Table of Contents

Section 1 – Risk Assessment

Risk Assessment Tool: Opensource GitHub risk assessment matrix by neviarrawlinson

We identified our top 5 risks based on the current 455Cyber CO system and used the tool to generate the risk Heatmap.

Risk 1: The current company implements BYOD (Bring Your Own Device) policy where each staff member has a laptop running Microsoft Windows configured by themselves. This could lead to insecure configuration on the client device (Unpatched OS, no anti-virus software, outdated and unsupported third-party application) that can introduce vulnerability to the company system if the device is connected to the company network.

CWE-16, CWE-284, and CWE-732.

Impact Score -> 5: The insecure device increases the attack surface and puts the whole company at risk of a successful Cyberattack. Since the company network system is already flat and insecure, a single compromise from an end device can wreak havoc.

Likelihood -> 5: The interviews with some of the team staff already informed that most of them do not have a good personal Cybersecurity practice, so it is good to assume the laptop that they're using is not properly configured securely.

Total score: 25

Mitigation: Abolish BYOD policy and start implementing COPE policy with RBAC and NAC. COPE will enable the company IT ownership of the client device to enforce proper configuration on the devices NAC will enforce policies for the devices to check for whether the device is in compliance before allowing the device access to the company network. RBAC authorized and granted enough access based on the access policies tied to the device's user role. Implementing Windows BitLocker for FDE and Defender for EDR.

Risk 2: The company network has already proven to be unprotected by the Red Team. This leads to an assumption that the network architecture is not segmented and enforces continuous monitoring for any internal device, potential escalated privilege attack, and lateral movement if a network endpoint is compromised.

CWE-419 and CWE-923

Impact Score -> 5: An unprotected and unsegmented network facilitates a rapid spread of Cyberattack throughout the whole system if the attack was successfully breached via one entry-point.

Likelihood -> 3: Strangely, even though this company system overall is very poor in Cybersecurity standard, giving a testimony of VP of Finance & Accounting Susan Butler that the company has

never been hacked before and she is the longest staff with the company. Therefore, the likelihood of this risk would be medium, but still its impact will be catastrophic.

Total Score: 15

Mitigation: Implement Zero-Trust architecture and VLAN segmentation between different network services.

Risk 3: Company used MS-Assess as their database, which is insecure according to enterprise standards. The same credential is shared across multiple users, and the credential is weak and can be cracked easily, which is a very bad security practice. The IT Manager attempted to leak the credential to the public, which indicates the credential is already compromised, and the attacker can now use it to assess the important database.

CWE-200, CWE-521, CWE-798

Impact Score -> 5: Since the database is not secure and holds all the important files and revenue data, the effect of credential compromise and weak credential will allow attackers to breach and leak or encrypt those data for a ransom that would affect the company revenue and reputation.

Likelihood Score -> 5: Since there is a potential credential compromise, the likelihood of this risk is nearby.

Total Score: 25

Mitigation: Since the company system is heavily Microsoft products, suggestions immediately migrate to Microsoft SQL Server (Azure SQL database) to move the most priority data first and use integrated windows authentication. Ensure a strict password policy is enforced and prohibit the same credentials being used across accounts.

Risk 4: Using third party firms for hosting the accounting systems increases the attack surface. The third-party firm could be vulnerable.

CWE-1104, CWE-1395

Impact Score -> 2: Since the CEO considers the accounting system by the third-party firm is secure, we can assume the CEO testimony to be valid.

Likelihood Score -> 2: If the third-party firm is trusted, then the likelihood of the risk associated with the firm is low.

Total Score: 4

Monitor: Even though the CEO trusts the third-party firm's security, we still need to add the firm to our asset list using a Third-party risk management platform (TPRM). Third party firms must provide SOC 2 Type II report and ISO 27001 to prove their Cybersecurity hygiene and practice.

Risk 5: Vulnerable File Server and unencrypted data storage on client laptop.

CWE-312, CWE-316, CWE-922, CWE-1329

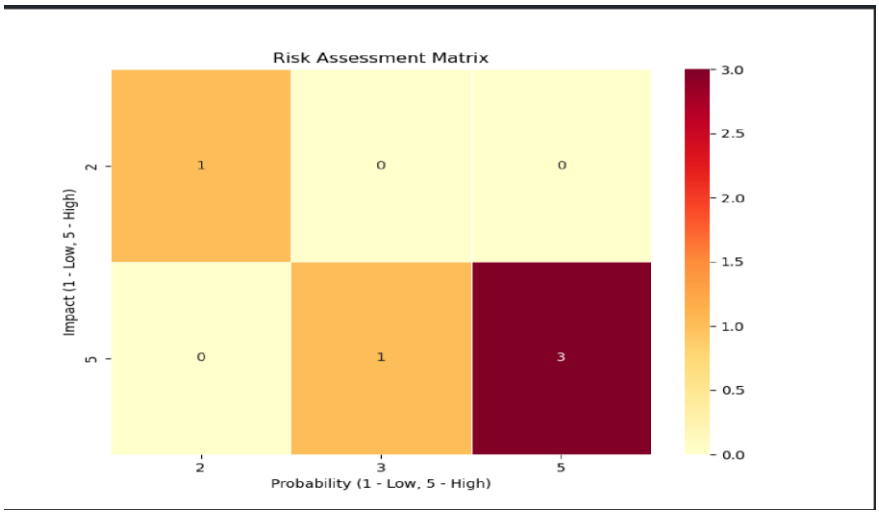
Impact - 5: The current file server approaching its EOL and decommission stage suggested that the server already has unknown vulnerabilities that can cause a zero-day attack and information leak. The encrypted data storage on the client laptop could be exposed if stolen.

