4-2 Project One: Multi-Level Approach to Enterprise Security

Joshua Merren

Southern New Hampshire University

CYB-420-13227-M01 Enterprise Security

Professor Aaron Tyler

29 January 2025

I. Threat Assessment

A. Vulnerabilities in the Risk Domain of People.

One of the most common vulnerabilities in organizations is human error, which can lead to security breaches if not sufficiently mitigated. Employees often use weak passwords or reuse the same password across multiple platforms, making it easier for attackers to gain unauthorized access (CISA, 2019). Cybercriminals can exploit these weaknesses without proper password management policies through brute-force attacks or credential stuffing. Additionally, a lack of regular cybersecurity training leaves employees susceptible to phishing attempts and social engineering tactics, where attackers manipulate individuals into divulging sensitive information. Insider threats, intentional or accidental, also pose a significant risk, as employees with access to critical systems may unintentionally expose or misuse data. Another concern is the lack of enforcement of multi-factor authentication (MFA), which adds an essential layer of security that prevents unauthorized access even if passwords are compromised (CISA, n.d.). Additionally, poor physical security, such as leaving workstations unlocked when unattended, can allow unauthorized individuals to access sensitive company data. Strengthening security awareness programs and enforcing strict authentication tools can significantly reduce these human-related risks. Another significant vulnerability is the lack of physical access control at entry points, which increases the risk of unauthorized personnel entering restricted areas. Without an RFID-based access control system, intruders or disgruntled employees could enter IT rooms, directly tampering with critical infrastructure. Implementing RFID card readers at key entry points ensures that only authorized personnel can access sensitive areas, reducing insider threats. These RFID readers should be integrated with the organization's Authentication Server, ensuring real-time entry logging and automated alerts for unauthorized access attempts.

B. Vulnerabilities in the Risk Domain of Process.

Weak or inconsistent security processes can create significant organizational vulnerabilities, making it easier for attackers to exploit operational weaknesses. A major issue is the failure to establish and enforce a comprehensive patch management policy, which can expose critical systems to known exploits (CISA, n.d.). Without a structured update process, outdated software and unpatched vulnerabilities remain open attack vectors for cybercriminals. Another process-related vulnerability is the absence of a robust incident response plan, which can result in delayed or inadequate reactions to security breaches. Inadequate access control policies can lead to unauthorized personnel gaining access to sensitive data, increasing the risk of insider threats and data leaks. A lack of proper employee offboarding procedures can also create risks, as former employees may retain access to company systems long after departure. Additionally, many organizations neglect routine security audits, missing critical opportunities to identify and address process gaps and vulnerabilities before attackers can exploit them. Poor documentation of security protocols further exacerbates these risks, as employees may be unaware of the correct procedures to follow in case of an incident. Establishing structured policies, conducting regular audits, and enforcing access control measures are critical in mitigating process-related security risks.

C. Vulnerabilities in the Risk Domain of Technology.

Technological vulnerabilities are a significant concern, as outdated or misconfigured systems provide easy targets for attackers. One of the most common vulnerabilities is unpatched software, which cybercriminals exploit using known exploits documented in vulnerability databases (CISA, n.d.). Additionally, misconfigured firewalls and open ports create security gaps that allow unauthorized access to the network (Sanjana, 2024). Weak encryption or a complete

lack of encryption for sensitive data at rest and in transit exposes organizations to data breaches, especially when attackers intercept communications. Poorly secured APIs can be another attack vector, as cybercriminals often exploit insecure endpoints to access internal systems. Using default or easily guessable configurations in network devices can lead to unauthorized access if improperly secured. Lack of centralized monitoring and logging can delay the detection of security incidents, allowing threats to persist undetected. Additionally, outdated hardware that lacks modern security features poses a significant risk, as legacy systems may not support newer encryption standards or security patches. Enforcing regular updates, conducting security audits, and enforcing strict configuration standards are essential to mitigating technological vulnerabilities.

II. Adversarial Mindset.

A. Assessing Vulnerabilities in the Risk Domain of People.

Thinking like an attacker is essential when identifying human-related vulnerabilities, as social engineering is one of the most effective ways to breach an organization. Attackers often exploit predictable behaviors, such as an employee's tendency to click on unverified links or download attachments from unknown sources. Understanding this, organizations should implement phishing awareness training to educate employees on recognizing deceptive emails and fraudulent websites (CISA, 2019). Attackers also take advantage of employees' lack of security awareness by tricking them into revealing credentials over the phone or through in-person impersonation. Social engineering tests, where ethical hackers simulate attack scenarios, can help organizations assess how employees respond to such tactics. Weak password practices are another concern, as attackers use brute-force techniques to crack simple passwords (CISA, 2019). Encouraging the use of password managers and enforcing complex password policies can

significantly reduce these risks. Additionally, attackers may exploit insider threats by bribing or coercing employees into leaking sensitive information. By anticipating these tactics, organizations can develop strategies to mitigate them, such as enforcing strict access control and implementing behavioral monitoring.

