THE UNIVERSITY OF WINNIPEG

ACS-3921/4921 Assignment 1

Course Name: Computer Security and Privacy

Group: 4

Group members:

Name:	**ID:**
W A Shadman	3132520
Sumeet Kaur Saund	3148723
Noorpreet Gill	3124419
Arshjot Ghuman	3114007
Vi Le	3119710
Austin Chapdelaine	3138187

Instructor: Victor Balogun

Date: 31 January 2023

Abstract

The company suffered a massive data breach where credit cards and company financial information were exfiltrated due to a phishing attack. The company was fined $200 million by Payment Card Industry Data Security Standard (PCI DSS) and Sarbanes-Oxley Act (SOX) for non-compliance with regulatory obligations.

Project Objective

- Our team aims to re-design the detailed network security of the company's data centre in Norwalk.
- Perform the risk analysis.
- Added the regulatory requirements and compliance
- Designing the security policies

Review of Literature

In order to re-design the detailed network diagram of the company's data centre, we have researched the practices and regulatory requirements of PCI DSS in order to protect the company's data and secure it. We also came up with security policies to ensure the security of the network in the company.

SOX and PCI-DSS Compliance and Requirements

SOX:

In a nutshell, the Sarbanes-Oxley Act of 2002 is meant to help protect investors from fraudulent financial reporting by corporations. The SOX Act of 2002, also known as the Corporate Responsibility Act of 2002, mandated significant modifications to current securities rules and levied penalties on offenders.

SOX is a framework that makes it more difficult for CEOs to avoid investigation for data breaches. Organizations must use proven auditing techniques to ensure data integrity and timeliness. These specifications need extensive tracking and system management of critical data.

Reforms took place in four principal areas:

1. Corporate responsibility
2. Increased criminal punishment
3. Accounting regulation
4. New protections

Source:

(*Database Compliance Explained: SOX Vs PCI DSS | DBmaestro*, 2020)

PCI-DSS:

Payment Card Industry Data Security Standard (PCI DSS) is a data security standard for enterprises that deal with branded credit cards from major card schemes. All organizations that store, handle, or transport sensitive authentication data or cardholder data must adhere to the PCI DSS security standard. Consumer protection standards are established by PCI DSS, which also lowers fraud and data breaches throughout the whole payment ecosystem. Any business that handles or accepts credit cards is subject to this standard.

Even if a corporation is PCI-compliant and experiences a data breach, it may still be responsible for paying penalties. However, if the firm in issue has taken all of the necessary procedures to become (and remain) PCI-compliant, the card brands may drastically reduce or even eliminate fines.

PCI DSS compliance involves three main components:

1. Handling the entry of consumer credit card data, namely ensuring that sensitive card information is collected and transmitted securely
2. Data storage is in accordance with the 12 security domains of the PCI standard, which include measures like encryption, constant monitoring, and security testing of access to card data
3. Annual verification of the existence of the necessary security controls, which may use forms, questionnaires, external vulnerability scanning services, and third-party audits

Source:

(*Database Compliance Explained: SOX Vs PCI DSS | DBmaestro*, 2020)

(*What Is PCI DSS Compliance? 12 Requirements | Stripe*, n.d.)

SOX Requirements:

The Sarbanes Oxley Act requires all financial reports to include an Internal Controls Report to show that the company's financial data are accurate and adequate controls are in place to safeguard financial data.

SOX all requires Year-end financial disclosure reports. An independent external SOX auditor is required to review controls, policies, and procedures during an audit. An audit will also look at personnel and may interview staff to confirm that their duties match their job description and that they have the required training to safely access financial information.

A review of a company's internal controls is often the largest component of a SOX compliance audit. Internal controls include all IT assets, including any computers, network hardware, and other electronic equipment that financial data passes through. A SOX IT audit will look at the following internal control items:

SOX sections require the following parameters and conditions must be monitored, logged and audited:

- Internal controls
- Network activity
- Database activity
- Login activity (success and failures)
- Account activity
- User activity
- Information Access

SOX auditing requires that "internal controls and procedures" can be audited using a control framework like COBIT. Log collection and monitoring systems must provide an audit trail of all access and activity to sensitive business information.

