# 4.3 Security

## 4.3.1 Cybersecurity Risk Assessment

This mini cyber security risk assessment measures the critical vulnerabilities within the organization’s computer network by identifying threats against different types of assets, such as data, hardware, software, services and people. It addresses eight of the greatest information security threats, i.e., data breaches, phishing, insider threats, and ransomware. The assessment assists the organization in prioritizing risks – high, medium, and low risks – while making decisions on which measures to adopt in mitigating cyber threats, thus building the cyber security posture of the organization.[[1]](#footnote-1)

Risk Assessment table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Assets | Types | Threats | Vulnerability | Mitigation strategies |
| Customer data | Data | Data breach | Poor access control and password policies weak | MFA with strong password policies implementation |
| Payroll system | Software | Insider threats | Excessive privileges | Least privileges setup and monitoring, auditing access logs regularly. |
| CRM application | Software | DoS | No load balancing or protection of DDoS | WAF, rate limiting, and CND protection implementation |
| Booking server | Hardware | Malware Infection | Outdate OS and antivirus | Update and restrict the external device and also regular patching |
| Staff login credential | Data | Phishing | Lack of user awareness | Provide training |
| Financial document and files | Data | Unauthorized access | Poor permission setup | Encryption technology implementation |
| Backup file | Service | Ransomware | Poor backup option usage | Backup recovery and segment infrastructure usage |
| Email communication | Data | Spoofing | No DMARC/SPF configured | Configure email authentication and monitor outbound traffics |
| Admin Laptop | Hardware | Device theft | No encryption | Implement disk encryption and device tracking software |

Risk Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| Assets | Likelihood | Impact | Risk Level |
| Customer data | High | High | Extreme |
| Payroll system | Medium | High | High |
| CRM application | Medium | High | High |
| Booking server | Medium | High | High |
| Staff login credential | High | Medium | High |
| Financial document and files | Medium | Medium | Medium |
| Backup file | Medium | High | High |
| Email communication | Medium | Medium | Medium |
| Admin Laptop | Low | High | Medium |

## 4.3.2 Recommended Security Control

The data asset with the highest risk in the cybersecurity threat assessment is taken to be customer personal and financial data stored in the organization’s CRM system. This is very sensitive data and an ideal target for cyber-attacks (data breaches, phishing and insider threats). Some of the security that provide as per the organization need includes:

* Firewall Deployment: Each site will implement a Fortinet FortiGate 60f firewall to implement centralized traffic filtering, application control, and intrusion detection, thus maintaining the same level of network security in all the branch offices.[[2]](#footnote-2)
* Encryption: Data will be encrypted while in motion as well as at rest, applying such industry standards as SSL and TLS. This also includes secure storage encryption and encrypted VPN/cloud communications for the security of sensitive information.
* Access Control: Role-Based Access Control (RBAC) will be applied using Microsoft Active Directory, whereby the user’s access systems and data related to their roles, hence improving internal security.
* VPN and Remote Access: IPsec VPNs with MFA will be deployed for all remote locations and branch offices to secure the channels of connectivity, keeping the data intact and verifying the user identity before access to the resources.
* Endpoint Protection: The endpoints will all benefit from enhanced protection, such as anti-virus, anti-malware, and EDR, among other features, with automatic updates and vulnerability patches so that the threat of device-level breaches is minimized.
* Wi-Fi Security: Wi-Fi networks will employ WPA2 Enterprise 802.1x using RADIUS and VLAN’s to separate guest and internal traffic for better wireless access control and internal exposure reduction.[[3]](#footnote-3)

To reduce these risks of this asset, three security controls are recommended on the basis of NIST SP800-53 and unit materials:

***Access Control (AC-2: Account Management)***

How it reduces risk: Access control prevents unauthorized users from accessing data and reduces exposure to insider threats and unauthorized access to data.[[4]](#footnote-4)

Implementation in the scenario: The CRM system’s cloud environment and CRM system will be subject to Role-Based Access Control (RBAC).[[5]](#footnote-5) Employees will only access data for their working purposes. This will be enforced with the help of cloud IAM services such as AWS IAM or Azure AD.

Network design considerations: Access policies will be only defined and deployed in the central directory service, part of the network authentication layer. The need is to upgrade the directory services and train the work-force.

Disadvantages: May induce user frustration in the event there is minimal access or tardy access requests if there are changes to job roles.

***Encryption (SC-12: Cryptographic Key Establishment & (SC-13: Cryptographic Protection)***

How it reduces risk: Encryption guarantees that in case of interception or interrogation of data by unauthorized individuals, the data is unavailable unless decryption keys are used.[[6]](#footnote-6)

Implementation in the scenario: AES-256 encryption of data at rest and in transit. By default, data stored in the cloud database (e.g., Amazon RDS, Azure SQL) will be encrypted. A TLS 1.3 protocol will be adhered to for shifting all the data.

Network design considerations: All endpoints and databases will be protected using encryption standards. Key management will be managed through native key-management services offered off-cloud, or using cloud-native Key Management Services (KMS).

Disadvantages: May add a bit to the system overhead and latency, and key management needs special expertise.

***Audit and Monitoring (AU-6: Audit Review, Analysis, and Reporting)***

How it reduces risk: Monitoring enables tracking down and addressing security incidents in a timely manner so that the damage due to breaches or misuse is minimized.[[7]](#footnote-7)

Implementation in the scenario: The logging and SIEM (Security Information and Event Management) instruments, such as Azure Sentinel or AWS CloudTrail/GuardDuty, will be used for tracking the activity of every user and events of all the systems.[[8]](#footnote-8)

Network design considerations: All vital systems, such as CRM, HR, and file servers, will be used to obtain logs. Suspicious activities will have alerts set for them.

Disadvantages: Can prove to be resource-heavy to administer, and it can fuel privacy issues among the users being surveilled.

1. <https://www.researchgate.net/publication/361513517_Cybersecurity_Risk_Assessment_and_Management> [↑](#footnote-ref-1)
2. <https://www.researchgate.net/publication/382057178_The_Importance_of_Network_Security_in_Protecting_Sensitive_Data_and_Information> [↑](#footnote-ref-2)
3. <https://www.researchgate.net/publication/375570681_Wireless_Technology_Security_and_Privacy_A_Comprehensive_Study> [↑](#footnote-ref-3)
4. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf> [↑](#footnote-ref-4)
5. <https://www.researchgate.net/publication/383295659_Role-Based_Access_Control_RBAC_Enabled_Secure_and_Efficient_Data_Processing_Framework_for_IoT_Networks> [↑](#footnote-ref-5)
6. <https://www.researchgate.net/publication/351100272_An_intelligent_cryptographic_key_management_model_for_secure_communications_in_distributed_industrial_intelligent_systems> [↑](#footnote-ref-6)
7. <https://www.researchgate.net/publication/357861875_Effectiveness_of_cybersecurity_audit> [↑](#footnote-ref-7)
8. <https://www.mdpi.com/2624-800X/5/1/2> [↑](#footnote-ref-8)