B. Assessing Vulnerabilities in the Risk Domain of Process.

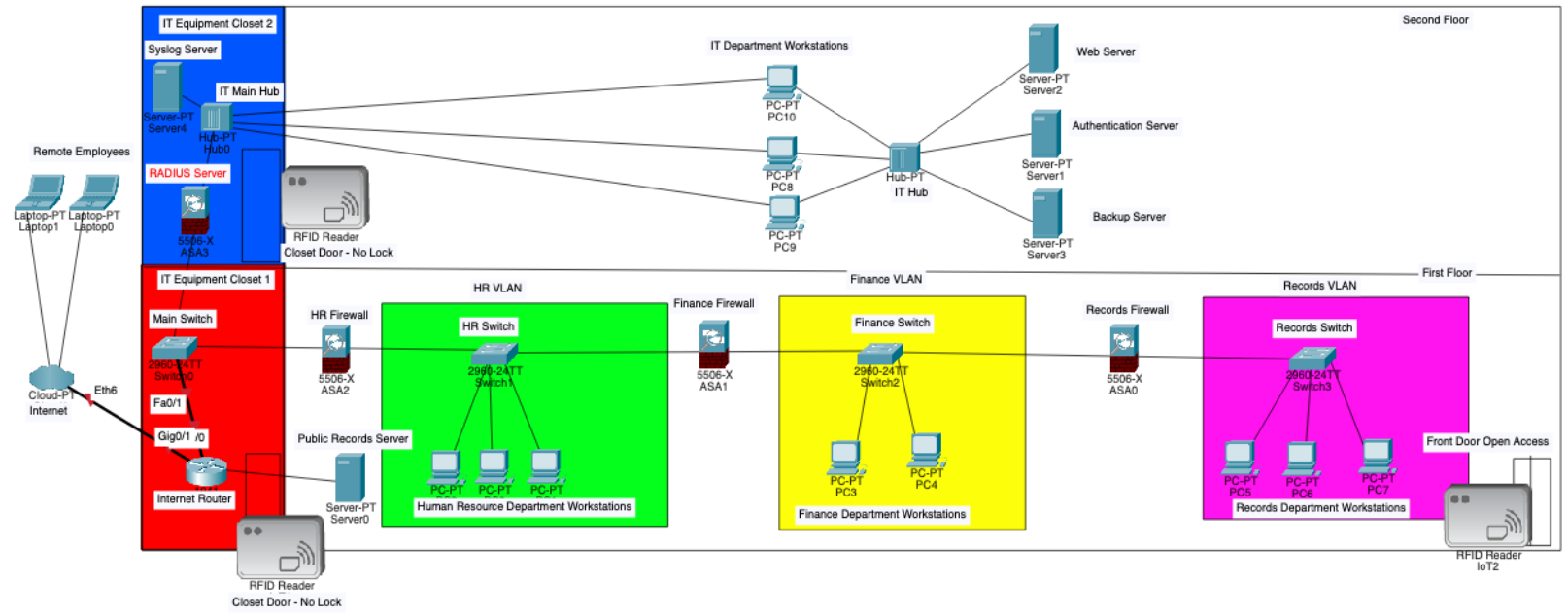
Attackers often look for weaknesses in an organization's security processes, exploiting gaps in patch management, access control, and incident response procedures. If an organization lacks a structured process for applying software updates, cybercriminals can target known vulnerabilities to gain access to systems (Sanjana, 2024). Weak access control policies may allow attackers to use stolen or weak credentials to escalate privileges and move laterally across the network. A poorly defined incident response plan can result in delayed or ineffective action when an attack occurs, giving adversaries more time to cause damage. Attackers may also exploit the lack of vendor security management, targeting third-party suppliers with access to the organization's internal network. Weak password reset policies, where help desk staff reset credentials without proper verification, provide another attack surface for social engineers. Insufficient monitoring of privileged user accounts may allow unauthorized changes to go unnoticed. Organizations must proactively analyze these vulnerabilities by conducting regular security assessments and refining security policies to close these gaps.

C. Assessing Vulnerabilities in the Risk Domain of Technology.

Attackers take advantage of technological weaknesses, particularly those related to misconfigurations, outdated systems, and insufficient network security. For example, misconfigured firewalls allowing unrestricted traffic increases the risk of external threats bypassing security defenses (Sanjana, 2024). Cybercriminals frequently scan for open ports and

unsecured databases, taking advantage of organizations that have not adequately restricted access. Unpatched software remains a primary target, as attackers rely on outdated vulnerabilities to infiltrate systems. Attackers can exploit weak encryption protocols through man-in-the-middle attacks by intercepting sensitive communications. Insufficient logging and monitoring allow attackers to operate undetected, extending the duration of their attacks. Additionally, insecure remote access configurations, such as weak VPN settings, make it easier for adversaries to gain unauthorized entry into corporate networks. Organizations should prioritize regular patching, implement strict network segmentation, and enforce strong encryption policies to mitigate these technological risks.

