INTE 31332 – Information Systems Auditing and Control (21/22)

Individual Assignment – Risk Assessment Report

J.P.H.G. Jayasundara

IM/2019/096

Department of Industrial Management

Faculty of Science

University of Kelaniya

Date of submission: 20/05/2023

Risk Assessment Report

The following risk assessment was conducted to evaluate the potential threats and vulnerabilities of listed assets for a hypothetical company. The rate of occurrence and associated risk level were assumed based on potential frequencies of threat occurrences. Possible treatment options are also recommended for the threats listed.

The rate of occurrence refers to the frequency or likelihood with which a specific risk event is expected to happen within a given time period. It represents the estimated number of times the risk event may occur. Here, in addition to numeric values to describe rate of occurrences, terms such as occasional/rare were also used. In this context, occasional refers to threats that may occur as often as several times a year or once/twice a year. Rare are those that may not occur for many years.

Risk level is a measure of the overall impact or severity of a particular risk. It combines the consequences or potential harm that can result from the risk event with the likelihood of its occurrence. High-risk threats are those with a high likelihood of occurrence and significant potential impact, while low-risk threats are those with a low likelihood of occurrence or minimal impact. Medium-risk threats fall between these extremes.

Asset	Threat	Vulnerability	Rate of Occurrence	Risk level	Treatment Plan
Personal Computer	Malware infections (viruses, trojans, worms, and ransomware)	Not updating virus guards correctly	5/ 10 times a year	High	Identify and isolate infected systems, run anti-malware software, Remove infected files, Update software and security patches
	Phishing attacks	Lack of awareness among employees	Once in 3 years	Medium	Organize regular awareness programs, Conduct phishing simulations to better prepare employees
	Password cracking	Using weak passwords	Once in 5 years	Medium	Introduce a password policy. *Ex. Minimum 8 characters with a mix of upper case and lower case letters, a number and special character*
	Pretexting - type of social engineering attack	Lack of awareness and carelessness	3 times a year	High	Conduct awareness programs, Verify requests through established channels to prevent unauthorized access

	Unsecured wireless networks	Weak or no encryption	Once in 5 years	Medium/Low	Use WPA2 encrypted security protocol and other network security protocols.
Printers	Print spooler attacks	Inadequate print spooler security configurations, unpatched vulnerabilities, or weak access controls	Twice a year	High	Keep the print spooler software up to date with the latest security patches and updates, Implement strong access controls and user authentication mechanisms for print spooler services.
	Print firmware attacks	Outdated or unpatched printer firmware, weak firmware security configurations	Once every few years	Medium	Regularly update printer firmware with the latest manufacturer-provided patches and security updates
	Printer data leakage	Insufficient data encryption, unsecured print jobs	Once a year	High	Implement encryption mechanisms, such as SSL/TLS, for print job transmission to protect data in transit.
	Printer supply chain attacks	Compromised printer hardware or software during the manufacturing or distribution process	Once in 5 years	Low	Establish strong relationships with trusted printer manufacturers and suppliers and confirm integrity of products
	Unauthorized access to printer configuration settings	Weak or default administrator passwords, or misconfigured printer settings	Several times a year	Medium/High	Change default administrator passwords to strong, unique passwords, Regularly review and audit printer configuration settings
Servers	DDoS attacks	Lack of traffic monitoring	Once/few times a year	High	Configure network devices and firewalls to filter and block malicious traffic, Implement rate limiting and traffic shaping mechanisms to manage traffic spikes
	SQL injection attacks	Improper input validation, lack of parameterized queries	Once/few times a year	Medium/High	Implement secure coding practices, such as input validation and parameterized queries, to prevent SQL injection vulnerabilities.

