The scenario is as follows, you are being asked to compose 5 critical “information asset risk

worksheets” for a chosen organization. The organization can be an existing company which you

are/were working for, or you may create a made-up scenario. You also have the option of

choosing SLIIT as your organization. However you will not get access to internal technical

information and therefore the components have to be made-up by yourself. Note the scale of the

organization is irrelevant, although your choice of organization will affect the number of potential

threats.

Consider the suitable and popular organization in Sri Lanka for that

Can use (SLT Mobitel) for that. If so give me all the necessary information for that with five Information Asset Risk Worksheet

Mobitel**1**

Certainly, let's create a scenario for "SLT Mobitel," a well-known telecommunications company in Sri Lanka. SLT Mobitel provides a wide range of telecommunications services, including mobile, fixed-line, internet, and digital solutions. Here are five critical information asset risk worksheets for SLT Mobitel:

---

\*Information Asset Risk Worksheet 1:\*

Organization Name: SLT Mobitel

Asset Name: Customer Personal Data

Asset Description: This includes customer names, contact details, billing information, call records, and internet usage history.

Threats:

1. Unauthorized Access: Unauthorized individuals gaining access to customer personal data.

2. Data Breach: Unauthorized disclosure or theft of customer personal information.

3. Insider Threats: Malicious actions or data breaches by current or former employees.

4. Phishing Attacks: Attempts to trick employees into revealing customer data.

5. Denial of Service (DoS) Attacks: Disruption of services affecting data security.

Risk Level (1-5):

1. Unauthorized Access: 4

2. Data Breach: 4

3. Insider Threats: 3

4. Phishing Attacks: 3

5. DoS Attacks: 2

Current Controls:

- Encryption of sensitive customer data.

- Access controls and authentication for customer databases.

- Employee training on security awareness and identifying phishing attempts.

Recommended Actions:

1. Enhance access controls and monitoring for customer databases.

2. Regularly audit and review access permissions.

3. Implement advanced threat detection and prevention mechanisms.

4. Conduct regular security awareness training for employees.

5. Develop a robust incident response plan.

---

\*Information Asset Risk Worksheet 2:\*

Organization Name: SLT Mobitel

Asset Name: Network Infrastructure

Asset Description: This includes the physical and digital infrastructure supporting SLT Mobitel's telecommunications services.

Threats:

1. DDoS Attacks: Distributed denial of service attacks targeting network availability.

2. Infrastructure Outages: Physical damage or technical failures affecting network reliability.

3. Unauthorized Access: Intrusions into critical network infrastructure components.

4. Data Exfiltration: Unauthorized extraction of sensitive network configuration data.

5. Insider Threats: Malicious actions by employees targeting network infrastructure.

Risk Level (1-5):

1. DDoS Attacks: 4

2. Infrastructure Outages: 3

3. Unauthorized Access: 4

4. Data Exfiltration: 3

5. Insider Threats: 2

Current Controls:

- Firewalls and intrusion detection systems.

- Redundant infrastructure and backup power systems.

- Regular vulnerability assessments and penetration testing.

Recommended Actions:

1. Enhance DDoS mitigation capabilities.

2. Implement real-time network monitoring and incident response procedures.

3. Strengthen physical security for critical infrastructure sites.

4. Enhance employee training on network security.

5. Develop and test disaster recovery plans.

---

\*Information Asset Risk Worksheet 3:\*

Organization Name: SLT Mobitel

Asset Name: Customer Billing Systems

Asset Description: This system manages customer billing, invoices, and payment processing.

Threats:

1. Unauthorized Access: Unauthorized individuals gaining access to billing systems and potentially manipulating customer invoices.

2. Data Breach: Unauthorized disclosure or theft of customer billing data.

3. Insider Threats: Malicious actions or data breaches by current or former employees.

4. Billing Errors: Accidental or intentional billing errors leading to financial losses.

5. Phishing Attacks: Attempts to trick employees into revealing billing system access.

Risk Level (1-5):

1. Unauthorized Access: 4

2. Data Breach: 4

3. Insider Threats: 3

4. Billing Errors: 2

5. Phishing Attacks: 3

Current Controls:

- Access controls and authentication for billing systems.

- Regular reconciliation and audit of billing records.

