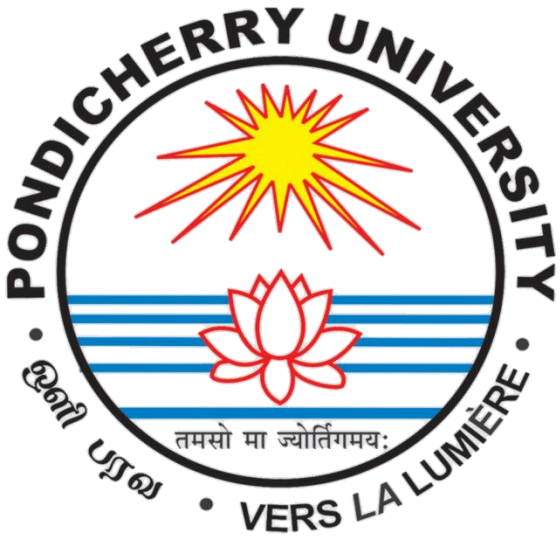
PONDICHERRY UNIVERSITY

(A Central University)



SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

M.Sc. Computer Science

NAME	:	CHOZHAN M
REGISTER NO	:	23370081.
SUBJECT	:	INFORMATION SECURITY MANAGMENT.
SUBJECT CODE	:	CSEL 446
SUBMISSION DATE	:	October 28,2024.

CPU

Risk: Central Processing Units (CPUs) are critical for the operation of any system, making them a prime target for malicious software and hardware attacks, such as CPU vulnerabilities like Spectre and Meltdown. These attacks exploit the way CPUs handle data processing, potentially allowing attackers to access sensitive data and compromise system integrity. Additionally, physical damage to the CPU can halt operations, leading to downtime and financial loss. Overheating is another **Risk**, especially in environments where systems are running at high load, potentially causing long-term damage to the hardware.

Owner: The IT Department, particularly hardware management personnel, are typically responsible for the maintenance, monitoring, and security of CPUs. They ensure the CPU operates efficiently and remains protected from both software and hardware threats. In managed environments, there may also be software-based monitoring tools that provide updates on the CPU's performance and detect any potential security threats.

Mitigation: Implementing proper monitoring solutions and installing firmware updates can protect the CPU against known vulnerabilities. Physical access controls, such as biometric or card access, help prevent unauthorized personnel from tampering with the hardware. Additionally, maintaining proper cooling systems and conducting routine maintenance can prevent overheating, prolonging the CPU's lifespan and maintaining system availability.

Switch

Risk: Network switches serve as a backbone for internal communication within an organization's IT infrastructure. A compromised switch can allow an attacker to intercept, modify, or reroute data packets, leading to potential data breaches. Denial of Service (DoS) attacks on switches can disrupt communication across the network, impacting productivity and service delivery. Unpatched software vulnerabilities in switches may also provide a pathway for attackers to access the broader network.

Owner: Network Administrators typically hold **Owner**ship over the security and configuration of network switches. Their role involves ensuring that all switches are securely configured, have up-to-date firmware, and are monitored for signs of intrusion or failure.

Mitigation: Implementing network segmentation reduces the scope of access, limiting the potential damage of a compromised switch. Network Access Control (NAC) solutions can enforce policies on who can connect to the switch, and regular firmware updates help protect against software-based vulnerabilities. Additionally, configuring switches to limit the rate of data requests can help mitigate the impact of DoS attacks. Using Intrusion Detection Systems (IDS) provides early warning signs if a switch is under attack.

Wi-Fi

Risk: Wi-Fi networks are inherently vulnerable to attacks, especially when unsecured or configured without adequate encryption. Common threats include man-in-the-middle attacks, where attackers intercept and manipulate network traffic, and unauthorized access, where attackers exploit weak passwords or unprotected networks to gain entry. Rogue access points also pose a **Risk**, potentially enabling attackers to create deceptive networks that lure users into sharing sensitive data.

Owner: The Information Security (Infosec) Team is typically responsible for the security of the Wi-Fi network. This team manages access, sets encryption protocols, and ensures network configurations are up-to-date with the latest security standards.

Mitigation: Using WPA3 encryption and strong, unique passwords on all Wi-Fi networks can significantly reduce the **Risk** of unauthorized access. Implementing regular password changes, along with network monitoring solutions, helps detect unauthorized devices or suspicious activity. Educating employees on avoiding rogue access points and using Virtual Private Networks (VPNs) for sensitive data can further enhance Wi-Fi security. For high-security environments, disabling SSID broadcast and restricting Wi-Fi access by MAC address are additional security measures.

Monitor

Risk: Monitors can present unexpected security **Risk**s, especially in shared or open environments. Unauthorized individuals may observe sensitive information displayed on screens, potentially leading to data breaches. Screens that display critical information in publicly accessible areas are vulnerable to shoulder surfing or "visual hacking" attacks. Moreover, unattended monitors may expose confidential information if left unlocked.

Owner: The responsibility for physical security of monitors typically falls to both the IT Department, in terms of provisioning secure hardware, and individual employees, who must ensure that sensitive information is not left visible on screens.

Mitigation: Using privacy screens on monitors reduces the **Risk** of visual hacking in high-traffic or shared areas. Implementing screen timeout policies that lock computers when not in use helps protect information from unauthorized viewing. Training employees to lock screens when leaving their desks can also reinforce a culture of security. In high-security settings, desk arrangements can be optimized to ensure monitors do not face public areas, minimizing exposure to unauthorized viewers

Printer

Risk: Printers, often overlooked, can be a major security vulnerability if not managed properly. They can store data from print jobs, which could be retrieved by unauthorized users, especially in shared workspaces. Network-connected printers are also susceptible to cyberattacks, such as malware infections and unauthorized access, potentially exposing sensitive documents. Unsecured printers can serve as entry points into the network, allowing attackers to gain access to more critical systems.

