Assigment 2

Information Assurance: Octave Approach in an Organization



**GROUP MEMBERS:**

ZEESHAN MALIK (F2021408013)

UZAIR SOHAIL (F2021408002)

AMIR HAMZA (F2021408037)

**SUBMITTED TO:**

MAM NOSHEEN

**Introduction to Organization:**

Samin Textiles Limited is a weaving unit with an average annual production capacity of 27.00 million running meters of the best quality greige cloth based on three shifts a day and 360 working days per annum.

At its inception Samin was primarily involved with the manufactured of narrow width commodity textiles that were easy to produce and easy to sell in the export market.

The narrow width business has seen a significant change in the product mix as well as the targeted customers. From simple twills and drills, Samin has shifted to the manufacture of specialized and niche items such as abrasive fabric for industrial use, mechanical stretch items for specialized work wear and corduroy and dyed-yarn fabric for the high-end fashion market.

With these changes in product range, so has the customer base shifted from the Far-East to Europe and whenever else in the world our top-quality fabric required.

Furthermore, in June 2022 the Company has expanded its production capacity by adding further 25 Picanol Airjet Omni Plus weaving machines, one knotting Machine and one Overhead Cleaner. Air supply for weaving machines has been reinforced with an additional Air Compressor from Cameron USA during the month of October 2023. As such the production capacity of the existing plant has increased by almost 20% from November 2022.

Over a period of twenty-four years of its existence, Samin has established itself as an internationally renowned greige fabric specialist giving priority to quality and un-paralleled service.

Samin has its own gas fired generators for prime source of electricity and WAPDA connection for backup source of power.

The Board of Directors of the Company comprises of the leading business / professionals of Pakistan.

Mr. Sarmad Amin Chairman

Mr. Jehanzeb Amin Chief Executive

Mr. Safder Hussain Tariq Director

Mr. Tariq Ali Director

Mr. Tariq Jillani Director

Mr. Salman Chaudyary Director

Mr. Jamil Masud Director

**Phase 1: Build Asset Based Threat Profiles**

**1. Identify Senior Management Knowledge:**

**Senior Management's View of Assets:**

* Tangible assets: IT infrastructure, servers, databases.
* Intangible assets: Intellectual property, customer data, financial records.

**Areas of Concern:**

* Ensuring confidentiality, integrity, and availability of critical assets.
* Compliance with industry standards and regulations.
* Mitigating risks related to cyber threats and data breaches.

**Security Requirements:**

* Robust encryption protocols for sensitive data.
* Access controls to limit unauthorized access.
* Regular security audits and assessments.

**Current Security Practices:**

* Encryption of sensitive data.
* Implementing multi-factor authentication.
* Conducting regular security training for employees.

**Current Organizational Vulnerabilities:**

* Lack of comprehensive incident response plan.
* Vulnerabilities in outdated software.
* Insider threats due to negligent or malicious employees.

**2. Identify Operational Area Management Knowledge:**

**Operational Area Management's View of Assets:**

* Operational systems: ERP systems, production databases.
* Customer-facing applications: E-commerce platforms, customer support portals.

**Areas of Concern:**

* Ensuring uptime and reliability of operational systems.
* Protecting customer data from unauthorized access.
* Mitigating risks associated with third-party integrations.

**Security Requirements:**

* Continuous monitoring of network traffic.
* Regular backups and disaster recovery plans.
* Secure coding practices for in-house applications.

**Current Security Practices:**

* Implementing firewalls and intrusion detection systems.
* Conducting penetration testing on critical systems.
* Enforcing strict access controls for sensitive data.

**Current Organizational Vulnerabilities:**

* Dependency on legacy systems vulnerable to exploits.
* Lack of patch management for software vulnerabilities.
* Inadequate training for employees on security best practices.

**3. Identify Staff Knowledge:**

**Staff's View of Assets:**

* Personal workstations: laptops, desktops.
* Access to corporate networks and data repositories.