Likelihood - 5: The chance for an attack on a vulnerable file server should be considered reasonably high and assume the staff could get their laptop stolen at any given moment.

Total Score: 25

Mitigation: The CEO given RPO is a day of data loss, so configure back up daily to meet the RPO. The RTO is 7 days, so a Cold storage would be necessary to restore the translation data in a week. Immediately move all the files to Microsoft Azure for the file server. For client laptops, ensure FDE and remote wipe are fully active in case the laptop gets stolen; the data can be deleted.

The final heatmap is as followed



Section 2 - Requirements

The requirements in the table below were created based on the analysis of the current system. Overall, 24 requirements were recommended to make certain that the systems and the network of 445CyberCo remain secure. A requirements statement was written and a proposed solution.

Requirement No	Requirement Statement	Proposed Solution
1	A centralized configuration and policy management system to manage the devices, and policies remotely	Using Active Directory domain services to enforce policies and configure devices centrally
2	Enforce a strong password policy to prevent unauthorized access and lead to data breaches and network compromise	By using the Active directory domain services, enforce strong password policies for all devices without having to configure it on each device individually
3	Implement a cloud-based endpoint management tool to manage endpoint devices	Implement Microsoft Intune manage endpoint devices in this organization

4	Configure regular backups to recover data in case of data loss	Use the proposed Active Directory domain controller proposed earlier to configure the windows devices to regularly backup their data to meet the CEO's RPO and RTO
5	Configuring remote wipe for devices in case the device is stolen to prevent data being compromised	Use Microsoft Intune software to configure remote wipe for endpoint devices being used.
6	Enforcing Patch management to patch vulnerabilities	Implement regular updates to ensure that devices get patched against the latest vulnerabilities
7	Prevent Remote shell access	Disable SSH port 22 for regular users, only enabled it for administrators
8	Implement the Principle of Least privilege to ensure that employees do not have access to more than they need to get their job done	Give each access to only the privileges necessary for them to complete their tasks and nothing more.
9	Network segmentation to ensure that if one device in the network gets	Segment the network into different sections such as a section for accounting

	hacked, only 1 section gets compromised rather than the entire enterprise network	and another section for finance. That way, if the finance network is compromised, the accounting remains safe. This can be done by using VLAN segmentation
10	Implement a Role-Based-Access-Control	Use RBAC to define roles for employees based on their responsibilities and user roles
11	Implement corporate owned personally enabled (COPE) by using RBAC and remove BYOD	Give employees corporate-owned devices and allow them to use the devices. Then use RBAC to define roles for employees based on their responsibilities/user roles and remove the BYOD policy
12	Implement a secure SQL database to ensure database security and resilience and replace it with the less secure MS-Access database	Replace the insecure MS-Access with Microsoft SQL server (Azure SQL database)

13	Implement Full Disk Encryption on devices by using a centralized system	Enabled BitLocker on devices by using the Active directory domain services to ensure that full disk encryption is enforced on these devices to ensure that the devices data remains secure
14	Change file server to a cloud service provider to ensure more security and resilience	Switch to Microsoft Azure for the file server which is known as **Azure files** by using storage migration service
15	Implementing an enterprise anti-virus system to protect the devices against viruses and malware	Implement the Microsoft Defender for business as the network is windows heavy, and this option is more cost effective. Includes AI-powered device protection
16	Due to the proposed system using Azure files in the cloud, it is recommended to implement a cloud-based anti-virus software.	Implement the Microsoft Defender for Cloud to protect assets that are implemented in the cloud.
17	Implement: Identify, protect, detect, respond, recover	By enforcing these, it can be ensured that “the five primary pillars for a successful and holistic cybersecurity