A review of a company's internal controls is often the largest component of a SOX compliance audit. Internal controls include all IT assets, including any computers, network hardware, and other electronic equipment that financial data passes through. A SOX IT audit will look at the following internal control items:

IT security: Ensure that proper controls are in place to prevent data breaches and have tools ready to remediate incidents should they occur. Invest in services and equipment that will monitor and protect your financial database.

Access controls: These refer to both the physical and electronic controls that prevent unauthorised users from viewing sensitive financial information. This includes keeping servers and data centres in secure locations, implementing effective password controls, and other measures.

Data backup: Maintain backup systems to protect sensitive data. Data centres containing backed-up data, including those stored off-site or by a third party are also subject to the same SOX compliance requirements as those hosted on-site.

Change management: This involves the IT department process for adding new users and computers, updating and installing new software, and making any changes to databases or other data infrastructure components. Keep records of what was changed, in addition to when it was changed and who changed it.

Requirements for PCI-DSS Compliance:

PCI security standards have technical and operational requirements set by the PCI SSC to protect cardholder data.

PCI DSS has a total of 12 requirements.

1. Install and maintain a firewall configuration to protect cardholder data.

Firewalls are devices that control computer traffic allowed into and out of an organization's network, and into sensitive areas within its internal network. Firewall functionality can also appear in other system components. Establish and implement firewall and router configuration standards that formalize testing whenever configurations change; identify all connections between the cardholder data environment and other networks (including wireless) with documentation and diagrams; that document business justification and various technical settings for each implementation; that diagram all cardholder data flows across systems and networks; and stipulate a review of configuration rule sets at least every six months.

Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment. Prohibit direct public access between the Internet and any system component in the cardholder data environment.

Install personal firewall software or equivalent functionality on any devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the cardholder data environment.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

The easiest way for a hacker to access your internal network is to try default passwords or exploits based on default system software settings in your payment card infrastructure. Far too often, merchants do not change default passwords or settings upon deployment. This is similar to

leaving your store physically unlocked when you go home for the night. Default passwords and settings for most network devices are widely known. This information, combined with hacker tools that show what devices are on your network can make unauthorized entry a simple task if you have failed to change the default settings.

All the vendor-supplied defaults should be changed or removed. Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified. Using strong cryptography, encrypt all non-console administrative access. Maintain an inventory of system components that are in scope for PCI DSS. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

3. Protect stored cardholder data

Cardholder data should not be stored unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored after authorization. If your organization stores PAN, it is crucial to render it unreadable.

Limit cardholder data storage and retention time to that which is required for business, legal, and/ or regulatory purposes, as documented in your data retention policy. Purge unnecessarily stored data at least quarterly. Do not store sensitive authentication data after authorization (even if it is encrypted). Render all sensitive authentication data unrecoverable upon completion of the authorization process. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely.

Mask PAN when displayed (the first six and last four digits are the maximum number of digits you may display), so that only authorized people with a legitimate business need can see more than the first six/last four digits of the PAN. This does not supersede stricter requirements that may be in place for displays of cardholder data, such as on a point-of-sale receipt. Document and implement procedures to protect any keys used for encryption of cardholder data from disclosure and misuse.

4. Encrypt transmission of cardholder data across open, public networks

Cyber criminals may be able to intercept transmissions of cardholder data over open, public networks so it is important to prevent their ability to view this data. Encryption is one technology that can be used to render transmitted data unreadable by any unauthorized person.

Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use

industry best practices to implement strong encryption for authentication and transmission. Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).

