**CY5200 Security Risk Management and Assessment**

**Module 2 Assignment**

**By: Kalp Shah**

**002232460**

**List of assets, threats, vulnerabilities, controls, and policies**

**Scale**

|  |  |
| --- | --- |
| **Risk** | **Range** |
| H | 75-100 |
| M | 36-74 |
| L | 0-35 |

**Assets**

|  |  |  |  |
| --- | --- | --- | --- |
| **Number** | **Asset** | **Description** | **Value** |
| A1 | Financial Resources | Includes paychecks, transfers, and balances | H |
| A2 | Personnel Information | Includes information about the employees like name, email addresses, paycheck details etc. | H |
| A3 | Documents | Includes draft regulations, contracts and procurement documents, draft regulations, reports, and memos. | H |
| A4 | PC | Hardware entity for personnels of HGA for their duties like submitting timesheets. | H |
| A5 | Employee Confidence | Crucial asset for HGA displaying trust for the agency. | H |
| A6 | Reputation | Intangible asset pertaining image and credibility of HGA. | H |
| A7 | Mainframe | Storage and retrieval medium of the databases from other agencies. | H |
| A8 | LAN Server | Central network component between PCs and other hardware entities and shared programs, storage etc. | H |
| A9 | Storage | Databases for storing general and sensitive information both regarding financials and personnels. | H |
| A10 | WAN | Connects different agencies LAN networks and mainframe for information sharing and smooth communications | H |
| A12 | Modem Pool | Service for employees who are travelling for checking emails and dial-ins. | H |
| A13 | Console | Interface for server administrators to perform sensitive and crucial tasks securely. | H |
| A14 | Printers | For printouts of documents via LAN by HGA employees. | H |
| A15 | Router | Provides an internet connection and protocol translation. | H |
| A16 | Programs and Tools | Interface for HGA personnels to perform their duties. | H |

**Threats**

|  |  |
| --- | --- |
| **Number** | **Threat** |
| T1 | Payroll Frauds |
| T2 | Payroll Errors |
| T3 | Interruption of Operations |
| T4 | Disclosure and Brokerage of Information |
| T5 | Network related Threats |
| T6 | Virus and Malware |
| T7 | Unauthorized Access |
| T8 | Theft |
| T9 | Natural Disaster |

**Vulnerabilities**

|  |  |
| --- | --- |
| **Number** | **Vulnerability** |
| V1 | Falsified Timesheets |
| V2 | Unauthorized Access |
| V3 | Bogus Time and Attendance Applications |
| V4 | Unauthorized Modification of the data |
| V5 | Payroll Errors |
| V6 | Lack of Contingency Planning |
| V7 | Virus/Malware spread |
| V8 | Corruption and Loss of Data |
| V9 | Network Related |
| V10 | Lack of physical security |
| V11 | Inadequate security of storage, database, and mainframe |
| V12 | Employee not compliant of PCs security |