III. Infrastructure Diagram.



A. Controls to Address Vulnerabilities in People.

Implementing a multi-layered security approach that focuses on human behavior and authentication is critical to mitigate vulnerabilities in people's risk domain. One of the most effective controls is enforcing multi-factor authentication (MFA), which ensures that even if an employee's password is compromised, an additional verification step is required for access (CISA, n.d.). Organizations should also implement mandatory cybersecurity awareness training programs that educate employees about phishing, social engineering, and password best practices. Employees must understand the risks of reusing passwords across platforms and recognize common attack vectors, such as spear-phishing attempts. Implementing role-based access control (RBAC) can limit employees' access to only the resources necessary for their specific job functions, reducing the potential for unauthorized access. Another important control is automatic session timeouts, which log out inactive users from their workstations, preventing unauthorized access in cases where employees leave their computers unattended. Organizations should also conduct regular security assessments and phishing simulations to measure employee preparedness and identify areas that require additional training. Lastly, organizations must conduct strict background checks before hiring employees with access to sensitive systems, as insider threats pose a significant risk (Seagate, n.d.). RFID badge readers should be installed at critical access points, such as the front entrance and IT Equipment Closets, to enhance physical security further. Employees would need RFID cards to gain entry, ensuring that only authorized individuals can access sensitive areas. Integrate this system with the existing authentication server to verify RFID scans, maintain entry logs, and detect and respond to unauthorized access attempts. Automated access tracking with alerts immediately notifies security teams of suspicious activity in restricted areas.

B. Controls to Address Vulnerabilities in Process.

Implementing well-defined policies and structured security frameworks reduces security vulnerabilities in organizational processes. A primary control measure is enforcing a strict patch management policy to update all software and operating systems regularly, reducing exposure to known vulnerabilities (CISA, n.d.). Organizations should also establish a formal incident response plan (IRP) that provides employees with clear procedures for responding to security breaches, including reporting, containment, and recovery steps. Conduct regular security audits to ensure compliance with security policies and identify gaps in existing procedures. Another essential control is third-party vendor risk management, which requires organizations to assess the security posture of any external partners with access to internal systems. Organizations should also implement data access logging and monitoring, which tracks all user interactions with sensitive information and generates alerts for suspicious activity. Additionally, organizations must strictly enforce employee onboarding and offboarding procedures to revoke access rights when an employee leaves immediately. Lastly, role-based approval workflows should be introduced for executing critical system changes, ensuring that sensitive modifications require multiple levels of approval. These structured controls reduce security risks associated with weak or inconsistent processes (Seagate, n.d.). The organization should incorporate the RFID system into its security policies by actively logging entry data and reviewing it during regular security audits. In addition, promptly updating RFID badge permissions when employees leave the company prevents former employees from using old credentials to gain unauthorized entry.

C. Controls to Address Vulnerabilities in Technology.

The risk domain of technology requires robust controls to protect infrastructure from cyber threats and unauthorized access. A key control is network segmentation, where different departments operate on separate VLANs to prevent unauthorized lateral movement by attackers (Sanjana, 2024). Implementing access control lists (ACLs) on network devices helps restrict unauthorized communication between departments, further limiting attack vectors. Another essential control is deploying an endpoint detection and response (EDR) system, which continuously monitors endpoints for signs of cyber threats (Cisco, 2024). Organizations should also implement intrusion detection and prevention systems (IDPS) to detect and block malicious activity at the network perimeter. Additionally, firewalls should be configured with the least privilege rules, ensuring that only essential traffic is allowed. Strong encryption policies should be enforced for data in transit and at rest to prevent breaches. Another crucial step is hardening servers and turning off unnecessary services, reducing the number of exploitable entry points for attackers. Finally, organizations should conduct penetration testing regularly to proactively identify and fix vulnerabilities before attackers can exploit them (Sanjana, 2024). Configure the existing Authentication Server to handle centralized authentication via RADIUS, ensuring that user logins and administrator access to routers and switches authenticate through a single secure system. The system eliminates needing a separate TACACS+ server, streamlining authentication while ensuring firm access control.

IV. Organizational Protection.

A.

