire lives with a known con artist or an ex-employee who is angry. Use a service like NORA, or non-obvious relationship awareness, to learn more about who has access to your confidential company data.
- **Use Multi-factor Authentication:** Many employees use weak passwords to access data and password-cracking technology has gotten very advanced, making it much easier than ever to break into an employee's computer and access sensitive information. Try implementing strong, multi-factor authentication measures to extremely sensitive applications within your company. This will make it much more difficult for an unauthorized user to access sensitive data.
- **Secure Desktops:** There are a few different services that your company can use to lock down all of its desktops.Because your employees aren't as accountable as they should be for all of their configurations, these services are very helpful.You will also be able to lock down particular components of an employee's computer apps using these services to assist you in further preventing threats.

- **Segment LANs:** It can be very difficult to find the many choke points inside LANs so instead, segment LANs with firewalls which will create a zone of trust at all points that each LAN connects with the corporate LAN.
- **Seal Information Leaks:** There are numerous ways that information can leak out of your business. Check your security policy to see what information cannot be shared. Software that scans your policy and notifies you when employees violate it on your network is another option. Additionally, there is software available that can examine the text of incoming emails to ensure that your employees are not disclosing confidential information.
- **Investigate Unusual Activities:** A lot of the time, when an employee betrays a company's trust, the majority of businesses are too busy looking for outside threats to notice. As a result, you should conduct an investigation whenever you notice unusual activity on your company's LAN. But keep in mind that there are laws in place to keep an eye on things, so before you break any of them, learn about them.
- **Implement Perimeter Tools & Strategies:** Why wouldn't you protect your internal server in the same way? Implementing perimeter strategies and tools for servers on the public internet would never make sense. Make sure you fix email and web servers and get rid of any unused applications. Also, try locking down configurations to enhance your security protocol.
- **Monitor Misuse:** Direct employee monitoring is an additional useful instrument. You can never be too careful with the private information that belongs to your business, whether you use keystroke logging or security cameras.

You will increase the security of the sensitive information that belongs to your business by putting these insider threat detection methods into practice. A comprehensive security policy will also explain to employees why it is necessary to keep company information secure and any legal consequences that will come from any violation of this policy. If your company has yet to implement a security policy that covers inside and outside threats, your employees could be violating your trust and stealing highly sensitive information that could cost your company hundreds of thousands of dollars.

Social Engineering Attacks: First, determine where social engineering attacks come from, such as "for emotions raised." Did any illegitimate messages come from the sender? Is there something odd about the website I'm on? Suspicious attachments or links? etc. Then, safeguard the following routines to avoid social engineering attacks:

Safe Communication and Account Management Habits:
- Never click on links in any emails or messages
- Use multi-factor authentication. Online accounts are much safer when using more than just a password to protect them
- Use strong passwords (and a password manager)
- Avoid sharing names of your schools, pets, place of birth, or other personal details
- Be very cautious of building online-only friendships

Safe Network Use Habits:
- Never let strangers connect to your primary Wi-Fi network
- Use a VPN
- Keep all network-connected devices and services secure

Safe Device Use Habits:
- Use comprehensive internet security software

- Don’t ever leave your devices unsecured in public
- Keep all your software updated as soon as available
- Check for known data breaches of your online accounts

Network Security Threats (Ransomware):

Attack Mitigation:

According to Scott, businesses ought to employ an information security team to train employees and identify and patch system flaws.

Scott stated, "The human element is the weakest."Employees can avoid common user mistakes like sharing flash drives between work and non-work machines, clicking on a malicious link, checking social media on a work computer and company email on a home computer, and so on with the assistance of the training.

Because some attacks may originate within the company, Scott also suggested conducting ongoing penetration tests and utilizing behavioral analytics to detect usage anomalies.

Scott stated, "It comes down to cyber hygiene and a layered defense."There is no one-size-fits-all solution. The following five measures of protection against ransomware were suggested by Ryan Sommers, manager of threat intelligence and incident response at LogRhythm Labs:

1. Preparation: Adopt a proactive patching strategy to limit access routes and eliminate vulnerabilities. Tools that automatically detect and respond to infections can safeguard endpoints.
2. Detection: Use dangerous knowledge sources to impede or if nothing else alert you to the presence of oddities in your organization's traffic. Look for malicious links in emails.
3. Containment: If you're infected, make sure you have an endpoint security system that can stop the process and detect it. To prevent additional encrypted files, block and isolate the local host from the network.
4. Eradication: Replace the ransomware-infected machines. The malicious message can be removed by cleaning network locations like file shares or mailboxes. If you decided to clean instead of replace, keep an eye on things to stop the same attack from happening again.
5. Recovery: Restore from a backup if you have one. Investigate what specific infection vector was used against the system, and how to protect it next time.

Environmental Threats: An organization may face environmental risk factor. It could create barriers for the operation of that organization.