- Employee training on identifying and reporting phishing attempts.

Recommended Actions:

1. Enhance access controls and monitoring for billing systems.

2. Implement automated billing error detection mechanisms.

3. Conduct regular security awareness training for employees.

4. Enhance data encryption for billing data.

5. Establish a process for reporting and correcting billing errors.

---

\*Information Asset Risk Worksheet 4:\*

Organization Name: SLT Mobitel

Asset Name: Employee Personal Data

Asset Description: This includes HR records, social security numbers, and other personal information of employees.

Threats:

1. Unauthorized Access: Unauthorized individuals gaining access to employee personal data.

2. Data Breach: Unauthorized disclosure or theft of employee personal information.

3. Insider Threats: Malicious actions or data breaches by current or former employees.

4. Phishing Attacks: Attempts to trick employees into revealing personal data.

5. Employee Data Leakage: Accidental sharing of employee personal data.

Risk Level (1-5):

1. Unauthorized Access: 3

2. Data Breach: 3

3. Insider Threats: 4

4. Phishing Attacks: 2

5. Employee Data Leakage: 2

Current Controls:

- Access controls and authentication for employee data systems.

- Employee training on security awareness and identifying phishing attempts.

- Data access auditing and monitoring.

Recommended Actions:

1. Enhance access controls and monitoring for employee data systems.

2. Conduct regular access audits and review access permissions.

3. Implement data loss prevention measures.

4. Strengthen employee training on data protection.

5. Develop incident response procedures for data breaches involving employee data.

---

\*Information Asset Risk Worksheet 5:\*

Organization Name: SLT Mobitel

Asset Name: Customer Support Systems

Asset Description: These systems manage customer support requests, including technical support and issue resolution.

Threats:

1. Unauthorized Access: Unauthorized individuals gaining access to customer support systems.

2. Data Manipulation: Unauthorized modification of customer support tickets.

3. Insider Threats: Malicious actions or data breaches by current or former employees.

4. Service Interruption: Disruption of customer support systems affecting service quality.

5. Phishing Attacks: Attempts to trick employees into revealing access to support systems.

Risk Level (1-5):

1. Unauthorized Access: 3

2. Data Manipulation: 2

3. Insider Threats: 3

4. Service Interruption: 3

5. Phishing Attacks: 2

Current Controls:

- Access controls and authentication for support systems.

- Regular monitoring of support ticket activity.

- Employee training on security awareness and identifying phishing attempts.

Recommended Actions:

1. Enhance access controls and monitoring for support systems.

2. Implement data integrity checks for support tickets.

3. Conduct regular security awareness training for employees.

4. Establish backup systems for uninterrupted customer support.

5. Enhance incident response procedures for support system security incidents.

These information asset risk worksheets will serve as a starting point for assessing and mitigating risks to critical information assets within SLT Mobitel. Each worksheet will require ongoing monitoring and updates to ensure the organization remains resilient against evolving threats.

Mobitel**2**

**Certainly, let's create a scenario for "SLT Mobitel Corporation," a prominent telecommunications company in Sri Lanka. SLT Mobitel offers various telecommunications services, including mobile, fixed-line, internet, and digital solutions. Here are five critical information asset risk worksheets for SLT Mobitel Corporation:**

**---**

**\*Information Asset Risk Worksheet 1:\***

**Organization Name: SLT Mobitel Corporation**

**Asset Name: Customer Personal Data**

**Asset Description: This includes customer names, contact details, billing information, call records, and internet usage history.**

**Threats:**

**1. Unauthorized Access: Unauthorized individuals gaining access to customer personal data.**

**2. Data Breach: Unauthorized disclosure or theft of customer personal information.**

**3. Insider Threats: Malicious actions or data breaches by current or former employees.**

**4. Phishing Attacks: Attempts to trick employees into revealing customer data.**

**5. Denial of Service (DoS) Attacks: Disruption of services affecting data security.**

**Risk Level (1-5):**

**1. Unauthorized Access: 4**

**2. Data Breach: 4**

**3. Insider Threats: 3**

**4. Phishing Attacks: 3**

**5. DoS Attacks: 2**

**Current Controls:**

**- Encryption of sensitive customer data.**

**- Access controls and authentication for customer databases.**

**- Employee training on security awareness and identifying phishing attempts.**

**Recommended Actions:**

**1. Enhance access controls and monitoring for customer databases.**

**2. Regularly audit and review access permissions.**

**3. Implement advanced threat detection and prevention mechanisms.**

**4. Conduct regular security awareness training for employees.**

**5. Develop a robust incident response plan.**

**---**

**\*Information Asset Risk Worksheet 2:\***

**Organization Name: SLT Mobitel Corporation**

**Asset Name: Network Infrastructure**

**Asset Description: This includes the physical and digital infrastructure supporting SLT Mobitel's telecommunications services.**

