**Security Individual Report**

Individual assignment structure:

1. Risk analysis: to cover assets, threats, and vulnerabilities with justifications
2. Risk mitigation strategy: risk avoidance, risk acceptance etc (refer to lecture notes for the full list)

• Risk Avoidance – Possibility of eliminating the existence • Risk Reduction – Reduction of opportunity and potential loss to the lowest level • Risk Spreading – Reduce the time available to steal assets and escape without apprehension • Risk Transfer – Transferring risks to other alternatives • Risk Acceptance – Accepting the possible risk impact.

1. Risk controls: to be aligned with the risk mitigation strategy (for example, if the strategy is risk acceptance, the controls should focus on how to minimize the impact by such risk, not on preventing risk from happening) **策略是大方向，而控制是执行策略的具体措施**
2. Implementation plan: to cover all the action items of all risk controls, including who is the owner, what are stakeholders/ resources involved and projected completion timeline
3. Policy: the policy should minimally address one control

**4. Lack of Encryption on Sensitive Data – Liang Hou**

**Risk Analysis**:   
Sensitive data was not encrypted at rest or in transit, allowing attackers to intercept and collect payment card information.

|  |
| --- |
| **Detailed Overview of the Asset**: Define the asset (sensitive customer data) and its value to the organization. Discuss why customer payment card data is considered sensitive and outline the regulatory implications (such as PCI DSS standards for payment security).  **Threat Justification**: Explain how unauthorized access to unencrypted data makes it vulnerable to interception. You could include the potential methods attackers used (e.g., malware that scraped unencrypted card data from POS systems).  **Vulnerabilities and Weaknesses**: Describe the lack of encryption in detail, covering both technical and procedural gaps. Explain the role of unencrypted data at rest and in transit, and discuss how these vulnerabilities make it easier for attackers to intercept data.  **Impact and Consequences**: Detail the impact of such a breach on customers (financial loss, identity theft) and the organization (reputation damage, financial penalties, litigation). |

**Risk Management Strategy**:   
Implement **end-to-end encryption (E2EE)** for sensitive data across all systems and ensure secure key management practices.

|  |
| --- |
| Strategies guide the overall direction for managing risks and can include approaches like risk avoidance (completely avoiding an activity to eliminate risk), risk transfer (shifting risk to another party, such as through insurance), risk reduction (minimizing the likelihood or impact of risk), and risk acceptance (acknowledging the risk and choosing to bear it). The strategy is the "what" and "why" behind the chosen course of action. |

|  |
| --- |
| **E2EE and Industry Best Practices**: Provide an in-depth explanation of why end-to-end encryption (E2EE) is critical and outline specific encryption standards like AES-256. Compare the strategy with alternatives, such as tokenization or point-to-point encryption.  **Justify the Chosen Strategy**: Discuss how E2EE addresses vulnerabilities in both data at rest and data in transit, including how it could prevent a similar breach. You might also consider other frameworks or guidelines that support E2EE, like NIST or ISO/IEC standards, to strengthen your justification.  **Alternative Strategies**: Briefly mention other strategies (e.g., tokenization) and justify why E2EE was chosen over them. |

**Mitigation Implementation Plan**:

* **Phase 1: Encryption Solution Selection (1 month)**
* **Responsibility**: IT Security Team.
* **Actions**: Select industry-standard encryption protocols (e.g., AES-256) and implement encryption for both data at rest and in transit.
* **Resources**: Encryption software, HSMs (Hardware Security Modules).
* **Phase 2: Implementation and Key Management (2 months)**
* **Responsibility**: IT Infrastructure and Security Teams.
* **Actions**: Encrypt all payment data and implement a key management system (e.g., secure key generation, rotation).
* **Resources**: Key management system, encryption libraries.
* **Phase 3: Monitoring and Updates (ongoing)**
* **Responsibility**: IT Security Team.
* **Actions**: Continuously monitor encryption systems for vulnerabilities and perform regular key rotations.
* **Resources**: Monitoring tools, auditing mechanisms.

**Assumptions**: All systems can be upgraded to support encryption, and existing hardware is compatible with encryption technologies.

**Phase 1: Encryption Solution Selection**

* **Detailed Process**: Discuss the evaluation criteria for selecting encryption software (compliance, interoperability, and scalability).
* **Stakeholders and Decision-Makers**: Specify roles involved in decision-making (e.g., cybersecurity specialists, IT managers) and justify their involvement.

**Phase 2: Implementation and Key Management**

* **Technical Implementation**: Describe the process of deploying encryption protocols across systems, focusing on data flows that require encryption.
* **Key Management Policies**: Include specifics on secure key storage, controlled access, and policies for key expiration and renewal. Describe the key lifecycle management framework.

**Phase 3: Monitoring and Updates**

* **Continuous Monitoring**: Detail the tools and protocols for monitoring encryption, and outline the processes for identifying vulnerabilities, such as anomaly detection systems.
* **Regular Key Rotations and Audits**: Explain why regular audits are crucial and describe protocols for securely handling key rotation to prevent unauthorized access.

**Policy**

* **Draft a Sample Policy**: Create a policy outline that addresses encryption requirements for sensitive data, specifying guidelines for E2EE, key management, and monitoring.
* **Employee and Stakeholder Responsibilities**: Define roles and responsibilities within the organization, including IT and security teams. Mention any required security awareness training for employees.
* **Compliance Standards**: Reference applicable standards (PCI DSS, NIST) and outline the consequences of non-compliance. Include an escalation process for breaches and security incidents.