5. Protect all systems against malware and regularly update anti-virus software or programs

Malicious software (a.k.a "malware") exploits system vulnerabilities after entering the network via users' e-mail and other online business activities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may supplement (but not replace) anti-virus software. This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). For systems not affected commonly by malicious software, perform periodic evaluations to evaluate evolving malware threats and confirm whether such systems continue to not require anti-virus software. Ensure that all anti-virus mechanisms are kept current, perform periodic scans, and generate audit logs, which are retained per PCI DSS Requirement

6. Develop and maintain secure systems and applications

Security vulnerabilities in systems and applications may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation.

Establish a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g., "high," "medium," or "low") to newly discovered security vulnerabilities. Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. Develop internal and external software applications including web-based administrative access to applications in accordance with PCI DSS and based on industry best practices.

Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and developing applications based on secure coding guidelines – including how sensitive data is handled in memory.

7. Restrict access to cardholder data by business need-to-know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need-to-know and according to job responsibilities. Need to know is when access rights are granted to only the least amount of data and privileges needed to perform a job.

Limit access to system components and cardholder data to only those individuals whose job requires such access. Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

8. Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Requirements apply to all accounts, including point-of-sale accounts, with administrative capabilities and all accounts with access to stored cardholder data. Requirements do not apply to accounts used by consumers (e.g., cardholders).

Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric. Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography.

Use of other authentication mechanisms such as physical security tokens, smart cards, and certificates must be assigned to an individual account. Do not use group, shared, or generic IDs, or other authentication methods. Service providers with access to customer environments must use a unique authentication credential (such as a password/passphrase) for each customer environment.

9. Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems, or hardcopies, and should be appropriately restricted. "Onsite personnel" are full- and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity's premises. "Visitors" are vendors and guests that enter the facility for a short duration – usually up to one day. "Media" is all paper and electronic media containing cardholder data.

Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. Develop procedures to easily distinguish between onsite

personnel and visitors, such as assigning ID badges. Physically secure all media, and store media back-ups in a secure location, preferably off-site. Maintain strict control over the storage and accessibility of media. Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. This includes periodic inspections of POS device surfaces to detect tampering, and training personnel to be aware of suspicious activity.

10. Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is very difficult without system activity logs.

Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including the creation of new accounts, the elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects.

Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, the origination of event, and identity or name of affected data, system component or resource. Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.

11. Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing security controls is especially important for any environmental changes such as deploying new software or changing system configurations.

Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed until passing scans are achieved. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, complete four consecutive quarters of passing scans. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans are conducted after network changes

and internal scans may be performed by internal staff.

Use network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.

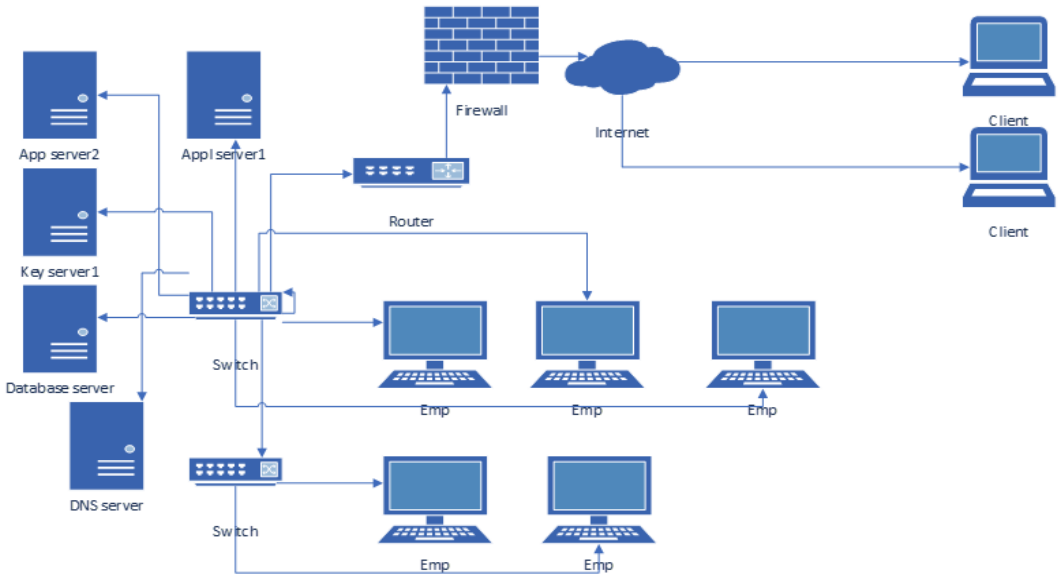
12. Maintain a policy that addresses information security for all personnel