To counteract adversaries targeting human vulnerabilities, organizations must implement security controls that directly address social engineering, insider threats, and human error. One of the most effective strategies is ongoing cybersecurity awareness training, which educates

employees on recognizing phishing attempts, suspicious requests, and credential theft tactics (CISA, 2019). Security teams should also conduct simulated phishing attacks to measure employee resilience and adjust training accordingly. Multi-factor authentication (MFA) should be enforced to prevent unauthorized access, even if passwords are compromised (CISA, n.d.). Organizations can also implement strict access control policies, such as limiting administrator privileges to only a few employees requiring elevated access. Insider threats can be mitigated by monitoring user activity logs for unusual behavior, such as repeated failed login attempts or access to unauthorized files. Additionally, organizations should implement zero-trust security models, which require continuous user access verification instead of assuming trust once logged in. Physical security controls, such as biometric authentication for access to server rooms, also help prevent unauthorized entry. By proactively addressing these vulnerabilities, organizations significantly reduce the risk of human-related security breaches. RFID-controlled entry systems actively prevent unauthorized personnel from accessing sensitive infrastructure, significantly reducing security risks. By requiring employee ID badges to enter secure areas, the organization can prevent intruders from physically tampering with networking equipment or accessing confidential data.

B.

Adversaries often exploit process gaps, such as weak patch management, lack of security monitoring, and insufficient disaster recovery planning. Organizations should implement a structured patch management policy to address vulnerabilities and prevent exploitation proactively (Sanjana, 2024). Implementing real-time security monitoring allows organizations to detect threats early and respond before they cause damage. Another essential control is creating a well-defined incident response plan, which includes protocols for detecting, containing, and

mitigating cyber incidents. Organizations should also enforce regular security audits and compliance assessments to identify weaknesses and ensure adherence to best practices. Organizations should design disaster recovery plans (DRPs) with redundant backups stored in secure, offsite locations to ensure the rapid recovery of critical data after a cyberattack or system failure (Seagate, n.d.). Prioritizing vendor risk management ensures that third-party service providers uphold the same security standards as internal operations. Role-based security policies should be applied to limit access to sensitive data, ensuring that only authorized individuals can perform critical functions. These measures significantly enhance an organization's security posture by closing process-related vulnerabilities.

C.

Technology-related threats require proactive controls that strengthen system integrity and network security. One of the most effective countermeasures is deploying next-generation firewalls (NGFWs) to monitor traffic, block unauthorized connections, and filter malicious content (Cisco, 2024). Implementing endpoint detection and response (EDR) solutions allows organizations to detect and respond to cyber threats in real-time. Perform regular vulnerability scans and penetration tests to identify and fix security weaknesses before attackers exploit them. Another key strategy is securing remote access, requiring virtual private networks (VPNs) with strong authentication mechanisms. Organizations should also ensure automated log monitoring is in place to detect suspicious activity, such as brute-force login attempts or unusual data transfers. Data encryption and secure key management also prevent attackers from accessing sensitive information, even if they breach network defenses. To protect network infrastructure against evolving threats, organizations must enforce firmware updates for hardware devices (Sanjana,

2024). Implementing these technology-focused controls helps organizations counteract sophisticated cyber threats and safeguard critical assets.

D.

Implement security controls to balance operational efficiency, cost, and usability. While multi-factor authentication (MFA) is an essential control, organizations must ensure it does not overly complicate user access or disrupt productivity (CISA, n.d.). Similarly, frequent security training should be engaging and practical rather than burdensome for employees. Automated patch management minimizes security risks without requiring manual intervention, reducing the workload on IT teams. Organizations must also balance intrusion prevention systems (IPS) policies to avoid excessive false positives that could interrupt legitimate operations. Redundancy in disaster recovery plans should be optimized to ensure security without excessive costs (Seagate, n.d.). The goal is to implement controls that provide maximum security with minimal disruption, ensuring the organization remains protected and efficient.

References

Choosing and protecting Passwords | CISA. (2019, Nov 18). Cybersecurity and Infrastructure Security Agency CISA. Retrieved January 29, 2025, from https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords

Cisco EndPoint Security. (2024, August 22). Cisco. Retrieved January 29, 2025, from https://www.cisco.com/c/en/us/products/security/endpoint-security/index.html#~types-of-endpoint-security

Known Exploited Vulnerabilities Catalog | CISA. (2024, June 25). Cybersecurity and Infrastructure Security Agency CISA. Retrieved January 29, 2025, from https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Multifactor authentication | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). Retrieved January 29, 2025, from https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication

Sanjana. (2024, December 3). *Top 10 cybersecurity misconfigurations and how to avoid them - ManageEngine Blog*. ManageEngine Blog. Retrieved January 29, 2025, from https://blogs.manageengine.com/active-directory/log360/2024/09/20/top-10-cybersecurity-misconfigurations-and-how-to-avoid-them.html

Seagate. (n.d.). *Why your business needs an enterprise Disaster Recovery Plan | Seagate US*. Seagate.com. Retrieved January 29, 2025, from https://www.seagate.com/blog/why-you-need-enterprise-disaster-recovery-plans/