**Additional Content Suggestions for Depth**

* **Case Studies and Examples**: Incorporate case studies of other organizations that suffered data breaches due to lack of encryption. Compare their mitigation approaches to Target’s case.
* **Real-World Encryption Implementations**: Discuss examples of robust encryption implementations in the industry to illustrate best practices.
* **Diagrams and Flowcharts**: Include visual aids, such as a flowchart of data handling before and after encryption. This can help illustrate the end-to-end encryption process and key management.
* **Appendices for Technical Details**: Add a section for in-depth technical aspects, like encryption algorithms or key management tools, if allowed. This could further explain the technical backbone of E2EE.

**Risk Analysis**

Qualitative Risk Analysis

In this section, system characterisation was used to identify assets, and based on these assets, related threats were suggested. Every threat (or risk point) had a well-supported argument. Then, all risk points were methodically listed and their risk levels were evaluated using a qualitative risk analysis method.

**Asset**

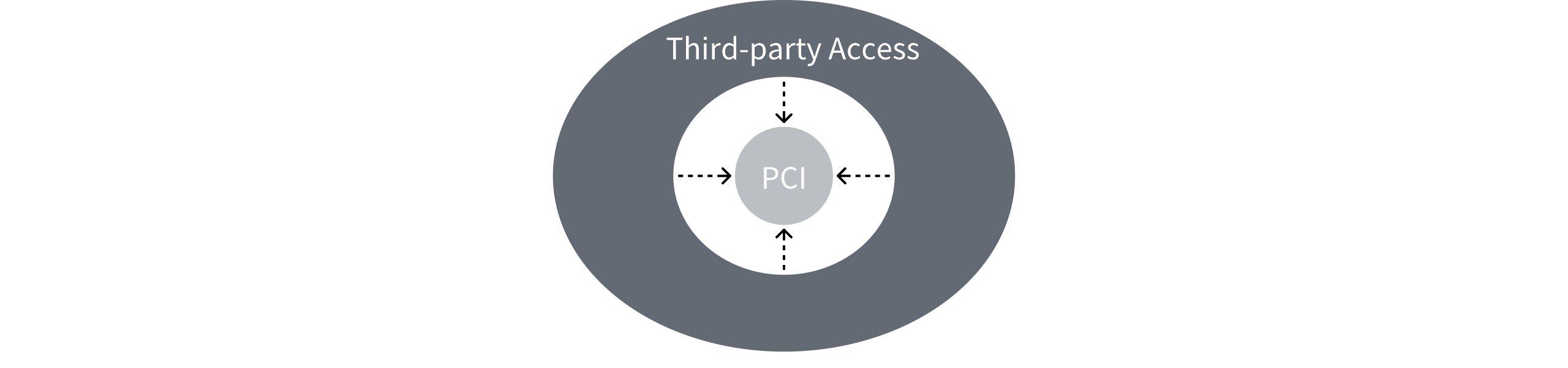
In the 2013 Target data breach, assets mostly included **Third-Party Access to the Internal Network** and **Customer Payment Card Information (PCI)** under the heading of Lack of Encryption on Sensitive Data.

1. Credit card numbers, debit card numbers, expiration dates, and CVV codes are all part of the Customer Payment Card Information (PCI). Because it allows customers to make purchases and is essential to preserving the retailer's reputation with its clientele, this sensitive financial information is essential.
2. Third-Party Access to own Network: Target's own systems, including payment processing networks, were made available to vendors like Fazio Mechanical. Although this access was necessary for maintenance, it also gave hackers a possible point of entry.

[ Justification ]

For any retailer, one of the most delicate and precious assets is customer payment information. It needs to be sufficiently safeguarded to prevent monetary loss, legal responsibility, and reputational harm.

Any third-party vendor who has access to a business's internal network is considered an indirect asset as their security procedures compromise the accuracy of the data held by the organization. The exposure of extremely sensitive assets, such as consumer payment information, may result from a breach using this access. Figure-1 illustartes the outcome of asset recognization.



**Threat & Vulnerability**

Threat: external factor; Vulnerability: internal factor.

(external factor) (internal factor)As per the system characterization, which includes highly sensitive assets like customer payment card information and third-party access to the internal network, threats (external factors) could originate from hackers who aim to steal unencrypted data, as was confirmed in the 2013 Target data breach, or from cybercriminals who target weaknesses in third-party vendors. The absence of end-to-end encryption on payment data and the combination of encryption and unfettered third-party access are two examples of vulnerabilities (internal factors) that must be carefully considered in addition to threats. The following is a list of the specific examples of threats and vulnerabilities:

1. **Cybercriminals (Hackers) Seeking to Steal Unencrypted Data (threat)**: Attackers target businesses to obtain unencrypted payment data that can be sold on the black market or used for fraudulent transactions.
2. **Cybercriminals Targeting Vulnerabilities in Third-Party Vendors (threat)**: Attackers often focus on third-party service providers with weaker security controls to gain access to a larger organization's sensitive assets. This indirect approach is often used when targeting heavily defended environments.
3. **Lack of End-to-End Encryption on Payment Data (vulnerability)**:During the breach, Target did not implement adequate encryption measures, particularly for data stored in its system after being transmitted from point-of-sale (POS) systems. Risk outcome may be data breach and massive financial loss. The lack of encryption on sensitive payment data directly contributed to one of the largest data breaches in retail history. Target faced significant financial penalties, including $18.5 million in settlements, not to mention loss of consumer trust and long-term brand damage.During the breach, Target did not implement adequate encryption measures, particularly for data stored in its system after being transmitted from point-of-sale (POS) systems. Risk outcome of this vulnerability mainly includes Data Breach and Massive Financial Loss. The lack of encryption on sensitive payment data directly contributed to one of the largest data breaches in retail history. Target faced significant financial penalties, including $18.5 million in settlements, not to mention loss of consumer trust and long-term brand damage.
4. **Lack of Encryption Combined with Unrestricted Third-Party Access (vulnerability)**: Although encryption on sensitive data is the main focus, the failure to isolate third-party vendors from critical payment systems and lack of encryption on payment data exacerbated the risk. Once attackers gained access through the third-party, the unencrypted payment data was easy to capture.
5. **Lack of Encryption Combined with Unrestricted Third-Party Access (vulnerability):** Although encryption on sensitive data is the main focus, the failure to isolate third-party vendors from critical payment systems and lack of encryption on payment data exacerbated the risk. Once attackers gained access through the third-party, the unencrypted payment data was easy to capture.