Establish, publish, maintain, and disseminate a security policy; review the security policy at least annually and update it when the environment changes. Implement a risk assessment process that is performed at least annually and upon significant changes to the environment that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment.

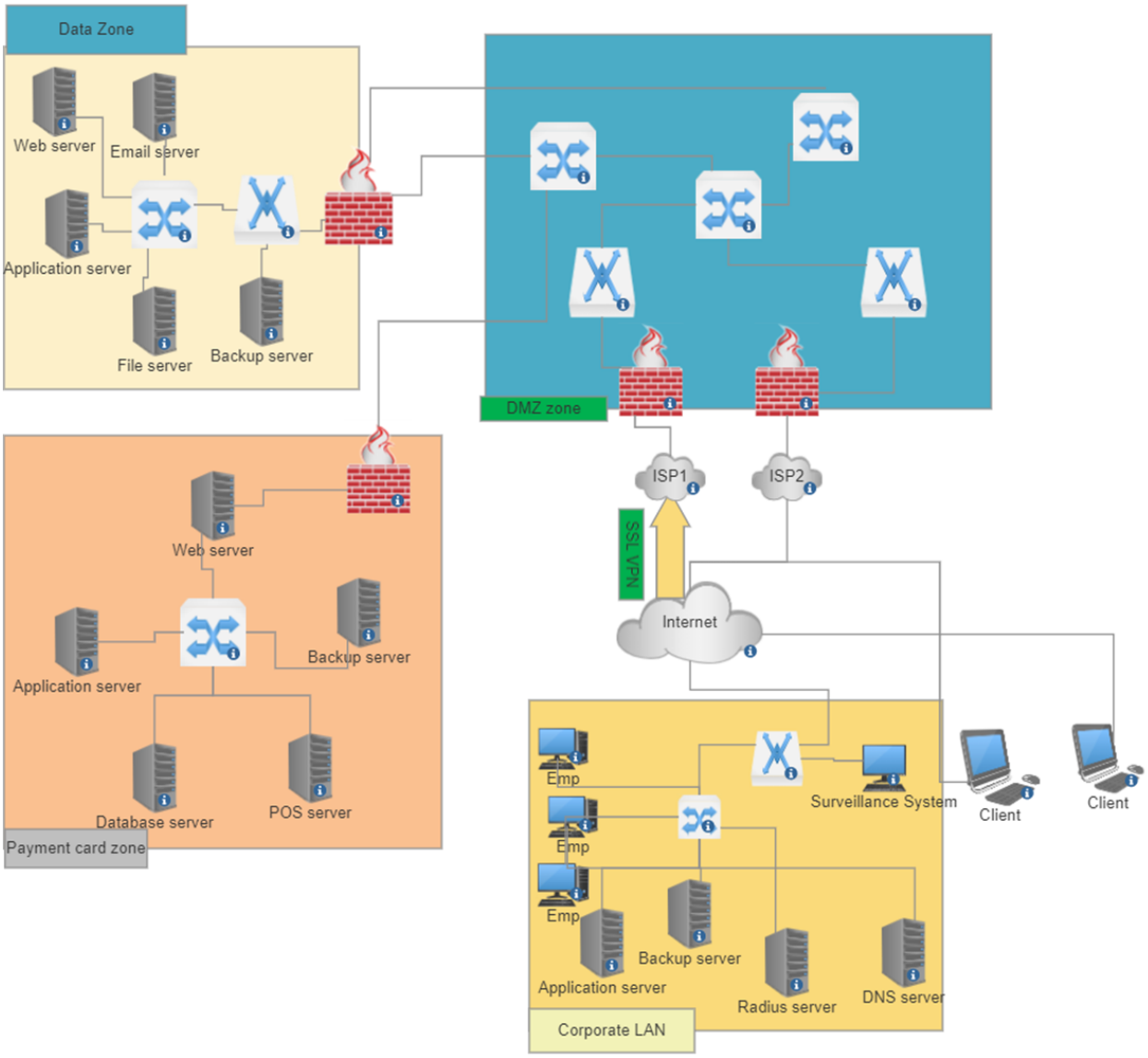
Develop usage policies for critical technologies to define their proper use by all personnel. Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. Service providers must also establish responsibility for their executive management for the protection of cardholder data and a PCI DSS compliance program.

Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures. Implement an incident response plan. Be prepared to respond immediately to a system breach.

Network Design (Before attack)



Network Design (After attack)



Risk Analysis

Asset	Type of Asset	Asset Value	Control Type	Control Family	Countermeasure Cost	CC / AV%	Residual Risk Rating
Application servers	Equipment	640,000 USD	Recovery	Technical	296,000 USD	46.25%	Low
Key Management Servers	Equipment	320,000 USD	Recovery	Technical	148,000 USD	46.25%	Low
Domain Name System Server	Equipment	1600,000 USD	Recovery	Technical	74,000 USD	46.25%	Low
Server OS	Software	22,400 USD	Response	Technical	500 USD	2.23%	Low
Switches	Equipment	280,000 USD	Prevention	Technical	50,000 USD	17.85%	Low
Routers	Equipment	13,600 USD	Prevention	Technical	2,000 USD	14.70%	Low
Firewalls	Software	21,798 USD	Prevention	Technical	5,000 USD	22.93%	Low

Processing Server model: PowerEdge 750XA Server Rack
Server price: 80,000 USD for each server rack including extra fees such as transport, insurance, and installation.
Our company have 4 Application servers and 2 Key Management Servers and 1 DNS servers

(*PowerEdge R750xa Rack Server | Dell USA*, n.d.)

Switch model: N8560-64C
Switch price: 20,000 USD for each switch include extra fee such as transport and insurance
Our company has 14 total switches, two switches for each server, one redundant. (n.d.)

Router model: SG-5105
Router price: 1,700 USD for each router include extra fees such as transport and insurance
Assume our company has 18 routers, each server has two routers and extra 4 routers for redundancy. (n.d.)

Software firewall license name: Fortinet NGFW license
Software firewall license price: 3,114 USD
Our company has firewall software for each server for a total of 7 software firewall licenses.

(*FC-10-00208-950-02-12*, n.d.)

Server OS license name: Window Server Datacenter - 16 cores
Server OS license price: 3,200 USD
All of our company's servers have this OS, the total is 7 Server OS licenses.

(*Windows Server 2022 Datacenter - 16 Core*, n.d.)

4 full-time staff manage all security maintenance of all servers of the company and each employee is paid 120,000 USD annually. On average about 37,000 USD is for maintenance for each server, including employee pay and equipment replacement.

(Ware, 2020)

Security Policies

1) **Physical Workplace Security:**

Facilities used for processing and storing information must have a specified security perimeter, as well as the proper access controls and security obstacles. Access must only be allowed to people after access authorisation has been verified at all physical access points (including specified entry/exit points) to the facilities housing information systems.

To reduce the hazards, certain steps must be taken. Information processing and storage facilities must undergo a periodic risk assessment to ascertain if the controls already in place are effective and whether further physical security measures are required. The types of equipment need to be physically shielded from environmental dangers and security risks. To secure facilities and supporting infrastructure, such as the electrical supply and cabling infrastructure, special controls could also be required. Everyone entering a facility used for information processing or storage, including maintenance staff, must be escorted at all times.