**Threats:**

**1. DDoS Attacks: Distributed denial of service attacks targeting network availability.**

**2. Infrastructure Outages: Physical damage or technical failures affecting network reliability.**

**3. Unauthorized Access: Intrusions into critical network infrastructure components.**

**4. Data Exfiltration: Unauthorized extraction of sensitive network configuration data.**

**5. Insider Threats: Malicious actions by employees targeting network infrastructure.**

**Risk Level (1-5):**

**1. DDoS Attacks: 4**

**2. Infrastructure Outages: 3**

**3. Unauthorized Access: 4**

**4. Data Exfiltration: 3**

**5. Insider Threats: 2**

**Current Controls:**

**- Firewalls and intrusion detection systems.**

**- Redundant infrastructure and backup power systems.**

**- Regular vulnerability assessments and penetration testing.**

**Recommended Actions:**

**1. Enhance DDoS mitigation capabilities.**

**2. Implement real-time network monitoring and incident response procedures.**

**3. Strengthen physical security for critical infrastructure sites.**

**4. Enhance employee training on network security.**

**5. Develop and test disaster recovery plans.**

**---**

**\*Information Asset Risk Worksheet 3:\***

**Organization Name: SLT Mobitel Corporation**

**Asset Name: Billing and Payment Systems**

**Asset Description: These systems manage customer billing, payments, and financial transactions.**

**Threats:**

**1. Unauthorized Access: Unauthorized access to financial data and customer accounts.**

**2. Payment Fraud: Unauthorized or fraudulent transactions.**

**3. Insider Threats: Malicious actions by employees targeting financial systems.**

**4. Data Corruption: Accidental or intentional data loss or manipulation.**

**5. Phishing Attacks: Attempts to manipulate customers or employees into fraudulent transactions.**

**Risk Level (1-5):**

**1. Unauthorized Access: 4**

**2. Payment Fraud: 4**

**3. Insider Threats: 3**

**4. Data Corruption: 2**

**5. Phishing Attacks: 3**

**Current Controls:**

**- Strong authentication and authorization for financial systems.**

**- Regular auditing and monitoring of financial transactions.**

**- Employee training on recognizing and reporting suspicious activities.**

**Recommended Actions:**

**1. Implement multi-factor authentication for financial system access.**

**2. Enhance transaction monitoring and anomaly detection.**

**3. Conduct regular employee background checks and access audits.**

**4. Implement data integrity checks and backups for financial data.**

**5. Conduct anti-phishing awareness campaigns for employees and customers.**

**---**

**\*Information Asset Risk Worksheet 4:\***

**Organization Name: SLT Mobitel Corporation**

**Asset Name: Network Customer Service Portal**

**Asset Description: This web portal allows customers to access their account information, submit service requests, and manage their services.**