[ Justification ]

Hackers actively seek opportunities where sensitive data is poorly protected or inadequately encrypted. In Target’s case, attackers gained access to its network, leading to the theft of over 40 million credit and debit card records. Fazio Mechanical’s systems were compromised first because they had weaker cybersecurity practices, providing an entry point into Target’s payment network. The attackers exploited this pathway to ultimately access unencrypted payment card information.

Encryption is fundamental security control that ensures sensitive data remains unreadable even if accessed by unauthorized parties. The absence of encryption meant that once hackers breached Target’s network, they could easily capture and exploit unprotected customer payment data. Even though the attack vector was initiated through the third-party vendor, the absence of end-to-end encryption on payment data allowed attackers to extract valuable information once they were inside the network. Strong encryption could have mitigated the damage even if attackers had gained initial access.Encryption is fundamental security control that ensures sensitive data remains unreadable even if accessed by unauthorized parties. The absence of encryption meant that once hackers breached Target’s network, they could easily capture and exploit unprotected customer payment data. Even though the attack vector was initiated through the third-party vendor, the absence of end-to-end encryption on payment data allowed attackers to extract valuable information once they were inside the network. Strong encryption could have mitigated the damage even if attackers had gained initial access.

In conclusion, while the attack began through third party’s (like Fazio Mechanical) access, **encryption on payment data** would have added a critical layer of defense. The **lack of encryption** made it easier for attackers to capture sensitive data once they infiltrated the network via the compromised vendor. The breach highlights the importance of both **network segmentation** to limit third-party access and **strong encryption** to protect sensitive data, even if perimeter defenses are compromised. The recognized risk points are listed in the following table (Table-1). And the magnitude of impact and likelihood are given via qualitative risk analysis. The final risk level for each risk point was calculated by the product of impact and likelihood, and the judge risk was presented in Figure-2.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Risk Point | Asset | Threat | Vulnerability | Impact | Likelihood | Risk Level (Impact × Likelihood) |
| 1 | Lack of Encryption on Customer Payment Card Information (PCI) | Customer Payment Card Information (PCI) | **Cybercriminals (Hackers) Seeking to Steal Unencrypted Data**: Hackers can intercept unencrypted payment data at rest or in transit. | **Lack of End-to-End Encryption on Payment Data**: Unencrypted data is vulnerable to being captured once attackers infiltrate the network. | High | High | Critical |
| 2 | Lack of Encryption Combined with Third-Party Access to Internal Network | Internal Network with access to payment data | **Cybercriminals Targeting Vulnerabilities in Third-Party Vendors**: Hackers use third-party vendors with weaker security as a gateway to access sensitive payment systems. | **Lack of Encryption Combined with Unrestricted Third-Party Access**: Vendors with access to the network but no encryption on sensitive data leave it exposed if breached. | High | Medium | High |