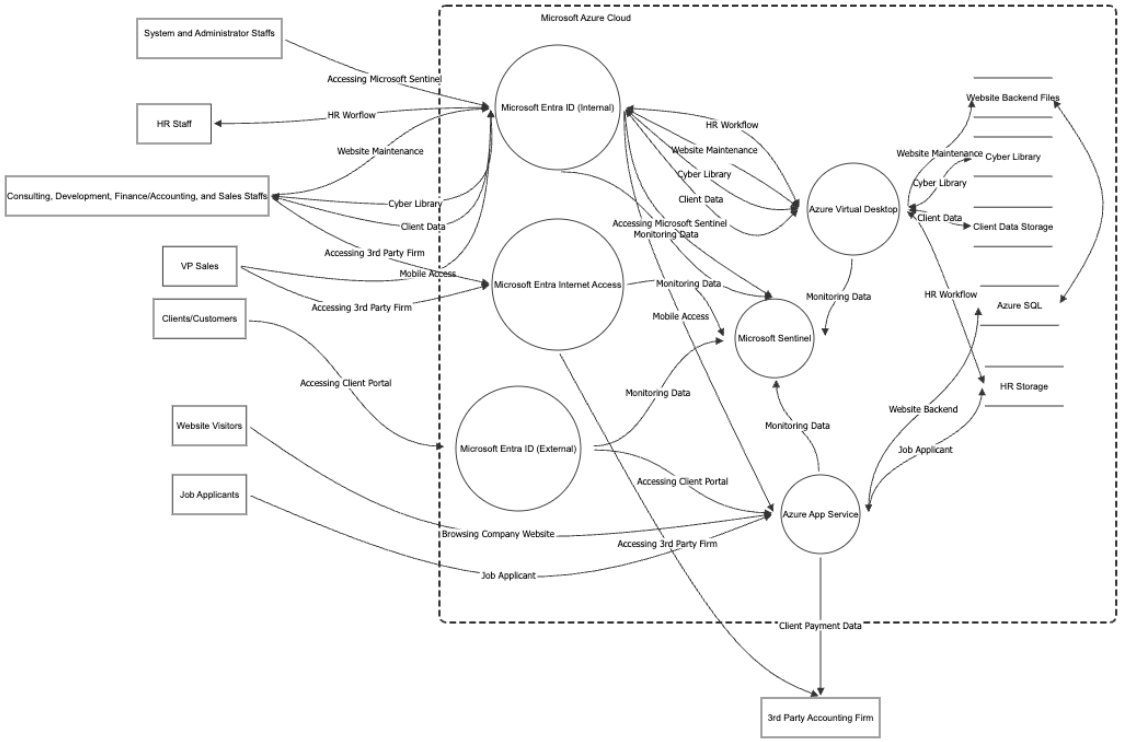
		program" are being utilized to ensure secure systems and networks
18	Implement cybersecurity user training every 6 months to ensure users stay up to date with current threats	The Cyber security professionals at the organization should prepare cybersecurity training for their users every 6 months
19	To ensure improvements for the company's web presence, a cloud platform needs to be utilized to allow "a shared calendar for scheduling client events, a staff-only project management portal that can contain contracts, deliverables, schedules, etc., as well as a client-facing ability to accept credit card payments."	Microsoft 365 enterprises can be implemented to achieve these objectives as it includes apps that can assist with these. A shared calendar for scheduling client events can be implemented with an outlook on the calendar. Microsoft planner for a project management portal. Dynamic Point is essential for accepting credit card payments as it allows the admin to embed popular payment services to it
20	Implementing a DLP (data loss prevention) is crucial in protecting confidential information by ensuring	For the 445Cyber, it would be useful to implement the Microsoft Purview data security capabilities which has a DLP

	that a user does not either accidentally or deliberately expose confidential information	capability to protect against confidential data exposure
21	Implement a Network Access Control (NAC) to deny access to noncompliant devices that do not meet the security standards of the network and place such devices in a quarantined area.	Implement the Cisco NAC in the network to ensure reliable security against noncompliant devices. This is useful as there are customers in this organization that need to access the guest network.
22	Implement a disaster recovery plan to allow the organization to resume normal operations	Design a Disaster recovery plan and outline the response to an incident and plans in place to return the business to normal operations
23	Implement a SIEM (secure information and event management) tool to help with log management, even collection, as well as Incident response and monitoring as well as a SOAR (Security Orchestration, Automation, and Response)	Microsoft Sentinel should be used for this purpose as it includes both a SIEM and a SOAR.

24	Write a secure coding policy by considering secure coding as well as best coding practices	Design a secure coding policy adhering to the OWASP Secure Coding Practices Quick Reference Guide as this guide provides useful information to allow the developers of 445Cyber to have a guideline to follow