**Threats:**

**1. Unauthorized Access: Unauthorized individuals gaining access to customer accounts and information.**

**2. Data Leakage: Accidental or intentional sharing of customer data with unauthorized parties.**

**3. Insider Threats: Malicious actions or data breaches by current or former employees.**

**4. Web Application Vulnerabilities: Exploitable vulnerabilities in the customer portal.**

**5. Phishing Attacks: Attempts to trick customers into revealing account credentials.**

**Risk Level (1-5):**

**1. Unauthorized Access: 4**

**2. Data Leakage: 3**

**3. Insider Threats: 3**

**4. Web Application Vulnerabilities: 4**

**5. Phishing Attacks: 3**

**Current Controls:**

**- Strong authentication and encryption for the customer portal.**

**- Regular security testing and patching of the portal.**

**- Employee training on recognizing phishing attempts.**

**Recommended Actions:**

**1. Implement continuous security testing and vulnerability scanning.**

**2. Enhance access controls and account recovery procedures.**

**3. Monitor for unusual account activities and implement alerts.**

**4. Train employees on secure coding practices.**

**5. Conduct phishing simulation exercises for employees.**

**---**

**\*Information Asset Risk Worksheet 5:\***

**Organization Name: SLT Mobitel Corporation**

**Asset Name: Employee Personal Information**

**Asset Description: This includes HR records, payroll information, and other personal data of employees.**

**Threats:**

**1. Unauthorized Access: Unauthorized access to sensitive employee data.**

**2. Data Breach: Unauthorized disclosure or theft of employee personal information.**

**3. Insider Threats: Malicious actions or data breaches by current or former employees.**

**4. Data Corruption: Accidental or intentional deletion or manipulation of employee data.**

**5. Phishing Attacks: Attempts to trick employees into revealing personal information.**

**Risk Level (1-5):**

**1. Unauthorized Access: 4**

**2. Data Breach: 4**

**3. Insider Threats: 3**

**4. Data Corruption: 2**

**5. Phishing Attacks: 3**

**Current Controls:**

**- Access controls and encryption for employee data.**

**- Employee training on security awareness and identifying phishing attempts.**

**- Regular audits of employee data access.**

**Recommended Actions:**

**1. Strengthen access controls and monitor access to employee data.**

**2. Conduct regular employee background checks and access audits.**

**3. Implement data integrity checks and backups for HR records.**

**4. Enhance employee training on secure handling of personal information.**

**5. Conduct anti-phishing awareness campaigns for employees.**

**These information asset risk worksheets will serve as a starting point for assessing and mitigating risks to critical information assets within SLT Mobitel Corporation. Each worksheet will require ongoing monitoring and updates to ensure the organization remains resilient against evolving threats.**

Mobitel**3**

Certainly, let's create a scenario for "SLT Mobitel," a well-known telecommunications company in Sri Lanka. SLT Mobitel offers a wide range of telecommunications services, including mobile, fixed-line, internet, and digital solutions. Here are five critical information asset risk worksheets for SLT Mobitel:

---

\*Information Asset Risk Worksheet 1:\*

Organization Name: SLT Mobitel

Asset Name: Customer Personal Data

Asset Description: This includes customer names, contact details, billing information, call records, and internet usage history.

Threats:

1. Unauthorized Access: Unauthorized individuals gaining access to customer personal data.

2. Data Breach: Unauthorized disclosure or theft of customer personal information.

3. Insider Threats: Malicious actions or data breaches by current or former employees.

4. Phishing Attacks: Attempts to trick employees into revealing customer data.

5. Denial of Service (DoS) Attacks: Disruption of services affecting data security.

Risk Level (1-5):

1. Unauthorized Access: 4

2. Data Breach: 4

3. Insider Threats: 3

4. Phishing Attacks: 3

5. DoS Attacks: 2

Current Controls:

- Encryption of sensitive customer data.

- Access controls and authentication for customer databases.

- Employee training on security awareness and identifying phishing attempts.

Recommended Actions:

1. Enhance access controls and monitoring for customer databases.

2. Regularly audit and review access permissions.

3. Implement advanced threat detection and prevention mechanisms.

4. Conduct regular security awareness training for employees.

5. Develop a robust incident response plan.

---

\*Information Asset Risk Worksheet 2:\*

Organization Name: SLT Mobitel

Asset Name: Network Infrastructure

Asset Description: This includes the physical and digital infrastructure supporting SLT Mobitel's telecommunications services.

Threats:

1. DDoS Attacks: Distributed denial of service attacks targeting network availability.

2. Infrastructure Outages: Physical damage or technical failures affecting network reliability.

3. Unauthorized Access: Intrusions into critical network infrastructure components.

4. Data Exfiltration: Unauthorized extraction of sensitive network configuration data.

5. Insider Threats: Malicious actions by employees targeting network infrastructure.

Risk Level (1-5):

1. DDoS Attacks: 4

2. Infrastructure Outages: 3

3. Unauthorized Access: 4

4. Data Exfiltration: 3

5. Insider Threats: 2

Current Controls:

- Firewalls and intrusion detection systems.