**Current Security Controls and Policies(CSCP)**

|  |  |  |
| --- | --- | --- |
| **Number** | **Category** | **Description** |
| CSCP 1 | Security Manual | In compliance with federal and financial policies |
| CSCP 2 | General Use | Duties and privileges segregation of personnels |
| CSCP 3 | General | Security awareness training |
| CSCP 4 | General | Password selection and security policy |
| CSCP 5 | General | Access Control Mechanism |
| CSCP 6 | Payroll Frauds and Errors | Time and attendance application |
| CSCP 7 | Payroll Frauds and Errors | Sign and submit time sheet |
| CSCP 8 | Payroll Frauds and Errors | Data validation, verification, and authorization |
| CSCP 9 | Payroll Frauds and Errors | Access control and identification |
| CSCP 10 | Payroll Frauds and Errors | Containerization of the server |
| CSCP 11 | Payroll Frauds and Errors | Time sheet verification twice and sanity checks |
| CSCP 12 | Payroll Frauds and Errors | Segregation of personnel duties |
| CSCP 13 | Payroll Frauds and Errors | Digital signature for integrity |
| CSCP 14 | Payroll Frauds and Errors | Regular backup |
| CSCP 15 | Interruption of Operations | COG Contingency Planning and Testing |
| CSCP 16 | Interruption of Operations | Spare PCs, LAN server and cables, and drives in case of malfunctions |
| CSCP 17 | Interruption of Operations | Installation of licensed software and regular installation of patches |
| CSCP 18 | Interruption of Operations | Log Audit |
| CSCP 19 | Interruption of Operations | Division Contingency Planning |
| CSCP 20 | Disclosure or Brokerage of Information | Need to know policy |
| CSCP 21 | Disclosure or Brokerage of Information | Secure and guard physical and digital storage |
| CSCP 22 | Disclosure or Brokerage of Information | Policy on PC locks |
| CSCP 23 | Disclosure or Brokerage of Information | Group oriented access control |
| CSCP 24 | Disclosure or Brokerage of Information | Security awareness training |
| CSCP 25 | Network Threats | Filtered and restricted network activity |
| CSCP 26 | Network Threats | Packets monitoring |
| CSCP 27 | Network Threats | Restricted remote logins and dial-in access |
| CSCP 28 | Non-HGA Computer Systems | Policy for the HGA system components provided by external organization |

**New security policies (NSP) recommended by CISO and team members**

|  |  |  |
| --- | --- | --- |
| **Number** | **Category** | **Description** |
| NSP 1 | Payroll Frauds | Advanced authentication mechanisms(smart tokens for One Time Password) |
| NSP 2 | Payroll Frauds | Administrative Procedures |
| NSP 3 | Payroll Frauds | Monitoring |
| NSP 4 | Payroll Frauds | Implement cryptographic techniques – Digital Signature |
| NSP 5 | Payroll Errors | Greater and improved compliance based on incentive system |
| NSP 6 | Continuity of Operations | Regular internal training and awareness sessions |
| NSP 7 | Continuity of Operations | Contingency plan rehearsal |
| NSP 8 | Continuity of Operations | Virus Prevention procedures |
| NSP 9 | Continuity of Operations | Improved backup procedures |
| NSP 10 | Information Disclosure/Brokering | Enhanced security refresher courses |
| NSP 11 | Information Disclosure/Brokering | Changes in storage policy for sensitive information |
| NSP 12 | Information Disclosure/Brokering | Installing and reviewing activity logs |
| NSP 13 | Network Threats | Stronger Identity and Access Management controls for dial-in |
| NSP 14 | Network Threats | Restricting sensitive outbound traffic |
| NSP 15 | Network Threats | Encrypted modems |
| NSP 16 | Network Threats | Inbound and outbound traffic encryption via WAN |

**Subset selection of assets, threats, and vulnerabilities**

|  |  |  |  |
| --- | --- | --- | --- |
| **Number** | **Asset** | **Description** | **Value** |
| A1 | Financial Resources | Includes paychecks, transfers, and balances | H |
| A2 | Personnel Information | Includes information about the employees like name, email addresses, paycheck details etc. | H |
| A4 | PC | Hardware entity for personnels of HGA for their duties like submitting timesheets. | H |
| A8 | LAN Server | Central network component between PCs and other hardware entities and shared programs, storage etc. | H |

|  |  |
| --- | --- |
| **Number** | **Threat** |
| T1 | Payroll Frauds |
| T3 | Interruption of Operations |
| T4 | Disclosure and Brokerage of Information |
| T9 | Natural Disaster |

|  |  |
| --- | --- |
| **Number** | **Vulnerability** |
| V1 | Falsified Timesheets |
| V2 | Unauthorized Access |
| V8 | Corruption and Loss of Data |
| V11 | Inadequate security of storage, database, and mainframe |