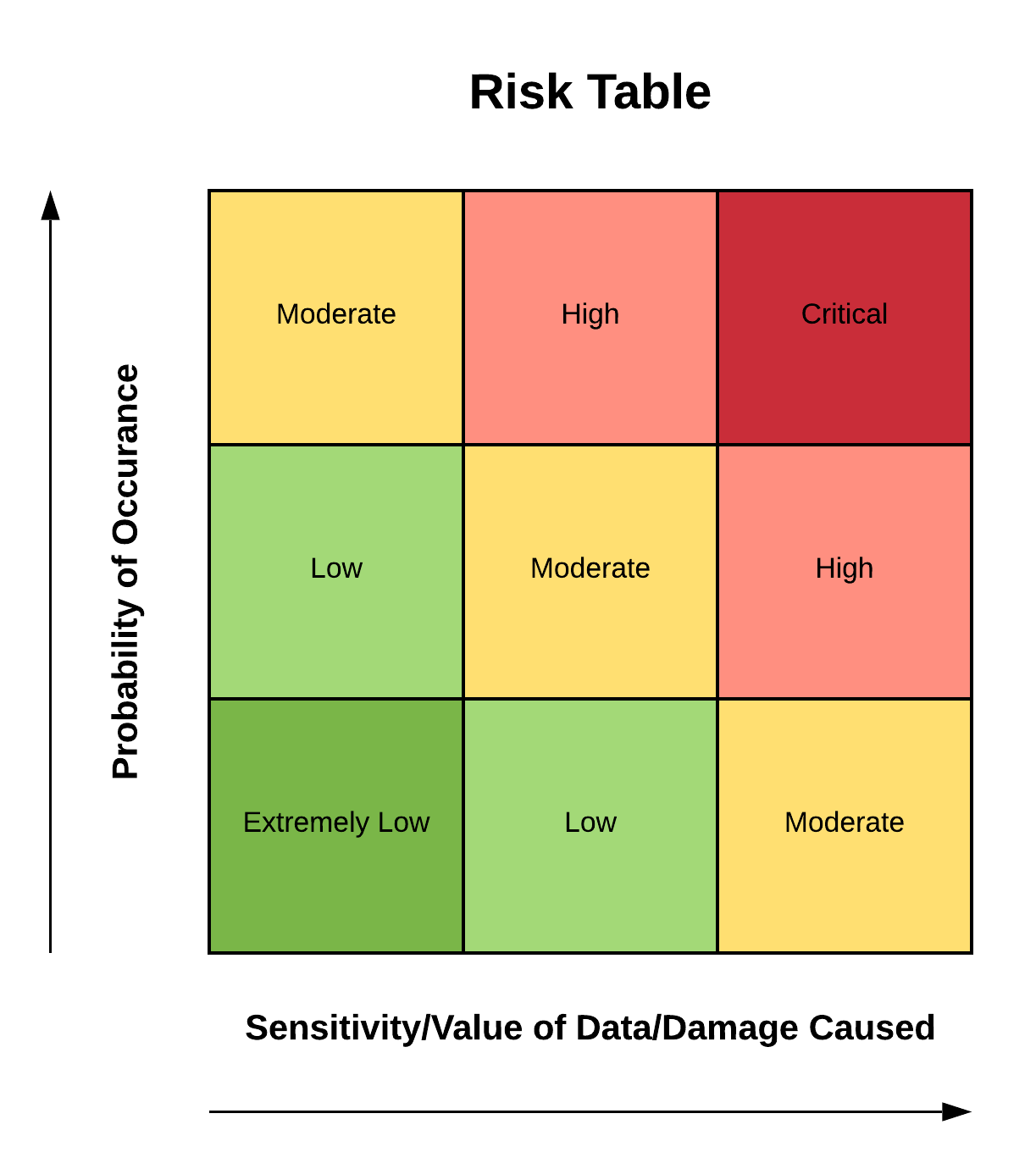


Figure-2

**Risk Mitigation:** Implement end-to-end encryption for all payment card data to protect it during storage and transmission.

**Risk Mitigation Strategy**

Above identified risk points, risk mitigation strategies were given with an integration of overall considerations.

Implementing a "Risk Reduction" risk mitigation strategy is preferable for risk point 1 (Lack of Encryption on Customer PCI) because encryption directly lowers the opportunity for sensitive data theft by guaranteeing that, even if attackers manage to access the payment data, it will be unusable without the decryption key, and end-to-end encryption protects data both in transit and at rest, significantly lowering the risk of exposure to cybercriminals.

Additionally, risk reduction using encryption is a realistic and efficient method to reduce the risk's impact and likelihood when taking into account its high impact and high possibility. The risk of exposure is significantly decreased by encrypting all payment information.

For risk point 2, implement a combination of "risk reduction" (through encryption and restricted access) and "risk transfer" (through contracts and insurance) risk mitigation strategies. The former is the main strategy because it reduces the likelihood of a breach by encrypting sensitive data and limiting third-party access, while the latter is a complementary strategy because it enables the organization to lessen the financial impact in the event of a breach involving a third-party vendor.

By implementing risk reduction, two main actions can be done. ① **Limiting third-party access** to critical payment systems and encrypting any sensitive data they may come into contact with **reduces the opportunity** for data theft through a third-party compromise. On the other hand, ② **Encrypting data** and ensuring strict access controls (such as segmenting networks and requiring multi-factor authentication) directly **reduces the risk** posed by third-party vulnerabilities.

For Risk Transfer: ① **Transferring risk** via contracts with third-party vendors places the onus on them to maintain a certain level of security. This can include requiring them to implement their own encryption protocols and liability agreements and ② **Cyber insurance policies** can be used to transfer some of the financial risk in case of a breach involving a third-party vendor. This limits the financial exposure of the organization.

In both cases, the focus is on **reducing the risk to an acceptable level**. Encryption is a powerful **risk reduction** tool that directly lowers the chance of a successful attack on unencrypted data. For third-party access, **risk transfer** adds an additional layer of protection by sharing the burden of risk with external parties through contracts and insurance.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Risk Point | Impact | Likelihood | Risk Level (Impact × Likelihood) | Risk Mitigation Strategy | Risk Response |
| 1 | Lack of Encryption on Customer Payment Card Information (PCI) | High | High | Critical | risk reduction | Implement end-to-end encryption for all payment card data to protect it during storage and transmission. |
| 2 | Lack of Encryption Combined with Third-Party Access to Internal Network | High | Medium | High | risk reduction  (primary strategy)  +  risk transfer  (complementary strategy) | **Risk Reduction:**   * **Limiting third-party access** to critical payment systems and encrypting any sensitive data they may come into contact with **reduces the opportunity** for data theft through a third-party compromise. * **Encrypting data** and ensuring strict access controls (such as segmenting networks and requiring multi-factor authentication) directly **reduces the risk** posed by third-party vulnerabilities.   **Risk Transfer:**   * **Transferring risk** via contracts with third-party vendors places the onus on them to maintain a certain level of security. This can include requiring them to implement their own encryption protocols and liability agreements. * **Cyber insurance policies** can be used to transfer some of the financial risk in case of a breach involving a third-party vendor. This limits the financial exposure of the organization. |

**Risk controls**

In the previous section "Risk Mitigation Strategy", the report discusses which strategies should be implemented for each risk point. This section will go further to suggest risk control measures according to selected risk mitigation strategies.