2) **Security Awareness and Training Policy:**

All employees should receive security awareness training so they can effectively carry out their duties and adequately protect corporate information. After completing the program, employees are required to sign a confidentiality agreement and submit documentation of their

success. The management should create the training such that it informs users about the company's security policy.

Goals for the security awareness and training policy should include educating people about the security policy and assisting in understanding how it protects the company, its customers, and its workers. The employees who are in charge of developing and maintaining the training must also be included in the policy. This staff must have the ability to identify technological developments that affect security and the company.

The policy should outline points on workstation maintenance, email and internet access regulations, and staff responsibilities for computer security for all users. A few essential components of security awareness training are recognizing social engineering techniques, minimizing system downtime, and safeguarding sensitive company data.

3) Change Management Policy:

The management, approval, and tracking of modifications to an information system are ensured by the change management policy of the company. The company has to ensure that the changes are implemented with care to have the least possible detrimental effects on the organization's consumers and services.

The processes for planning, evaluating, reviewing, approving, communicating, implementing, documenting, and post-change review are all included in the change management policy. Accurate and timely documentation, ongoing supervision, and a formal, defined approval procedure are all essential components of change management. The SDLC, hardware, software, database, and application changes to system settings, including transfers, additions, and deletions, are covered by the change management policy.

4) Remote Access Policy:

Connecting to the company's network remotely entails using any host. The remote access policy aims to reduce the possible risk of losses brought on by the unapproved usage of resources. All workers should be covered by this policy, which should also contain guidelines for using intranet resources and sending or receiving emails. Disk encryption and VPN access specifications should also be part of the policy.

The prerequisites for onsite access should also apply to remote access. Employees must refrain from using their remote access for illicit purposes, for instance, and must not let unauthorized people use their work equipment. Strong passphrases, logging out when leaving their device alone, and not connecting to other networks while connected to the internal network

should also be required under the policy. They should also mandate that customers use the most recent versions of their operating systems and anti-malware programs.

5) **Password Creation and Management Policy:**

The password generation and management policy offer guidelines on how to create, put into place, and evaluate a defined procedure for correctly establishing, updating, and storing strong and secure passwords used to confirm user identities and get access to corporate systems or information. The policy ought to cover education and knowledge of the value of selecting a strong password. Rules for updating temporary passwords and the dangers of reusing old passwords should be addressed.

The policy should also include minimum standards for password complexity and length. Users should be made aware of the dangers of choosing an easy term or their sensitive information as their password. Any exceptions to the policy, such as software applications or other information systems that have different password requirements, should be noted. The maximum number of retries and password logouts should be mentioned, along with the steps for recording all failed login attempts.

6) **Network Security Policy:**

By adhering to a defined process for conducting an ongoing evaluation of network activity and information system performance, a comprehensive network security policy assures the confidentiality, integrity, and availability of data on a company's systems. Systems must have the proper hardware, software, or procedural auditing measures, according to the policy. Failures to log in, the start-up or shutdown of information, and the use of privileged accounts are all examples of audit events. Anomalies in the firewalls, activity on routers and switches, and devices added or withdrawn from the network are among the other logging entries. Organizations should record information about the action, such as the date, time, and place of origin. The appropriate activities conducted during an auditable event must be specified in the policy, together with who is in charge of what. For instance, IT could resolve an issue before informing the ISO. The policy should make this procedure very clearly.

Depending on the infrastructure of an organization, the Network Security policy may spawn other policies. Other rules can include wireless communication standards, router and switch security, and Bluetooth baseline criteria. All of these regulations ought to provide guidelines for acceptable network access activity.

7) **Access Authorization, Modification, and Identity Access Management:**

Employing access authorisation necessitates that businesses adhere to the Principle of Least Privilege (PoLP). According to this viewpoint, systems and users should only have access to the data they require to do their assigned tasks. A procedure for creating, describing, reviewing, and changing access to systems and sensitive data should be developed and documented by the organization. The common parties involved in this procedure are HR and IT, who grant access upon hiring and termination.