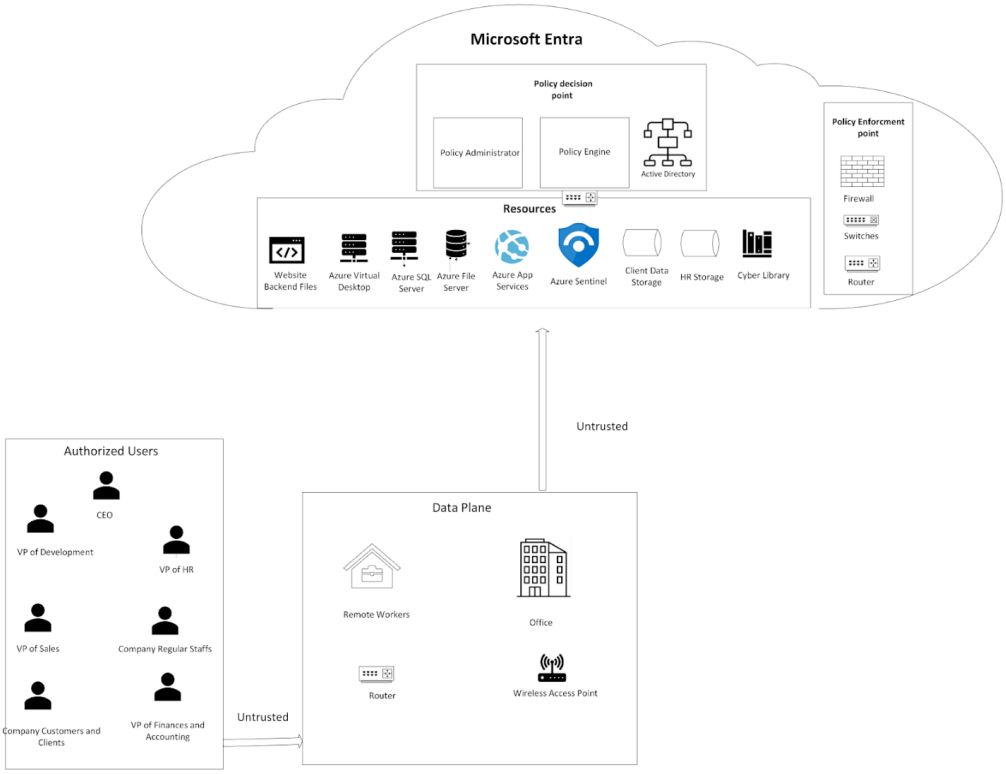
Section 3 – System and network design

Here we have the data flow diagram for our proposed cloud-based system.



Since the company already utilized a lot of Windows native systems, we have proposed a complete cloud-based solution for the company's new System and Network Design. We implement Microsoft Entra ID as the major cloud service that met the requirement of implementing Zero Trust Architecture, Identity and Access Management, and Active Directory service for proper authentication and RBAC authorization to ensure specific resources only be granted to specific user entities. All company internal staff MUST go through Microsoft Extra ID in order to access their given resources for work. The staff can access their resources either on a laptop or mobile device. The admin can configure Microsoft Extra ID with proper Policy configurations like OS health check, anti-virus software up-to-date, secure password policy and MFA to securely allow the staff to access the company resources on Azure Cloud. The consulting, development, finance/accounting, and sales staff's work is being done on Azure Virtual Desktop. This would resolve the issue of stolen laptops, since the work data is preserved on the cloud. The system staff can simply disable the account associated with the lost laptop on Microsoft Entra ID to prevent data compromise and issue a new company laptop with a new account set up for replacement. Data storage for Website Backend, Cyber Library Tools, Client Data, and HR is segmented to prevent file cross-contamination problems. Azure file storage offered dynamic options to set up policies like strict access control for sensitive files like the client and HR data, Operational Backup to meet the CEO RPO and RTO criteria and Vaulted Backup for long term protection of data that more resistant to ransomware attack as the vaulted backup will be stored on another file server. We used Azure App Service to securely host our company website, and we specified that our client/customers MUST go through Microsoft Extra ID (External) with the client account that we set up to securely visit their client portal on our website. Other website visitors or job applicants can access our website anonymously, but their access policy can be configured to be more

restrictive. Job Applicant sensitive data will be properly encrypted and stored in a highly protected HR File Storage. To enable secure remote access to the third-party accounting firm by the VP Sales and Finance/Accounting staff, it must be done via Microsoft Entra Internet Access which provides a Secure Web Gateway to connect with the third-party service. The client payment data also will be routed to the third-party firm for invoice and billing. Finally, all activities done by the company or website visitors are being monitored and centralized into Microsoft Sentinel Cloud-Native SIEM platform for our system admin staff to keep watch for any alert of unusual activity.



Microsoft Entra ID is a cloud based Zero trust architecture network. In the diagram above, we have all the entities from the company staff and the company clients as authorized users trying to access the company resources through Microsoft Entra ID. Even though they are authorized, they still need to be properly authenticated and authorized for proof of concept to be given only enough

privilege access to resources based on the configured Active Directory and PDP in the Microsoft Entra ID.

Section 4 – Threat Modeling

OWASP STRIDE Threat Model

Spoofing

- An attacker can pretend to be a trusted system and be allowed access
- An attacker can send phishing email pretending to be the CEO and thus gain access to the resources
- An attacker can hijack a user's sessions and pretend to be them and bypass Microsoft Entra ID

Tampering

- The attacker can view the information being sent from authorized users to the wireless access point by pretending to be the wireless access point
- Gaining access to the file servers and viewing confidential information regarding the customers of 445 CyberCo.
- An attacker intercepting traffic and then modifying information and acting as man in the middle thus conducting a man in the middle attack

Repudiation

- The attacker deletes important files by using an authorized user's account, thus violating non-repudiation
- The attacker does something malicious, delete all the logs and it cannot be proved they did it

Information disclosure

- The attacker gaining access to the Microsoft Entra system and exposing sensitive/confidential information in the dark web
- A disgruntled authorized user downloading confidential information to bypass DLP and then exposing that information
- An authorized user accidentally exposing confidential information due to a misconfiguration in the DLP system