- Redundant infrastructure and backup power systems.

- Regular vulnerability assessments and penetration testing.

Recommended Actions:

1. Enhance DDoS mitigation capabilities.

2. Implement real-time network monitoring and incident response procedures.

3. Strengthen physical security for critical infrastructure sites.

4. Enhance employee training on network security.

5. Develop and test disaster recovery plans.

---

\*Information Asset Risk Worksheet 3:\*

Organization Name: SLT Mobitel

Asset Name: Billing and Payment Systems

Asset Description: Systems responsible for customer billing, payment processing, and financial transactions.

Threats:

1. Unauthorized Access: Unauthorized individuals gaining access to billing and payment systems.

2. Payment Fraud: Unauthorized transactions or fraudulent fund transfers.

3. Data Corruption: Accidental or intentional deletion or modification of billing data.

4. Insider Threats: Malicious actions or data breaches by employees.

5. Phishing Attacks: Attempts to trick employees into revealing payment-related data.

Risk Level (1-5):

1. Unauthorized Access: 4

2. Payment Fraud: 3

3. Data Corruption: 2

4. Insider Threats: 3

5. Phishing Attacks: 3

Current Controls:

- Strong access controls and encryption for billing and payment systems.

- Regular auditing of financial transactions and reconciliation.

- Employee training on identifying phishing attempts.

Recommended Actions:

1. Implement multi-factor authentication for financial system access.

2. Conduct regular fraud detection and prevention audits.

3. Enhance data backup and recovery procedures.

4. Conduct employee awareness programs on financial security.

5. Strengthen email filtering to detect and block phishing attempts.

---

\*Information Asset Risk Worksheet 4:\*

Organization Name: SLT Mobitel

Asset Name: Customer Service Data

Asset Description: Data related to customer inquiries, complaints, and service requests.

Threats:

1. Unauthorized Access: Unauthorized individuals gaining access to customer service data.

2. Data Leakage: Accidental or intentional sharing of customer service data.

3. Insider Threats: Malicious actions or data breaches by employees.

4. Data Corruption: Accidental or intentional deletion or modification of data.

5. Social Engineering: Attempts to manipulate employees into divulging sensitive customer service data.

Risk Level (1-5):

1. Unauthorized Access: 4

2. Data Leakage: 3

3. Insider Threats: 3

4. Data Corruption: 2

5. Social Engineering: 3

Current Controls:

- Access controls and monitoring for customer service databases.

- Employee training on data protection and recognizing social engineering attempts.

Recommended Actions:

1. Enhance access controls and monitoring for customer service databases.

2. Implement data loss prevention measures.

3. Conduct regular employee training on social engineering awareness.

4. Establish incident response protocols for data breaches.

5. Conduct periodic security assessments of customer service systems.

---

\*Information Asset Risk Worksheet 5:\*

Organization Name: SLT Mobitel

Asset Name: Intellectual Property (IP)

Asset Description: This includes proprietary software, network designs, and telecommunications technology developed by SLT Mobitel.

Threats:

1. Intellectual Property Theft: Unauthorized access or theft of proprietary technology and designs.

2. Insider Threats: Malicious actions or data breaches by employees targeting IP.

3. Espionage: External entities attempting to gain access to SLT Mobitel's IP.

4. Unauthorized Disclosure: Inadvertent sharing of IP with unauthorized parties.

5. Data Corruption: Accidental or intentional modification of IP data.

Risk Level (1-5):

1. Intellectual Property Theft: 4

2. Insider Threats: 3

3. Espionage: 4

4. Unauthorized Disclosure: 2

5. Data Corruption: 2

Current Controls:

- Strict access controls and encryption for IP repositories.

- Employee training on the importance of IP protection.

Recommended Actions:

1. Enhance access controls and monitoring for IP repositories.

2. Implement data loss prevention mechanisms.

3. Conduct regular IP audits and assessments.

4. Educate employees on recognizing potential IP threats.

5. Develop an incident response plan for IP breaches and espionage attempts.

These risk worksheets will serve as a foundation for identifying, assessing, and mitigating potential risks to critical information assets within SLT Mobitel. Keep in mind that the specific threats and recommended actions would need to be tailored based on the organization's actual security posture and the evolving threat landscape.