	Malware	Unpatched software, inadequate security configurations	Several times a year	High	Regularly update server operating systems, applications, and security patches, Deploy and keep up-to-date antivirus and antimalware solutions on servers.
	Insider threats	Malicious or disgruntled employees with authorized access to the server infrastructure.	Occasional/once every few years	Medium	Conduct thorough background checks and provide security awareness training to employees, Implement data loss prevention (DLP) solutions to monitor and prevent unauthorized data exfiltration.
	Insecure remote access	Unencrypted remote access and weak/default credentials	Once/few times a year	Medium	All remote access sessions should be encrypted using a strong encryption protocol such as TLS or SSH, Default credentials should be disabled, and unique passwords should be assigned to each user.
Switch	Unauthorized access to network traffic	Lack of access controls, or unsecured management interfaces.	Once/few times a year	Medium	Implement strong access controls, such as role-based access control (RBAC), to restrict access to switch management interfaces, Implement secure management protocols, such as SSH or HTTPS, for remote access to switches.
	Spoofing attacks	Lack of port security measures	Once every few years	Medium	Enable port security features, such as MAC address filtering to allow only authorized devices to connect to switch ports, Regularly monitor switch ports and review connected devices for any signs of unauthorized or rogue devices.
	MAC address flooding attacks	Lack of MAC address limiting or insufficient switch memory management	Occasional/once every few years	Medium	Implement traffic shaping and rate limiting to prevent excessive traffic that could result in MAC address flooding.
	VLAN hopping attacks	Inadequate VLAN configuration, or unsecured trunk ports.	Once every few years/rare	Low/Medium	Implement proper VLAN segmentation and configure access control lists (ACLs) to control traffic between VLANs, Disable

					unused or unnecessary trunk ports and regularly review and validate trunk port configurations.
	Unauthorized configuration changes	Insufficient change management processes	Occasional/once every few years	Medium	Establish change management processes that require documented approvals for configuration changes, Regularly backup switch configurations and maintain configuration change logs for auditing purposes.
Router	IP spoofing attacks	Lack of ingress and egress filtering, or unauthenticated routing updates.	Occasional/may occur several times a year	Medium/High	Implement ingress and egress filtering to validate the source and destination IP addresses of incoming and outgoing traffic, Use secure routing protocols, such as BGP (Border Gateway Protocol) with authentication, to prevent unauthorized routing updates, Implement anti-spoofing measures like Unicast Reverse Path Forwarding (uRPF), to detect and prevent IP spoofing attacks.
	DNS spoofing attacks	Lack of DNSSEC (DNS Security Extensions) implementation	Once every few years	Medium/High	Implement DNSSEC to add an added layer of security to DNS resolution and prevent DNS spoofing attacks, Implement DNS caching mechanisms to mitigate the impact of DNS spoofing attacks.
	Exploitation of firmware vulnerabilities	Outdated or unpatched router firmware	Rare (once in 5 years)	Medium	Regularly update router firmware, Follow best practices provided by the manufacturer for securing and updating router firmware.
	Unauthorized access to the wireless network	Unsecured wireless networks	Occasional/Rare	Medium	Enable MAC address filtering to allow only authorized devices to connect to the wireless network.
	Physical theft of router hardware	Inadequate physical security	Rare (once in 5-10 years)	Low	Implement physical security measures like securing the router in a locked cabinet or rack, using cable locks to secure the router