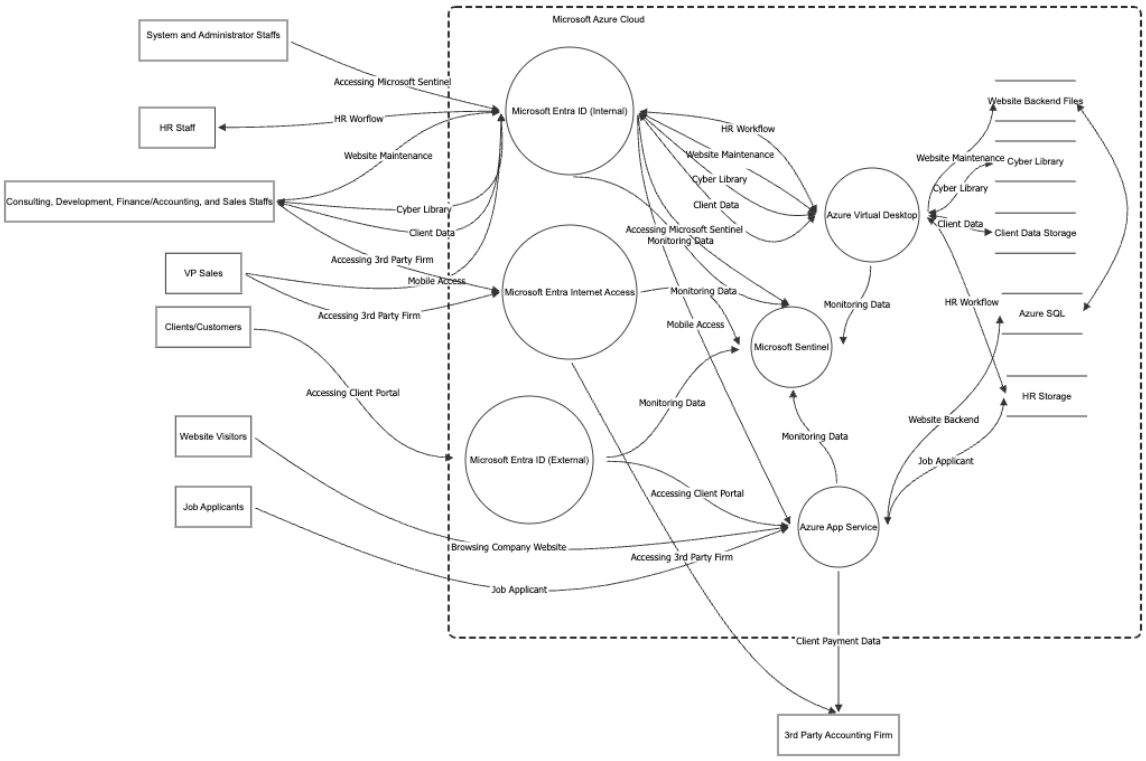
Denial of Service

- An attacker using a botnet to send so many requests to the server, causing it to be unavailable
- An AI bot sending so many requests to a server and making it unavailable
- An attacker cutting power to the company, making the servers unavailable

Elevation of Privilege

- An attacker using the account of a legitimate user with limited privileges and using a vulnerability elevates the privileges and gets access to admin tools
- An attacker gains access to the admin account

- An attacker gains access to a low privilege account and with a vulnerability creates an admin account for themselves



Azure SQL (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
2	SQL Injection	Information disclosure	Critical	N/A		Attacker can inject malicious SQL query from the company website frontend to cause a disclosure of sensitive data.	Enable Microsoft Defender for SQL to provide advance SQL attack protection on the SQL database.
3	SQL Injection	Tampering	Critical	N/A		Attacker can inject malicious SQL qeries that cause a deletion of data	Enable Microsoft Defender for SQL to provide advance SQL attack protection on the SQL database.

Client Data Storage (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
8	Disgruntle Employee	Information disclosure	High	N/A		A disgruntle employee or insider threat could download sensitive client information to disclose it to public	Azure File Storage has a DLP feature to prevent data with high sensitive label from being exfiltrated without proper permission.

Azure App Service (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
7	Malicious Macro File Upload	Elevation of privilege	Critical	N/A		Attacker can upload malicious macro disguised as resume that cause the HR staff to open and potential escalation of privilegde by stealing the HR staff credential.	Implementing Azure Web Application Firewall with content scanning with Microsoft Defender

Browsing Company Website (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
6	Botnet Attack	Denial of service	High	N/A		An attacker could used botnet to overwhelmed the website with requests and causing disruption in site availability.	Implementing Azure Web Application Firewall with DDoS protection and enforce rate limit policy.

Job Applicant (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
5	Botnet Attack	Denial of service	High	N/A		An attacker could used botnet to overwhelmed the website with requests and causing disruption in site availability.	Implementing Azure Web Application Firewall with DDoS protection and enforce rate limit policy.

CAPEC

All the official descriptions here are from the official CAPEC MITRE

CAPEC-98: Phishing

There is a possibility that attackers target the employees of the 445 CyberCo with phishing attack.

Official description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business to prompt the user to reveal some confidential information (very frequently authentication credentials) that can later be used by an attacker. Phishing is essentially a form of information gathering or "fishing" for information.

CAPEC-173: Action Spoofing

Official Description: “An adversary can disguise one action for another and therefore trick a user into initiating one type of action when they intend to initiate a different action. For example, a user might be led to believe that clicking a button will submit a query, but in fact it downloads software. Adversaries may perform this attack through social means, such as by simply convincing a victim to perform the action or relying on a user's natural inclination to do so, or through technical means, such as a clickjacking attack where a user sees one interface but is actually interacting with a second, invisible, interface.”