|  |  |  |
| --- | --- | --- |
| **Risk Point-1**: Lack of Encryption on Customer Payment Card Information (PCI)  **Risk Mitigation Strategy**: Risk Reduction (focus on reducing the opportunity and potential impact of data theft by implementing strong encryption protocols). |  |  |
| **Risk Control Measures** |  |  |
| **No.** | **Item.** | **Des.** |
| 1 | **Implement End-to-End Encryption** | * Ensure that all payment card information (PCI) is encrypted at every stage of the data lifecycle (at rest and in transit). * Use strong encryption standards such as AES-256 for data storage and TLS 1.2+ for data in transit. |
| 2 | **Regular Encryption Key Management** | * Develop and maintain a secure key management system to generate, store, and rotate encryption keys regularly. * Use hardware security modules (HSMs) for key storage and ensure only authorized personnel have access to encryption keys. |
| 3 | **Data Loss Prevention (DLP) Tools** | * Deploy DLP solutions to detect and prevent unencrypted payment data from being transmitted outside of authorized networks or systems. |
| 4 | **Secure Payment Systems** | * Regularly review and audit payment systems for vulnerabilities that could expose encrypted data. * Implement automated patching and security updates for all payment-related systems. |
| 5 | **Encryption Compliance and Audits** | * Conduct regular audits to ensure encryption practices meet relevant industry standards (e.g., PCI DSS) and regulatory requirements. * Maintain detailed logs and reports of encryption operations for compliance verification. |
| **Risk Point-2**: Lack of Encryption Combined with Third-Party Access to Internal Network  **Risk Mitigation Strategy**: Risk Mitigation Strategies: Risk Reduction & Risk Transfer (Minimize the exposure of sensitive data to third-party vendors while transferring some financial risks to external parties through contracts and insurance). |  |  |
| **Risk Control Measures** |  |  |
| **No.** | **Item.** | **Des.** |
| 1 | **Network Segmentation and Access Control** | * Implement network segmentation to restrict third-party access to only non-critical systems, ensuring that third-party vendors do not have direct access to sensitive payment data. * Use strict access controls such as multi-factor authentication (MFA) and least-privilege access principles for third-party vendors. |
| 2 | **Encryption of Data Shared with Third Parties** | * Encrypt all data shared with or accessible by third-party vendors, ensuring that even if vendors are compromised, the sensitive data remains protected. * Implement encrypted communication protocols (e.g., SFTP, HTTPS) for data transmission between the organization and third parties. |
| 3 | **Vendor Security Audits and Risk Assessments** | * Conduct regular security audits and risk assessments of third-party vendors to ensure they meet the organization's encryption and security standards. * Require vendors to follow strict security guidelines, including encryption protocols and data protection policies, as part of the contract. |
| 4 | **Cybersecurity Insurance for Third-Party Vendor Breaches** | * Obtain cybersecurity insurance that covers financial losses from breaches related to third-party vendor vulnerabilities, including data theft and unauthorized access. * Include clauses in third-party contracts that shift financial liability for breaches due to vendor negligence onto the vendor (risk transfer). |
| 5 | **Third-Party Monitoring and Incident Response** | * Implement real-time monitoring of third-party vendor activities and network access to detect and respond to suspicious behavior or unauthorized data access. * Ensure that third-party contracts include incident response requirements, mandating immediate notification and collaboration in the event of a breach. |

The **risk controls** align with the **risk reduction** and **risk transfer** strategies by focusing on encryption to secure sensitive data and reduce exposure, while also using vendor contracts and insurance to mitigate financial risks associated with third-party breaches. The controls focus on reducing the likelihood of a breach and minimizing the potential impact should one occur, ensuring that both technical and contractual safeguards are in place to protect customer payment information and sensitive internal systems.

**Implementation plan**

**Lack of Encryption on Customer Payment Card Information (PCI)**

**Risk Mitigation Strategy: Risk Reduction**

**Action Item 1: Implement End-to-End Encryption**

|  |  |  |
| --- | --- | --- |
| **Action Item 1: Implement End-to-End Encryption** |  |  |
| **Owner** |  | Chief Information Security Officer (CISO) |
| **Stakeholders** |  | * IT Department * Network Security Team * Payment Processing Team |
| **Resources Involved** |  | * Encryption software (e.g., AES-256) * IT infrastructure * hardware security modules (HSMs) |
| **Projected Completion Timeline:** 6 months |  |  |
| **Task 1.1** | 1 month | Select and procure encryption solution |
| **Task 1.2** | 3 months | Implement encryption on all payment data systems |
| **Task 1.3** | 2 months | Test and audit the encryption implementation |

**Action Item 2: Regular Encryption Key Management**

|  |  |  |
| --- | --- | --- |
| **Action Item 2: Regular Encryption Key Management** |  |  |
| **Owner** |  | IT Security Manager |
| **Stakeholders** |  | * IT Department * Compliance Team |
| **Resources Involved** |  | * Key management software * HSMs * secure key storage solutions |
| **Projected Completion Timeline:** 3 months |  |  |
| **Task 2.1** | 1 month | Procure key management system |
| **Task 2.2** | 1 months | Implement automated key rotation and storage procedures |
| **Task 2.3** | 1 months | Train relevant staff on secure key handling |

**Action Item 3: Data Loss Prevention (DLP) Tools Deployment**

|  |  |  |
| --- | --- | --- |
| **Action Item 3: Data Loss Prevention (DLP) Tools Deployment** |  |  |
| **Owner** |  | Network Security Manager |
| **Stakeholders** |  | * IT Department * Security Operations Center (SOC) |
| **Resources Involved** |  | * DLP software * network monitoring tools |
| **Projected Completion Timeline:** 4 months |  |  |
| **Task 3.1** | 2 month | Procure and configure DLP tools |
| **Task 3.2** | 1 months | Deploy DLP system across all endpoints and network gateways |
| **Task 3.3** | 1 months | Test DLP system and monitor for unauthorized data transmissions |