Owner: The IT Department generally manages printer security, overseeing device configurations, access controls, and firmware updates to minimize vulnerabilities. In organizations, document management and security teams may also collaborate to ensure sensitive data is properly handled during printing.

Mitigation: Implementing access controls, such as PIN or badge-based authentication for printing, can ensure only authorized personnel access print jobs. Regularly updating printer firmware and enabling encryption for data in transit help to prevent unauthorized access. Disabling unnecessary network features and implementing a secure disposal policy for printers (ensuring memory is wiped before disposal) further enhance security.

Fiber Cable

Risk: Fiber optic cables are critical for high-speed, long-distance communication and are generally robust. However, they can be vulnerable to physical damage, leading to data transmission disruptions. Fiber cables are also susceptible to tapping or eavesdropping attacks, allowing data interception if physical security around the cable infrastructure is compromised.

Owner: Network and Infrastructure Teams are responsible for fiber optic cable management. They ensure proper installation, monitoring, and physical security, safeguarding against tampering and damage.

Mitigation: Fiber cables should be installed in secure, concealed conduits to prevent tampering or accidental damage. Regular inspections can help identify weak points or potential vulnerabilities in the physical infrastructure. Deploying Intrusion Detection Systems (IDS) for the network can detect unusual activity, which may indicate a compromised cable. Additionally, using encrypted data transmission over fiber connections reduces the **Risk** of data exposure if cables are tapped.

Network Switch

Risk: Network switches, vital for internal data traffic management, are susceptible to various threats, including unauthorized access and Denial of Service (DoS) attacks. A compromised switch can allow attackers to intercept data, potentially leading to a network-wide security breach. Improperly configured switches can also expose sensitive network traffic to external threats, increasing the **Risk** of data loss or tampering.

Owner: The Network Administration Team generally owns switch security, ensuring that devices are securely configured, patched, and monitored for any suspicious activities.

Mitigation: Configuring switches with strong access control lists (ACLs), enabling port security, and deploying VLAN segmentation can help minimize **Risk**s. Regular firmware updates and proper configuration of network protocols protect switches from known vulnerabilities. Additionally, monitoring tools can provide real-time alerts of any unusual activity, helping to detect and address potential threats promptly.

Server

Risk: Servers are central to an organization's data storage and application management, making them high-value targets for cyberattacks, such as data breaches, ransomware, and unauthorized access. Inadequate security on servers can expose sensitive data, disrupt services, and result in financial and reputational damage. Physical threats, such as theft or environmental hazards (e.g., fires), also pose significant **Risk**s.

Owner: The IT and Security Teams manage server security. Their responsibilities include maintaining system updates, managing access, and monitoring for any unusual activity.

Mitigation: Servers should be located in a secure, access-controlled environment, ideally within a data center equipped with surveillance and fire suppression systems. Regular software and firmware updates, combined with strong password policies and multi-factor authentication, help prevent unauthorized access. Data backup protocols and disaster recovery plans are also essential to minimize the impact of server outages or data loss. Implementing endpoint detection and response (EDR) tools can further enhance server security by providing real-time monitoring and automated responses to detected threats.

Main UPS

Risk: The main Uninterruptible Power Supply (UPS) ensures the continuous operation of critical systems during power outages. However, UPS systems can be vulnerable to power surges, physical tampering, and environmental threats. Failure of the UPS can lead to data loss, hardware damage, or operational downtime, especially in environments dependent on constant power supply.

Owner: The Facilities and IT Teams jointly own UPS management. Facilities teams handle the physical maintenance, while IT teams ensure it meets the power demands of critical systems.

Mitigation: Regular testing and maintenance are essential to ensure the UPS operates effectively during power disruptions. Installing the UPS in a secure, climate-controlled room prevents physical tampering and overheating. Routine battery checks and replacements are also necessary to maintain power reliability. Redundant UPS configurations can provide an additional layer of protection, and automated monitoring systems can alert teams to potential failures in real time.

Scanner

Risk: Scanners, particularly networked ones, can store scanned documents, potentially exposing sensitive information if the device is improperly configured or accessed by unauthorized users. They may also be susceptible to malware attacks and unauthorized access, compromising the confidentiality of scanned data. Scanners shared among users are especially vulnerable, as there's a higher **Risk** of sensitive data being left accessible to unintended users.

Owner: The IT Department generally oversees scanner security, ensuring configurations are properly secured and access is controlled.

Mitigation: Implementing user authentication on scanners restricts access to authorized personnel. Regularly wiping or encrypting stored data reduces the **Risk** of exposure. Networked scanners should be configured with secure communication protocols (e.g., SSL/TLS) to protect data in transit. User training to reinforce the secure handling of sensitive data can also help mitigate **Risk**s associated with document scanning.

MCP (Microcontroller-based Processor)

Risk: MCPs, widely used in embedded systems for process control, are vulnerable to both cyber and physical attacks. Cyber **Risk**s include firmware exploitation, where attackers inject malicious code to control the device or extract data. Physical threats include tampering, where unauthorized individuals can alter or damage components, potentially affecting device operation.

Owner: Embedded System Engineers and the IT Department share responsibility for MCP security, overseeing device configurations and monitoring for any unauthorized activity.

Mitigation: MCPs should use firmware with secure boot capabilities and be regularly updated to patch any discovered vulnerabilities. Access control measures and encrypted communication protocols help secure data transmission. For physical security, MCPs should be housed in tamper-resistant casings and located in secure areas. Routine vulnerability testing, combined with intrusion detection on associated networks, can further protect MCPs from potential attacks.