CAPEC-123: Buffer Manipulation

Official Description: “An adversary manipulates an application interaction with a buffer to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer

space itself that is the target of the attack rather than any code responsible for interpreting the content of the buffer. In virtually all buffer attacks, the content that is placed in the buffer is immaterial. Instead, most buffer attacks involve retrieving or providing more input than can be stored in the allocated buffer, resulting in the reading or overwriting of other unintended program memory."

CAPEC-165: File Manipulation

Official Description: "An attacker modifies file contents or attributes (such as extensions or names) of files in a manner to cause incorrect processing by an application. Attackers use this class of attacks to cause applications to enter unstable states, overwrite or expose sensitive information, and even execute arbitrary code with the application's privileges. This class of attacks differs from attacks on configuration information (even if file-based) in that file manipulation causes the file processing to result in non-standard behaviors, such as buffer overflows or use of the incorrect interpreter. Configuration attacks rely on the application to interpreting files correctly in order to insert harmful configuration information. Likewise, resource location attacks rely on controlling an application's ability to locate files, whereas File Manipulation attacks do not require the application to look in a non-default location, although the two classes of attacks are often combined."

CAPEC-268: Audit Log Manipulation

Official Description: "The attacker injects, manipulates, deletes, or forges malicious log entries into the log file, in an attempt to mislead an audit of the log file or cover tracks of an attack. Due

to either insufficient access controls of the log files or the logging mechanism, the attacker is able to perform such actions."

CAPEC-81: Web Server Logs Tampering

Official Description: "Web Logs Tampering attacks involve an attacker injecting, deleting or otherwise tampering with the contents of web logs typically for the purposes of masking other malicious behavior. Additionally, writing malicious data to log files may target jobs, filters, reports, and other agents that process the logs in an asynchronous attack pattern. This pattern of attack is similar to "Log Injection-Tampering-Forging" except that in this case, the attack is targeting the logs of the web server and not the application."

CAPEC-204: Lifting Sensitive Data Embedded in Cache

Official Description: "An adversary examines a target application's cache, or a browser cache, for sensitive information. Many applications that communicate with remote entities or which perform intensive calculations utilize caches to improve efficiency. However, if the application computes or receives sensitive information and the cache is not appropriately protected, an attacker can browse the cache and retrieve this information. This can result in the disclosure of sensitive information."

CAPEC-125: Flooding

Official Description: “An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When successful this attack prevents legitimate users from accessing the service and can cause the target to crash. This attack differs from resource depletion through leaks or allocations in that the latter attacks do not rely on the volume of requests made to the target but instead focus on manipulation of the target's operations. The key factor in a flooding attack is the number of requests the adversary can make in a given period of time. The greater this number, the more likely an attack is to succeed against a given target.”

CAPEC-233: Privilege Escalation

Official Description: “An adversary exploits a weakness enabling them to elevate their privilege and perform an action that they are not supposed to be authorized to perform.”

Threat Modeling Report with OWASP pytm

In our new proposed network, we decided to utilize the python library known as the OWASP pytm which is a threat modeling framework that allows for a professional threat modeling report to be generated. As this is an open-source tool, it does not require any subscriptions or account creation to be utilized. After creating the DFD diagram using threat dragon, we utilized that specific DFD to assist us with writing the python code for threat modeling by using pytm. The code written is precisely based on the DFD diagram but has more details such as what ports are being used, what risks and mitigations are there based on each dataflow.

This was implemented in Kali Linux and by first closing the git repository of pytm. Then a virtual environment was set up and using the requirements.txt file, all the needed python packages were installed in the virtual environment. Then inside the pytm folder, the tm4.py file was created which was the code written to generate threat modeling. By using the "python tm4.py --report docs/advanced_template.md | pandoc -f markdown-tex_math_dollars -t html > 445CyberCo.html" command, we were able to generate a html file that included a full report on the threat modeling of our new proposed network with detailed explanations of risks and their severity levels.

Security Controls:

In our new proposed network, our main EDR and SIEM tools are Microsoft Sentinel. Microsoft Sentinel is a cloud native, especially Microsoft cloud environment. Every data flow from between the cloud resources like application logs from the web portal, Azure Blob Storage, Entra ID logon sessions, etc.. will be ingested into Microsoft Sentinel as the central security dashboard for the company system and administrator to monitor. Microsoft Sentinel can also be configured with certain alert rules to triage any suspicious activity in the company cloud environment to trigger the company SOC team to initiate the Sentinel Playbooks (SOAR) for automated response. For EDR implementation on the user laptop, we will use Microsoft Defender to be deployed on all of the company laptops. Recalling that we abolished BYOD to COPE, having Defender as a requirement would be easy to set up and ensure that the company laptops are 100% protected. Furthermore, we will also ensure that Microsoft BitLocker is also active on laptops to enable FDE and prevent company data from being exposed in case of stolen/lost laptops.

Why is our new proposed network aligned with ZTA?

The main answer is Microsoft Entra ID. With Microsoft Entra ID, we ensure that before the company staff can access the company asset on Azure cloud, they must be properly authenticated and pass the device health check. The system admin staff can configure the security setting that each staff member must follow a strong password policy with MFA requirement. Microsoft Entra ID can also be an IAM where after authentication, the staff only being given enough privilege access to the specific resources based on their role which satisfied the principle of least privilege and RBAC. Even after the staff already passed the authenticated part, their activities are still being continuously monitored by Microsoft Sentinel to stay up to date for any potential suspicious actions.