**Action Item 4: Secure Payment Systems**

|  |  |  |
| --- | --- | --- |
| **Action Item 3: Data Loss Prevention (DLP) Tools Deployment** |  |  |
| **Owner** |  | IT Infrastructure Manager |
| **Stakeholders** |  | * Payment Processing Team * IT Department |
| **Resources Involved** |  | * Patching tools * network security systems |
| **Projected Completion Timeline:** Ongoing |  |  |
| **Task 4.1** | 2 month | Perform initial vulnerability assessment on payment systems |
| **Task 4.2** | 2 months | Implement automated patch management |
| **Task 4.3** | Ongoing | Conduct quarterly vulnerability scans and updates |

**Action Item 5: Encryption Compliance and Audits**

|  |  |  |
| --- | --- | --- |
| **Action Item 5: Encryption Compliance and Audits** |  |  |
| **Owner** |  | Compliance Officer |
| **Stakeholders** |  | * IT Security Team * External Auditors |
| **Resources Involved** |  | * Compliance audit software * network security systems |
| **Projected Completion Timeline:** Ongoing |  |  |
| **Task 5.1** | 2 month | Perform initial vulnerability assessment on payment systems |
| **Task 5.2** | 2 months | Schedule quarterly internal reviews and external audits |
| **Task 5.3** | Ongoing | Maintain compliance documentation and reports for regulators |

**Lack of Encryption Combined with Third-Party Access to Internal Network**

**Risk Mitigation Strategies: Risk Reduction & Risk Transfer**

**Action Item 1: Network Segmentation and Access Control**

|  |  |  |
| --- | --- | --- |
| **Action Item 1: Network Segmentation and Access Control** |  |  |
| **Owner** |  | Network Administrator |
| **Stakeholders** |  | * IT Security Team * Third-Party Vendors * SOC |
| **Resources Involved** |  | * Network segmentation tools * firewall systems * MFA software |
| **Projected Completion Timeline:** 5 months |  |  |
| **Task 1.1** | 3 month | Implement network segmentation, separating sensitive payment systems |
| **Task 1.2** | 1 months | Deploy multi-factor authentication (MFA) for third-party access |
| **Task 1.3** | 1 months | Review and restrict third-party access rights |

**Action Item 2: Encryption of Data Shared with Third Parties**

|  |  |  |
| --- | --- | --- |
| **Action Item 2: Encryption of Data Shared with Third Parties** |  |  |
| **Owner** |  | Third-Party Risk Manager |
| **Stakeholders** |  | * IT Department * Legal Team * Vendor Management |
| **Resources Involved** |  | * Encryption tools * secure communication protocols (e.g., SFTP, HTTPS) |
| **Projected Completion Timeline:** 4 months |  |  |
| **Task 2.1** | 2 month | Implement encrypted communication protocols for vendor data exchanges |
| **Task 2.2** | 2 months | Ensure encryption of any sensitive data accessible by third parties |

**Action Item 3: Vendor Security Audits and Risk Assessments**

|  |  |  |
| --- | --- | --- |
| **Action Item 3: Vendor Security Audits and Risk Assessments** |  |  |
| **Owner** |  | Vendor Management Officer |
| **Stakeholders** |  | * Third-Party Vendors * Legal Team * IT Security Team |
| **Resources Involved** |  | * Vendor audit tools * risk assessment templates * legal contracts |
| **Projected Completion Timeline:** Ongoing |  |  |
| **Task 3.1** | 1 month | Implement encrypted communication protocols for vendor data exchanges |
| **Task 3.2** | Ongoing | Ensure encryption of any sensitive data accessible by third parties |
| **Task 3.3** | 2 months | Review and update vendor contracts to enforce encryption standards |

**Action Item 4: Cybersecurity Insurance for Third-Party Vendor Breaches**

|  |  |  |
| --- | --- | --- |
| **Action Item 3: Vendor Security Audits and Risk Assessments** |  |  |
| **Owner** |  | Legal and Risk Officer |
| **Stakeholders** |  | * Legal Department * Insurance Providers * Third-Party Vendors |
| **Resources Involved** |  | * Cyber insurance policies * vendor contracts |
| **Projected Completion Timeline: 2 months** |  |  |
| **Task 4.1** | 1 month | Negotiate and purchase cybersecurity insurance |
| **Task 4.2** | 1 month | Review and update vendor contracts to transfer liability for breaches |

**Action Item 5: Third-Party Monitoring and Incident Response**

|  |  |  |
| --- | --- | --- |
| **Action Item 3: Vendor Security Audits and Risk Assessments** |  |  |
| **Owner** |  | SOC Manager |
| **Stakeholders** |  | * IT Security Team * Third-Party Vendors * Incident Response Team |
| **Resources Involved** |  | * Real-time monitoring tools * incident response platforms |
| **Projected Completion Timeline:** Ongoing |  |  |
| **Task 5.1** | 2 month | Implement real-time monitoring of third-party activities |
| **Task 5.2** | 2 month | Develop and test an incident response plan for third-party breaches |
| **Task 5.3** | Ongoing | Conduct periodic response drills and update protocols |

This **implementation plan** provides a structured approach to mitigating the risks associated with the **lack of encryption** on sensitive data and **third-party access** vulnerabilities. The **timeline and responsibilities** ensure that all relevant stakeholders are engaged in protecting critical assets like customer payment information, while also ensuring that financial risks are minimized through **risk transfer** mechanisms like insurance and contractual obligations. The projected timelines allow for continuous improvement, while the **ongoing monitoring and audit processes** ensure that security measures remain effective over time.

**Policy**

**Policy Title:** Vendor Security Management Policy   
**Policy Number:** TGT-VSMP-001   
**Effective Date:** [Insert Date]   
**Revision History:** First Issue   
**Owner:** Target Corporation Information Security Department   
**Approved by:** [Insert Approving Body]   
**Applies to:** All third-party vendors who have access to Target’s systems, networks, or data.