**Areas of Concern:**

* Ensuring secure handling of sensitive information.
* Avoiding social engineering attacks and phishing attempts.
* Reporting security incidents promptly.

**Security Requirements:**

* Strong password policies.
* Security awareness training.
* Secure remote access protocols.

**Current Security Practices:**

* Regular software updates and patches.
* Use of virtual private networks (VPNs) for remote access.
* Awareness campaigns on phishing and social engineering tactics.

**Current Organizational Vulnerabilities:**

* Use of unsecured personal devices for work purposes.
* Lack of encryption for data in transit.
* Insufficient monitoring of employee activities on corporate networks.

**4. Create Threat Profile:**

**Critical Assets:**

1. Customer Database containing personally identifiable information (PII).
2. Production servers hosting mission-critical applications.

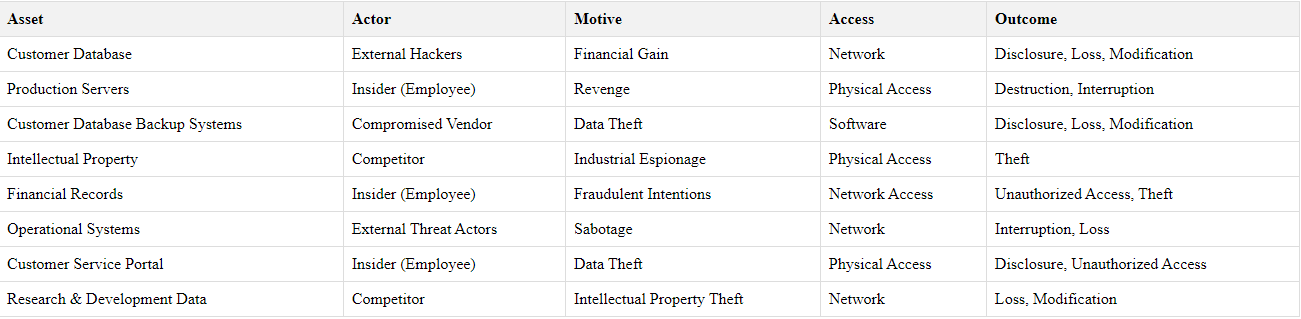
**Security Requirements for Critical Assets:**

* Encryption of PII data.
* Role-based access control for production servers.
* Regular data backups and disaster recovery plans.

**Threats to Critical Assets:**

1. External Cyber Attack:
   * Actor: Sophisticated hacking group.
   * Motive: Financial gain or espionage.
   * Access: Network intrusion through phishing or malware.
   * Outcome: Data breach or service disruption.
2. Insider Threat:
   * Actor: Disgruntled employee.
   * Motive: Revenge or sabotage.
   * Access: Authorized network access.
   * Outcome: Unauthorized data access or deletion.
3. Supply Chain Attack:
   * Actor: Compromised vendor or supplier.
   * Motive: Access to sensitive data or systems.
   * Access: Through compromised software or hardware.
   * Outcome: Compromise of critical systems or data leakage.

**Threat Profile:**



**Phase 2: Identify Key Components**

**1. Identify Key Components:**

**Hardware:**

* **Servers:** These critical components host essential applications and databases, serving as the backbone of the organization's IT infrastructure. They store and process data vital for business operations.
* **Network Devices:** Routers, switches, and firewalls form the core network infrastructure. Routers facilitate communication between different networks, switches enable devices within a network to communicate, and firewalls enforce network security policies, controlling incoming and outgoing traffic.

**Software:**

* **Operating Systems:** Windows Server and Linux are foundational operating systems that power servers and provide the environment for running applications and services. They manage hardware resources and provide essential functionalities.
* **Databases:** MySQL and Oracle are widely used relational database management systems (RDBMS) for storing and managing structured data. They play a crucial role in storing and retrieving information for various applications.
* **Applications:** Custom-built or third-party applications are used to support business operations, ranging from enterprise resource planning (ERP) systems to customer relationship management (CRM) software. These applications automate processes and facilitate efficient workflow management.