					to a fixed structure, and installing surveillance cameras or alarms in the vicinity to protect the router from theft.
Network Cables	Eavesdropping on network traffic	Unsecured/unencrypted network protocols	Occasional/once every few years	Medium/High	Use encryption protocols like SSL/TLS or IPSec to secure network traffic and protect data confidentiality.
	Packet sniffing attacks	Compromised network monitoring tools	Occasional/rare	Medium/High	Regularly update and patch network monitoring tools, Monitor network traffic for suspicious packet capture activities or unauthorized use of network monitoring tools.
	Physical tempering of the hardware	Lack of physical security measures	Rare	Medium	Secure cables (use locking cabinets or cable trays) to prevent unauthorized access.
	Man-in-the-Middle attacks	Lack of encryption on network traffic	Occasional/once every few years	Medium/High	Implement WPA2 or WPA3 encryption protocols, Implement strong access controls
	Cable damages	Improper cable installation/ accidental cable damage	Occasional/rare	Low/Medium	Ensure proper cable installation including correct cable routing. Use cable conduits, protective covers and inspect cables regularly for wear, fraying etc. and replace if needed.
Data Centers	Environmental threats like fires, flooding.	Inadequate fire suppression systems, weaknesses in construction	Rare/once every several years	High	Install and maintain fire suppression systems like automatic sprinklers, dry pipe sprinkler, fire alarms, Establish proper segregation between water-based systems and sensitive equipment to minimize the risk of water damage
	Physical security breaches	Weak perimeter security	Occasional/once every few years	Medium/High	Restrict access to critical areas, Implement robust physical access controls, such as biometric authentication, access cards, and video surveillance systems.
	Power outages	Inadequate power backup systems	Many times a year	High	Deploy UPS to provide backup power during outages, Install backup generators to

					supply extended power during prolonged outages.
	Hardware failures	Faulty hardware components	Once every few years	Medium	Monitor hardware, Implement RAID (Redundant Array of Independent Disks) configurations or clustering, to mitigate the impact of hardware failures
	Network attacks on data center infrastructure	Weak network security controls	Several times a year/once every few years	High/Medium	Implement intrusion detection/prevention systems, and access controls, Segment the network into different security zones to limit lateral movement in case of a breach.
Fire Extinguishers	Misuse/unauthorized use	Lack of control over access to fire extinguishers	Once every 10 years (exceedingly rare)	Medium/Low	Implement physical security measures, like placing fire extinguishers in locked cabinets or using tamper-evident seals.
	Inadequate/expired fire suppression materials	Fire extinguishers with such materials will fail to properly combat fires	Once every 10-12 years	Medium	Conduct routine checks to ensure fire extinguishers are properly pressurized and their fire suppression materials are within expiration dates.
	Inadequate training for staff	Lack of awareness among employees on fire drills and proper use of fire extinguishers	Once a year	Medium	Conduct regular fire drills to practice emergency procedures, Implement comprehensive fire safety training programs.
	Improper storage of fire extinguisher	Placing fire extinguishers in hard to access places, hindering their use in an emergency	Once every few years	Low/Medium	Ensure fire extinguishers are strategically placed in easily accessible and visible locations, following local fire safety codes and regulations.
	Lack of an emergency evacuation plan	Lack of an emergency evacuation plan may cause unnecessary panic and delays	Once a year	Medium/High	Communicate and train employees on the emergency evacuation plan, including their roles and responsibilities during a fire incident, Conduct regular drills to practice the evacuation procedures and evaluate the effectiveness of the plan.

IT Staff	Insider threats (compromised IT staff)	IT staff with privileged access may become compromised by external attackers	Several time a year	High	Implement segregation of duties to limit staff privileges, Implement regular monitoring and auditing to detect unusual activity.
	Spear phishing	Lack of effective email filtering systems and limited awareness on spear phishing	Thrice a year	Medium/High	Conduct awareness programs to educate IT staff about spear phishing, Deploy advanced email filtering systems that can detect and block spear phishing emails.
	Inadequate security training/knowledge	Lack of related knowledge make IT staff more susceptible to making security mistakes.	Several times a year/occasional	Medium	Provide comprehensive and ongoing security training to IT staff members to ensure they are well-equipped with the necessary knowledge and skills to manage security threats effectively.
	Tailgating	Lack of awareness about the risk of unauthorized individuals gaining physical access to restricted areas by following authorized personnel.	Occasional/Once every few years	Medium/Low	Conduct regular awareness training to educate staff members about the risks of tailgating, Implement strict access control measures, including the use of access cards, biometrics, or security personnel to prevent unauthorized physical access.
	Impersonation attacks	Insufficient verification procedures	Occasional/Once every few years	Medium	Implement strong authentication like multi-factor authentication, Develop strict verification procedures for sensitive transactions or requests.