1. **Overview**

Sensitive data encryption is a critical component of any organization’s security strategy, particularly in safeguarding customer information and internal assets from cybercriminals. This document addresses the risks associated with the lack of encryption on sensitive data, specifically focusing on customer payment card information (PCI) and third-party access to internal networks. The purpose of this document is to outline the roles, regulations, and teams responsible for managing these risks and implementing the necessary encryption controls to ensure data confidentiality and security.

2. **Purpose**

The purpose of this document is to provide a comprehensive overview of the risks associated with the lack of encryption on sensitive data, such as customer payment card information (PCI) and data accessed by third-party vendors. It outlines the strategies, controls, and responsibilities required to mitigate these risks, ensuring the integrity, confidentiality, and security of sensitive information. This document serves as a guideline for the implementation of encryption standards, risk management practices, and compliance with relevant regulations.

3. **Scope**

This document applies to all systems, processes, and stakeholders involved in handling sensitive customer data, specifically customer payment card information (PCI) and data that third-party vendors access or manage. It covers the following:

* **Data Encryption Standards:** Ensuring that encryption protocols are implemented to protect data both at rest and in transit.
* **Third-Party Vendor Access:** Managing the risks associated with third-party access to sensitive data by ensuring encrypted communication and appropriate access controls.
* **Risk Management:** Outlining the strategies to mitigate risks related to unencrypted sensitive data, including risk reduction, risk transfer, and compliance audits.

4. **Policy**

This section outlines the security requirements and management strategies regarding third-party vendors who may have access to the organization's sensitive data, including customer payment card information (PCI). Proper third-party risk management and the inclusion of security standards in vendor contracts are critical to protecting sensitive data from unauthorized access or exposure.

4.1 **Vendor Security Requirements**

To safeguard sensitive data and mitigate risks associated with third-party access, all vendors handling, transmitting, or storing the organization’s sensitive data must adhere to the following security requirements:

* **Encryption of Sensitive Data**: Vendors must ensure that all sensitive data, particularly customer payment card information (PCI), is encrypted both at rest and in transit. This includes the use of strong encryption protocols (e.g., AES-256 for data at rest and TLS for data in transit).
* **Authentication and Access Control**: Vendors must implement strict access controls, including multi-factor authentication (MFA) and role-based access management, to limit access to sensitive data. Only authorized personnel should have access to encrypted data, and access must be logged and monitored.
* **Security Certifications**: Vendors must hold relevant industry certifications (e.g., **PCI DSS**, **ISO 27001**) to demonstrate their compliance with industry standards for data security and encryption practices.
* **Incident Reporting**: Vendors must report any security incidents or breaches involving the organization’s sensitive data within 24 hours of discovery. A clear incident response protocol must be in place to address data breaches, especially those involving unencrypted data.
* **Security Audits**: Vendors are required to undergo regular security audits and provide the organization with the results to verify compliance with encryption and other security measures.

4.2 **Third-Party Risk Management**

To manage the risks posed by third-party vendors, the organization must implement a comprehensive **Third-Party Risk Management (TPRM)** program. This program will evaluate and mitigate risks associated with vendors who have access to sensitive data:

* **Vendor Risk Assessment**: Before engaging with any vendor, the organization must perform a thorough risk assessment to evaluate the vendor’s data security practices, particularly regarding encryption. The assessment will include evaluating the vendor’s encryption protocols, key management practices, and compliance with industry security standards.
* **Ongoing Monitoring**: Vendors will be subject to continuous monitoring to ensure compliance with the organization’s encryption policies and security requirements. The Confidentiality / Security Team (CST) will regularly review vendor performance, assess new risks, and address any identified security gaps.
* **Vendor Security Reviews**: Vendors must undergo regular security reviews to ensure they are maintaining adequate security controls. These reviews will focus on encryption practices, access control, incident response, and data protection.
* **Third-Party Audits**: Independent third-party audits may be conducted to verify the security controls of vendors, particularly those handling sensitive data. Audit results must be shared with the organization to ensure ongoing compliance.

4.3 **Vendor Contracts**

All vendor contracts must include explicit security provisions that address the protection of sensitive data through encryption and other security measures. The following elements must be included in contracts with third-party vendors:

* **Data Encryption Requirements**: Contracts must specify that all sensitive data, particularly customer payment card information (PCI), must be encrypted both at rest and in transit. The encryption standards (e.g., AES-256, TLS) and protocols for key management must be clearly outlined.
* **Confidentiality Agreement**: Vendors must sign a confidentiality agreement that prohibits them from sharing, disclosing, or misusing the organization’s sensitive data. This includes provisions requiring the protection of data through encryption.
* **Security Compliance Clause**: Contracts must include a clause requiring vendors to comply with relevant security standards (e.g., **PCI DSS**, **GDPR**, **ISO 27001**) and to implement appropriate encryption controls. The vendor must also agree to security audits and provide documentation demonstrating compliance with these standards.
* **Incident Response Obligations**: Contracts must specify the vendor’s obligations in the event of a data breach or security incident. This includes immediate notification to the organization, cooperation in the investigation, and taking appropriate steps to mitigate any damage.
* **Termination for Non-Compliance**: Contracts must include a termination clause that allows the organization to end the agreement if the vendor fails to comply with the encryption or security requirements outlined in the contract. Non-compliance with data encryption protocols will be grounds for contract termination.

Vendor security requirements, third-party risk management, and carefully structured vendor contracts are essential to safeguarding the organization’s sensitive data, particularly in environments where third-party access is involved. By enforcing these policies, the organization ensures that vendors adhere to strict encryption and security standards, minimizing the risk of unauthorized access or data breaches.

5. **Policy Compliance**

Ensuring compliance with the organization’s security policies, particularly those concerning the encryption of sensitive data, is critical to protecting customer payment card information (PCI) and other confidential data. This section outlines how compliance will be measured, managed, and enforced, including procedures for handling exceptions and consequences for non-compliance.