Valid access authorisation, anticipated system usage, and other criteria required by companies must all be taken into account before access is provided. The access authorization policy and password management policy should be followed when creating an access authorization and modification map. Group membership, special rights, temporary or guest accounts, and shared users must all be taken into consideration by HR and IT. As they are essential to protecting user data, these rules and procedures must be continually updated.

8) **Data Retention Policy:**

The data retention policy outlines the kinds of data the company must keep and how long it must keep it. The policy specifies how the data will be kept and disposed of as well. By removing redundant and out-of-date data, this approach will free up additional storage space. Data organization for future use will also be aided by a data retention strategy. Documents, customer records, transactional data, email communications, and contracts are examples of different types of data. For companies that keep sensitive data, this policy is crucial. Organizations' obligations for data retention should be based on regulatory norms.

9) **Encryption Policy**

Any transmission of protected or sensitive data that isn't encrypted must go through an encrypted channel. Protected or sensitive data that has been encrypted may be transmitted through encrypted or unencrypted means. Emails containing protected data or sensitive data must be encrypted since all conversations involving email addresses outside of the organization use an unencrypted channel. If the encryption method requires a password, it must be given to the recipient using a different channel, for as by calling and leaving the password on the caller's voicemail. It is never permitted to include the password in an email message that also contains encrypted data.

Sensitive cardholder data must always be protected during transmission over open, public networks using robust cryptography and security protocols, ensuring that only trusted keys and certificates are accepted, the protocol being used only supports secure versions or configurations, and the encryption strength is appropriate for the encryption methodology being used.

Data that is intended to be transferred physically, either wholly within the organisation or a third party, must be encrypted before being stored on a medium, such as a CD, DVD, or portable drive. It is not advised to archive the protected or sensitive material on a physical medium, although it is allowed, provided the data is encrypted. All archiving ought to be done digitally so that it may be backed up by ITS and kept in a secure data centre.

On all cited computers and electronic devices covered by this Policy, ITs will install software that can encrypt the full hard drive. Users that need encryption software should get in touch with ITs to set up installation.

10) System Maintenance Policy:

To perform activities, including transactions on a daily basis, maintenance of the system is also required when necessary to ensure effective operations and troubleshooting. The main objective is this policy to define the roles, responsibilities and critical elements for the efficient operations and support of the IT system at the institution/organization. Planning, performing, archiving, and checking on records of upkeep and fixing data framework parts as per the producer or vendor details or potentially authoritative prerequisites. Endorsement and checking of all maintenance activities, whether performed nearby or from a distance and whether the hardware is repaired on-site or taken to another location; Necessities that an assigned association official expressly supports the expulsion of the data framework or framework parts from authoritative offices for off-site upkeep or fixes; Cleaning hardware to eliminate all data from related media before expulsion from authoritative offices for off-site upkeep or fixes; Checking all possibly affected security controls to confirm that the controls are as yet working appropriately following support or fix activities; Remembering the suitable upkeep-related data for hierarchical upkeep records. Requiring that the non-accompanied workforce perform upkeep on the data framework has required admittance approvals and assigning authoritative faculty with expected admittance approvals and specialized capability to direct the support exercises of the workforce who try not to have access approvals.

11) Vulnerability Management Policy:

There must be at least quarterly vulnerability scans of the internal and external networks, or after any substantial network changes. Failures from vulnerability scans that were evaluated as Critical or High will be remedied, and then rescanned, until all risks were eliminated. During vulnerability scanning, any indication of a compromised or exploited information resource must be notified to the (District/Organization) information security officer and IT support. Configuration guidelines will be updated as soon as new vulnerabilities are found.

Source: (Security, n.d.)

Zero-Trust Case

As a potential vector of attack and at risk of phishing, our company should be doing more to monitor and authenticate remote employee devices. By adopting a zero-trust model, we can limit the impact of future breaches by reducing the attacker's lateral movement. All users are not trusted by default, and any access to company systems must be monitored and authenticated beforehand. Examples of common policies are multifactor authentication and checking device identity. Once they have access, users are limited to roles that restrict access to only essential information, employing the least privilege principle.