Why is our new proposed network aligned with a data-centric security model?

To ensure our proposed network follows a data-centric security model, we can implement Microsoft Purview Information Protection to secure sensitive PII data like the client data and HR data to be strictly encrypted at rest in the Azure Blob storage. Each file type stored on Azure can be labeled for their priority and importance. DLP rules like unauthorized file upload to another domain with a file that is labeled as "Restricted" can ensure that the staff or attacker cannot exfiltrate the important data.

Section 5. Recommend a strategy and plan

Chaos Engineering for Testing System Resiliency

To test the resiliency of our new proposed cloud solution, we will implement the principle of chaos engineering utilizing open-source Chaos Toolkit from GitHub. Chaos engineering is basically a

controlled and automated security process of intentionally causing failures in a system to see how it behaves to study whether the system can recover and maintain resiliency for such failures that can occur in the future but not as a drill. Potential experiments we can utilize Chaos Toolkit to test our 455Co Cloud System would be designing a python script with necessary modules installed from the Chaos Toolkit and simulating a DOS attack on our company website hosted on Azure App Service. The expected DOS attack on our website should trigger an alert from Microsoft Sentinel, and the web application firewall on Azure should be initiated to start blocking the traffic from the host machine that is sending heavy requests. Another experiment would be intentionally causing the azure server to be down and observe if our website can start back up within a defined RTO by checking if Azure load balancer works as expected in moving our website to another Azure server in a healthy stage. We should also be expecting to see the server error log in Microsoft Sentinel report. These tested experiments can be set to run daily, weekly, or any time interval to ensure that our 445Co system is always ready to handle and recover from real future failures.

Open-source tool with AI Integration for Security Coding Compliance

To ensure all the code and program files from the developer teams following the secure coding rules, we can utilize the GitHub Advanced Security tool CodeQL with AI-powered semantic code analysis engine to scan all GitHub Pull requests from the developers for detecting any potential vulnerabilities in the code to keep the developer teams stick with secure coding policy.

Integration of Microsoft Sentinel built-in Fusion AI

Microsoft Sentinel has a ML security feature Fusion AI that can be enabled by our security staff. According to Microsoft, Fusion is built with machine learning algorithms, to detect advanced multistage attacks or APT by correlating many low-fidelity alerts and events across multiple

products into high-fidelity and actionable incidents. This would enable lesser false positive alerts and help our security team direct their focus on monitoring the threat more effectively and efficiently. Fusion is constantly being trained on the 30 days of historical data from Microsoft Sentinel to keep the ML engine up to date with the relevant information about the data flow and logs from our company cloud network.

Incident response

Incident response and handling will be crucial for these new proposed systems to ensure operations go smoothly. The plan will make certain that there are steps that can be followed to prepare for, respond, and recover from potential cyber-attacks that may occur. It should be also noted that an effective incident response plan is crucial for ensuring customer trust, limiting damage and possible data loss, and avoiding reputation damage, and maintaining regulatory compliance. The SANS incident response guide will be utilized in addition with some other sources to develop the proper incident response plan for 445CyberCo.

Section 6. Incident Response

Step 1: Preparation

Preparation is most likely one of the most important steps for ensuring a successful incident response plan. An incident response team needs to be created, and roles are given to each member. To ensure that the team is ready for different types of incidents, playbooks, policies, as protocols need to be made for such incidents.

It will be essential that the team gets incident training and simulations to make certain that they are prepared should an incident occur. As such, they need to become familiar with the incident response tools within the Microsoft Entra ecosystem. The New Microsoft Incident Response

guides should be utilized as training materials for the team. Some recommended tools from Microsoft Entra will be mentioned in step 2.

Step 2: Identification

Identification of the incident is crucial as well because the sooner the incident is identified, the higher the chances are of limiting data loss, reputation damage, etc.

Anomalies need to be detected by using various tools within the Microsoft Entra ecosystem. Useful tools are as follows: Microsoft Sentinal Alerts, Microsoft Entra audit logs, Incidents and alerts in the Microsoft Defender portal, and the many other tools available within Microsoft Entra. By utilizing the logs, the severity levels of the incident need to be found.

According to SANS, the scope, nature, and impact of the incident need to be determined.

Step 3: Containment

Containment is extremely important because stopping the spread of the malware and threat will ensure that the main objectives of the incident response plan are met.

Utilizing resource isolation with multiple tenants will be necessary in Microsoft Entra to ensure the threat does not spread to the rest of the network.

Make sure that the containment is implemented in a secure manner and not comprise the function of the rest of the network/systems.

Step 4: Eradication

Eradication is important as it involves actually removing the threats from the system or network and patching vulnerabilities.

In Eradication, the threat such as any malware needs to be removed from the systems and networks. The root cause of the incident needs to be determined to prevent a similar incident from happening again.

Step 5: Recovery

Recovery is one of the most essential aspects of the incident response as it allows for the Restore the impacted systems, data, configurations, etc. Recovery is one of the most essential aspects of the incident response as it allows for restoring the impacted systems, data, configurations, etc. to normal by utilizing backups and system restore points. Keep monitoring the systems to ensure no residual threats remain.