**Networking Equipment:**

* **Firewalls:** Firewalls are essential security appliances that monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between a trusted internal network and untrusted external networks, protecting against unauthorized access and cyber threats.
* **Intrusion Detection Systems (IDS):** IDS are security appliances or software solutions designed to detect and respond to suspicious network activity or potential security breaches. They analyze network traffic patterns and alert administrators to potential security incidents, helping to mitigate risks and protect critical assets.

**2. Technology Vulnerabilities:**

**Design Vulnerability:**

* Design vulnerabilities stem from flaws in the architectural design of software or hardware components. For example, the lack of input validation in custom applications may allow attackers to exploit vulnerabilities and execute arbitrary code, leading to unauthorized access or data breaches.

**Implementation Vulnerability:**

* Implementation vulnerabilities arise from errors introduced during the coding or integration of software components. For instance, buffer overflow vulnerabilities in software applications may occur due to improper input validation, potentially leading to system crashes or remote code execution by attackers.

**Configuration Vulnerability:**

* Configuration vulnerabilities result from weaknesses in the setup or configuration of hardware or software components. Default passwords or misconfigured access control lists (ACLs) on network devices may create security gaps that can be exploited by attackers to gain unauthorized access to sensitive systems or data.

**3. Evaluate Selected Components:**

**Running Vulnerability Analysis Tools:**

* Utilizing advanced vulnerability assessment tools like Nessus or OpenVAS allows for comprehensive scanning of selected components to identify potential security vulnerabilities. These tools perform automated scans to detect missing patches, misconfigurations, or outdated software versions, providing valuable insights into the security posture of the IT infrastructure.

**Reviewing Technology Vulnerabilities:**

* Thorough analysis of vulnerability assessment reports enables the prioritization of risks based on severity and potential impact on critical assets. By reviewing and interpreting the findings, organizations can develop effective mitigation strategies and remediation plans to address identified vulnerabilities and strengthen overall security defenses.

**Phase 3: Develop Security Strategy and Plans**

**1. Conduct Risk Analysis:**

**Identifying the Impact of Threats to Critical Assets:**

* Assess the potential consequences of identified threats on critical assets, such as servers, databases, and network infrastructure.
* Consider factors like confidentiality, integrity, and availability to determine the severity of each threat scenario.

**Creating Risk Evaluation Criteria:**

* Establish criteria for evaluating and prioritizing risks based on their impact on critical assets, likelihood of occurrence, and potential harm to the organization.
* Define risk tolerance levels and thresholds to guide decision-making and resource allocation.

**Evaluating the Impact of Threats to Critical Assets:**

* Apply the risk evaluation criteria to assess the impact of identified threats on critical assets.
* Quantify the potential loss or damage resulting from each threat scenario and prioritize risks based on their significance to the organization's objectives and operations.

**2. Develop Protection Strategy:**

**Designing Measures to Mitigate Identified Risks:**

* Develop strategies and countermeasures to address identified risks and vulnerabilities identified in Phase 2.
* This may include implementing technical controls such as encryption, access controls, and intrusion detection systems, as well as administrative controls such as policies, procedures, and training programs.

**Implementing Security Controls and Safeguards:**

* Deploy security controls and safeguards to protect critical assets from identified threats.
* Ensure that security measures are aligned with the organization's risk management objectives and compliance requirements.
* Monitor and update security controls regularly to adapt to evolving threats and vulnerabilities.

**Developing Incident Response and Recovery Plans:**

* Establish incident response and recovery plans to effectively respond to security incidents and minimize their impact on critical assets.
* Define roles and responsibilities, escalation procedures, and communication protocols.
* Conduct regular exercises and drills to test the effectiveness of incident response procedures and enhance preparedness.