The zero-trust model assumes breach, so let's review what would happen if that same attack occurred. The attacker would first need to have a company-recognized device and multifactor authentication credentials to access the company network. If they manage to gain access, their options to execute a lateral attack are limited due to the role the user has. All requests for data access are controlled and encrypted in transit. Their access to other systems in our company is both limited and monitored, providing network administrators to prevent any further attacks on other systems. This will lessen the impact of future attacks while letting employees stay remote.

Bibliography:

PCI Security Standards Council. (n.d.). Retrieved January 28, 2023, from https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

sarbanes oxley. Sarbanes. (n.d.). Retrieved January 28, 2023, from https://www.sarbanes-oxley-101.com/sarbanes-oxley-audits.htm#:~:text=The%20Sarbanes%20Oxley%20Act%20requires,reports%20are%20also%20a%20requirement

Virginia State University. (2017, August 29). *Policy 6410 system maintenance - virginia state university*. VSU.edu. Retrieved January 29, 2023, from https://www.vsu.edu/files/docs/policies/6000/policy-6410-system-maintenance.pdf

Database Compliance Explained: SOX vs PCI DSS | DBmaestro. (2020, June 17). DBmaestro. Retrieved January 30, 2023, from https://www.dbmaestro.com/blog/database-compliance-automation/explained-sox-vs-pci-dss

What is PCI DSS compliance? 12 requirements | Stripe. (n.d.). What Is PCI DSS Compliance? 12 Requirements | Stripe. Retrieved January 30, 2023, from https://stripe.com/en-ca/guides/pci-compliance

Security, A. (n.d.). *10 Must Have IT Security Policies for Every Organization*. Adsero Security. Retrieved January 30, 2023, from https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/

Vulnerability Management Policy | August 02, 2022 | SecurityStudio | Retrieved January 30, 2023 from https://securitystudio.com/policy-templates/vulnerability-management-policy/#:~:text=Purpose,the%20risks%20associated%20with%20them.

Loyola University Chicago | 2015 | Encryption Policy: Information Technology Services: Loyola University Chicago | Retrieved January 2023 from https://www.luc.edu/its/aboutits/itspoliciesguidelines/encryption.shtml

PowerEdge R750xa Rack Server | Dell USA. (n.d.). Dell. Retrieved January 30, 2023, from https://www.dell.com/en-us/shop/dell-poweredge-servers/poweredge-r750xa-rack-server/spd/poweredge-r750xa/pe_r750xa_14823_vi_vp

F. (n.d.). *FS 64-Port 100Gb L3 Stackable Data Center Spine Switch - FS*. FS.com. Retrieved January 30, 2023, from https://www.fs.com/products/110481.html

F. (n.d.). *SG-5105 All in One Multi-WAN Security Gateway with 8 Gigabit Ethernet (GbE) Ports, 1x SFP, 1x SFP+, Up to 10 Gigabit WAN Ports, Built-in WLAN Controller, SPI Firewall, Routing, Load Balancing, IPSec/L2TP VPN and DoS Defense Supported - FS*. FS.com. Retrieved January 30, 2023, from https://www.fs.com/products/115393.html

FC-10-00208-950-02-12. (n.d.). FortiGate 201E License FC-10-00208-950-02-12 Price - 1 Year UTM License for Fortigate FG-201E. Retrieved January 30, 2023, from https://www.router-switch.com/fc-10-00208-950-02-12.html

Windows Server 2022 Datacenter - 16 Core. (n.d.). Recycled Software. Retrieved January 30, 2023, from https://shop.recycled-software.com/product/windows-server-2022-datacenter-16-core/

Ware, A. (2020, May 18). *The Hidden Costs of High-Performance Storage Ownership*. HPCwire. Retrieved January 30, 2023, from https://www.hpcwire.com/2020/05/18/the-hidden-costs-of-high-performance-storage-ownership/