5.1 **Compliance Measurement**

To maintain the integrity and security of sensitive data, the organization will regularly measure and monitor compliance with encryption and data protection policies through the following methods:

* **Internal Audits**: Regular internal audits will be conducted by the **Confidentiality / Security Team (CST)** to evaluate adherence to encryption policies. These audits will focus on the encryption of data at rest and in transit, encryption key management, and third-party vendor compliance with security standards.
* **Automated Monitoring Tools**: The organization will deploy automated security tools to monitor data flows and verify that sensitive data is being encrypted as required, both at rest and during transmission. Any anomalies or instances of unencrypted sensitive data will be flagged for review.
* **Vendor Compliance Reviews**: For third-party vendors handling sensitive data, the organization will conduct periodic reviews to ensure that vendors are adhering to the encryption and security requirements outlined in their contracts.
* **Employee Training and Certification**: Employees handling sensitive data will undergo regular training sessions on encryption practices. Compliance will be measured through assessments, certifications, and regular performance evaluations to ensure employees understand and implement the required encryption protocols.

5.2 **Exceptions**

In some cases, there may be justified exceptions to encryption policies, typically due to operational limitations or technical constraints. Exceptions must be managed and documented carefully to minimize risk:

* **Exception Request Process**: Employees or third-party vendors seeking an exception to the encryption policy must submit a formal **Exception Request** to the **Confidentiality / Security Team (CST)**, outlining the reason for the exception, the scope, and the potential impact on data security.
* **Risk Assessment**: The CST will conduct a thorough risk assessment of the proposed exception to determine whether it poses a significant risk to sensitive data. If the risk is deemed acceptable, compensating controls (e.g., enhanced monitoring, restricted access) must be implemented to mitigate the impact.
* **Approval of Exceptions**: Only the **Chief Information Security Officer (CISO)** or an authorized representative may approve exceptions to the encryption policy. Each exception must be reviewed on a case-by-case basis, with the decision documented for future audits.
* **Review and Expiry**: Approved exceptions will be subject to periodic reviews to reassess their necessity and risk level. Exceptions may have an expiration date, after which compliance with the encryption policy will be required unless a new request is submitted and approved.

5.3 **Non-Compliance**

Failure to comply with the organization’s encryption policies can lead to severe consequences, including the exposure of sensitive data, reputational damage, and legal penalties. The following steps will be taken in cases of non-compliance:

* **Incident Identification**: Non-compliance with encryption policies may be identified through internal audits, monitoring tools, employee reports, or security incidents. The CST will investigate all potential cases of non-compliance to assess the scope and impact of the violation.
* **Corrective Action Plan**: In cases where non-compliance is identified, the CST will work with the responsible party (e.g., employee, vendor) to develop and implement a **Corrective Action Plan**. This plan may include:
* Immediate encryption of unprotected sensitive data.
* Training or re-education on encryption protocols.
* Technical improvements to ensure future compliance.
* **Disciplinary Actions**: Employees found to be in non-compliance with encryption policies may face disciplinary actions, up to and including termination, depending on the severity of the breach. Vendors failing to meet encryption requirements may be subject to contract termination or other penalties as outlined in their agreements.
* **Legal and Financial Penalties**: In cases where non-compliance leads to a data breach or violation of legal requirements (e.g., **PCI DSS**, **GDPR**), the organization may face fines, legal action, or reputational damage. Those responsible for the breach may be held accountable for the financial and legal repercussions.
* **Reporting Non-Compliance**: All incidents of non-compliance must be reported to the **CISO** and documented for audit purposes. In severe cases involving data breaches, the organization must follow applicable legal reporting requirements to notify regulators and affected parties.

6. **Related Standards, Processes, and Policies**

This policy aligns with several industry standards and regulatory requirements that mandate the encryption of sensitive data, particularly for organizations handling customer payment card information (PCI). Key regulations include:

* **PCI DSS (Payment Card Industry Data Security Standard):** A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. PCI DSS mandates encryption of cardholder data both at rest and in transit.
* **GDPR (General Data Protection Regulation):** The European Union's regulation on data protection and privacy, which emphasizes the importance of data encryption to protect personal data from unauthorized access.
* **CCPA (California Consumer Privacy Act):** A state law in California that grants consumers rights over their personal data and requires businesses to protect it, with encryption as a key security control.
* **SOX (Sarbanes-Oxley Act):** A U.S. regulation that imposes data protection requirements on companies to prevent fraud, including encryption of sensitive financial information.

Organizations must comply with these statutes and industry standards to ensure the secure handling of sensitive information and avoid legal penalties.

7. **Definitions and Term**

|  |  |
| --- | --- |
| Terms | **Definitions** |
| **PCI (Payment Card Information)** | Refers to customer payment card data, including credit and debit card numbers, cardholder information, and related transactional data. |
| **Encryption** | The process of encoding data to prevent unauthorized access, ensuring that only authorized parties can decrypt and read the information. |
| **End-to-End Encryption (E2EE)** | A system of communication where only the communicating users can read the messages, with encryption applied at every stage. |
| **DLP (Data Loss Prevention)** | A strategy to prevent unauthorized transmission or access to sensitive information within or outside of an organization. |
| **MFA (Multi-Factor Authentication)** | A security system that requires multiple methods of verification from independent categories of credentials to verify a user’s identity. |
| **HSM (Hardware Security Module)** | A physical computing device that safeguards and manages digital encryption keys, ensuring only authorized access. |
| **CST (Confidentiality / Security Team)** | The internal team responsible for implementing and monitoring data encryption and security protocols. |

8. **Revision History**