Step 6: Lessons Learned

Lessons learned are crucial as it will ensure that a similar incident does not happen again. Post-incident reviews need to be conducted to determine what went well, what went wrong, and what can be improved as well as possible areas of improvements according to SANS. Ensure to document everything that happened, and what can be done to improve. According to SANS update "Update policies, procedures, communications plans, and technologies" based on the lesson learned.

Contributions

Kamyar

Kamyar worked on section 2 and listed 28 requirements needed to ensure the security of the 445CyerCo. He listed all the sources he utilized and also wrote a requirement statement as well as a proposed solution. Then Kamyar worked on section 3 and used Microsoft vision to design the network diagram based on the DFD made from threat dragon. Next, he worked on writing

about the STRIDE and CAPEC threats. He then used the OWASP pytm for part b to make detailed threat modeling. Next, he worked on section 6 and wrote a detailed incident response plan about the designed network. He clearly explained each section and made contributions to writing the essay. He recorded a demo of the tools he worked on.

David

David worked on section 1 and used the Risk Assessment Matrix Generator from tool GitHub to generate the risk matrix. Then he worked on the threat dragon for section 3 and designed a detailed data flow diagram with it. Next, he worked on section 4c and 4d and explained the security controls as well as how our design aligns with the zero-trust architecture. He used the open-source Chaos Toolkit from GitHub to work on section 5. He clearly explained each section and made contributions to writing the essay. He recorded a demo of the tools he worked on.

References

https://learn.microsoft.com/en-us/windows-server/identity/identity-and-access

https://www.cisco.com/site/us/en/products/security/secure-client/index.html

https://www.microsoft.com/en-us/security/business/microsoft-intune

https://csrc.nist.gov/glossary/term/role_based_access_control

https://www.microsoft.com/en-us/sql-server

https://azure.microsoft.com/en-us/products/storage/files

https://www.passwordmanager.com/best-enterprise-password-managers/

https://nordpass.com/features/

https://www.av-test.org/en/antivirus/business-windows-client/windows-11/october-2025/microsoft-defender-antivirus-enterprise-4.18-252514/

https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-business

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-plans-and-pricing

https://support.microsoft.com/en-us/office/frequently-asked-questions-about-microsoft-planner-d1a2d4e6-a4d7-408c-a48a-31caaa267de5

https://community.dynamics.com/blogs/post/?postid=11b80073-e8f5-4420-8b93-b5277d8f5826

https://www.microsoft.com/en-us/security/business/data-security-governance/microsoft-purview-data-security

https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-access-control-nac.html

https://www.cisco.com/c/en/us/tech/security-vpn/network-admission-control-nac/index.html

https://www.ibm.com/think/topics/disaster-recovery-plan

https://learn.microsoft.com/en-us/azure/sentinel/overview?tabs=defender-portal

https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/assets/docs/OWASP_SCP_Quick_Reference_Guide_v21.pdf

https://www.geeksforgeeks.org/system-design/zero-trust-architecture-system-design/

https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id

https://techcommunity.microsoft.com/blog/microsoft-security-blog/announcing-new-microsoft-azure-information-protection-policy-decision-point-capa/250542

https://tetrate.io/learn/what-is-zero-trust-architecture-zta

https://www.intersecinc.com/blogs/the-logical-components-of-zero-trust

https://www.youtube.com/watch?v=LaDSrwAOszQ&start=303

https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

https://azure.microsoft.com/en-us/products/web-application-firewall

https://medium.com/@arielhacking/examples-of-stride-threats-for-payment-applications-87a0ad0c3a21

https://threat-modeling.com/the-ultimate-list-of-stride-threat-examples/#1-tampering-threat-examples

https://capec.mitre.org/data/definitions/98.html

https://capec.mitre.org/data/definitions/173.html

https://capec.mitre.org/data/definitions/123.html

https://capec.mitre.org/data/definitions/165.html

https://capec.mitre.org/data/definitions/268.html

https://capec.mitre.org/data/definitions/81.html

https://capec.mitre.org/data/definitions/204.html

https://capec.mitre.org/data/definitions/125.html

https://capec.mitre.org/data/definitions/233.html

https://owasp.org/www-project-pytm/

https://pypi.org/project/pytm/0.3/

https://attack.mitre.org/

https://medium.com/@efamharris/improving-azure-visibility-and-secrets-monitoring-with-wazuh-and-custom-dashboards-94ece676a9b9

https://www.youtube.com/watch?v=_oO4zju8M0E

https://codeql.github.com/

https://learn.microsoft.com/en-us/azure/sentinel/fusion

https://www.microsoft.com/en-us/security/blog/2020/02/20/azure-sentinel-uncovers-real-threats-hidden-billions-low-fidelity-signals/

https://www.bitsight.com/blog/how-create-incident-response-plan-5-steps

https://www.sans.org/security-resources/glossary-of-terms/incident-response

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-audit-logs

https://www.microsoft.com/en-us/security/blog/2024/01/17/new-microsoft-incident-response-guides-help-security-teams-analyze-suspicious-activity/

https://learn.microsoft.com/en-us/entra/architecture/secure-multiple-tenants

https://github.com/chaostoolkit

https://github.com/neviarrawlinson/risk-assessment-matrix