Risk to the Environment, as Defined: the likelihood of experiencing a negative outcome, as well as the potential for flooding, cyclones, tornadoes, and other natural disasters to have a negative impact on business operations and the surrounding environment. resulting from the activities of groups.

Environmental Risk Assessment for Business: Risk assessment is simply the process of knowing the probability of happening a specific event and these events consequences. Environment uncertainty process has four steps.

1. Identifying the hazard or hazards,
2. Assessing the consequences,
3. Finding out the possibilities of happening these events, and
4. Categorizing the risk and uncertainty.

To protect a company from the negative effects of environmental issues, it is important to know what kind of risk is present. Recognizing the gamble will immensely diminish the likelihood of expected harm. The area of damage can then be better understood with the help of the consequence's measurement. The probability calculation will then assist you in determining the likelihood that the incident will occur.

Lastly, putting the total risks in order will help you decide which action to take to protect your business.

Other Criteria

To reduce ransomware infections, the organizations also can follow a comprehensive list of recommendations, though not exhaustive, to reduce the risk posed by ransomware infections:

Data Protection:

- Schedule data backups frequently and ensure that they are offline and stored in a separate, secure location. For redundancy, think about keeping multiple backups in different places. Regularly test your backups.
- If an online backup and recovery service is used, contact the service immediately after a ransomware infection is suspected to prevent the malware from overwriting previous file versions with the newly encrypted versions.
- Encrypt network data - particularly any sensitive and/or protected data - at rest and in transit to prevent an unauthorized threat actor from ex-filtrating data off the network and releasing it publicly.

System Management:

- Schedule scans as frequently as permitted and make sure your antivirus software is up to date with the most recent definitions.
- Enable automated patching for operating systems, software, plugins, and web browsers.
- To prevent unauthorized changes to user privileges, adhere to the Principle of Least Privilege for all user accounts and enable User Access Control (UAC).
- Implement application whitelisting to prevent unauthorized or malicious software from executing.
- Turn off unused wireless connections.
- Use ad blocking extensions in browsers to prevent “drive-by” infections from ads containing malicious code.
- Disable Windows Script Host and Windows PowerShell.
- Disable Remote Desktop Protocol (RDP), Telnet, and SSH connections on systems and servers if it is not needed in your environment. Block inbound traffic to associated ports.
- Audit access, ensure that login credentials are complex, and implement a 2FA solution to prevent unauthorized access if remote access is required.
- Use the web and email protection to block access to malicious websites and scan all emails, attachments, and downloads and configure email servers to proactively block emails containing suspicious attachments such as .exe, .vbs, and .scr.
- Use a behavior blocker to stop ransomware from running or modifying systems or files without permission.
- Consider utilizing a free or commercially available anti-ransomware tool by leading computer security vendors.

Network Management:

- Ensure your firewall is enabled and properly configured.
- Close and monitor unused ports.
- Require multi-factor authentication (MFA) for all user accounts, particularly those with elevated privileges.
- Monitor for unusual/suspicious outbound data transfers that could indicate the ex-filtration of data that may precede a ransomware infection.
- Prior to infection, establish a baseline for the performance of the network for network monitoring.

This will make it simpler to look for anomalies and malicious activity after the infection.

- If ransomware or other network intrusion leads to a criminal investigation, keep network log files for a full year.

Mobile Device Management:

- For Android devices: disable the “unknown sources” option in the Android security settings menu, only install apps from the official Google Play store, and avoid "rooting" the device.

Appendix

References

1. ANDRIOAIE, A., 2022. *HEIMDAL SECURITY.* [Online]
   Available at: https://heimdalsecurity.com/blog/what-is-vulnerability-risk-management/
   [Accessed 27 November 2022].

2. 2. Anon., n.d. *CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY.* [Online]
   Available at: https://www.cisa.gov/defining-insider-threats
   [Accessed 27 November 2022].

3. Haque, F., 2022. *The Strategy Watch.* [Online]
   Available at: https://www.thestrategywatch.com/environmental-risks-assessment/
   [Accessed 27 November 2022].

4. Pribanic, E., 2020. *TechFunnel.* [Online]
   Available at: https://www.techfunnel.com/information-technology/10-ways-to-prevent-insider-threats/
   [Accessed 27 November 2022].

5. Rayome, A. D., 2016. *Infographic: The 5 phases of a ransomware attack.* [Online]
   Available at: https://www.techrepublic.com/article/infographic-the-5-phases-of-a-ransomware-attack/
   [Accessed 27 November 2022].

6. Schwarzkopf Dr, E. T., 2021. *NJCCIC.* [Online]
   Available at: https://www.cyber.nj.gov/mitigation-guides/ransomware-risk-mitigation-strategies
   [Accessed 27 November 2022].

7. ZUOGUANG WANG, L. S. A. H. Z., 2020. Defining Social Engineering in Cybersecurity. *IEEE Access,* Volume 8.