**Threat/Vulnerabilities pairs for assets A1, A2, A3, A4 with probabilities ranging from 0-100**

**Taking assumptions:**

T1, T3, T4 exploits V1 on assets A1, A2, A4

T1, T3, T4 exploits V2 on assets A2, A4, A8

T3, T4, T9 exploits V8 on assets A1, A2, A4, A8

T1, T3, T4, T9 exploits V11 on assets A1, A2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | H | H | H | 0 |
| V2 on A2, A4, A8 | H | H | H | 0 |
| V8 on A1, A2, A4, A8 | 0 | H | L | H |
| V11 on A1, A2 | M | H | H | H |

**Explanation to the assigned values of selected threats**

**Payroll fraud** is very critical. It is one of the most common threats that leads to significant loss of the agencies. This financial fraud generally exploits lack of authentication and authorization measures along with irregular audit and security checks.

**Interruption of Operations** is very important for the HGA. The reputation is directly connected to this threat along with the employee confidence. Hindering operations can lead to significant delay in paying the personnels of all federal agencies which is a crucial and most important sector of any nation.

**Disclosure and Brokerage of Information** can cause great damage. Such threat affects the sensitive information of the financial assets and personnels that not only breach trust and reputation but can also be misused for malicious purposes.

**Natural Disasters** could be small or could be catastrophic. In any case, the destruction of property in terms of information or hardware results in a serious loss to HGA and all other agencies linked to it.

**Asset Vulnerability pairs**

|  |  |
| --- | --- |
| **Asset** | **Vulnerability** |
| A1 Financial Resources | V1 Falsified Timesheets  V8 Corruption and Loss of Data  V11 Inadequate security of storage, database, and mainframe |
| A2 Personnel Information | V1 Falsified Timesheets  V2 Unauthorized Access  V8 Corruption and Loss of Data  V11 Inadequate security of storage, database, and mainframe |
| A4 PC | V2 Unauthorized Access  V8 Corruption and Loss of Data |
| A8 LAN Server | V2 Unauthorized Access  V8 Corruption and Loss of Data |

**Assumed Values when risk value(s) are considered:**

|  |  |
| --- | --- |
| **Addition** | **Multiplication** |
| H+H=H | H\*H=H |
| H+M=H | H\*M=H |
| H+L=H | H\*L=M |
| M+L=M | M\*L=M |
| M+M=M | M\*M=M |
| L+L=L | L\*L=L |

**Initial Risk Impact**

For the below matrix, if threat x vulnerability pair exists, probability for the lost asset is H keeping resilience as 0.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T4xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | H | 0 | 0 | H | H | 0 | H | H | H | 0 | H | H | 0 | 0 | H | H |
| A2 | H | H | 0 | H | H | H | H | H | H | H | H | H | 0 | 0 | H | H |
| A4 | H | H | 0 | 0 | H | H | H | 0 | H | H | H | H | 0 | 0 | H | 0 |
| A8 | 0 | H | 0 | 0 | 0 | H | H | 0 | 0 | H | H | 0 | 0 | 0 | H | 0 |

**Scenario 1 :**

Estimating Risks H, M, L based on the new Vulnerabilities discovered by new CISO and team

**Residual Asset Security Risks**

Risk of asset A1: H\*(H+H+H+H+L+M+H+H+H) = H

Risk of asset A2:

H \* (H+H+H+H+H+H+H+L+H+M+H+H+H) = H

Risk of asset A4: H\* (H+H+H+H+L+H+H+H) = H

Risk of asset A8: H\* (H+H+H+H+L+H) = H

**Residual Vulnerability Security Risk**

Risk due to V1: [(H\*H) + (H\*H) + (H\*H)]= H

Risk due to V2: [(H\*H) + (H\*H) + (H\*H)] = H

Risk due to V8: [(H\*H) + (H\*H) + (H\*H) + (H\*H)] = H

Risk due to V11: [(H\*H) + (H\*H) + (H\*H)] = H

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A2 | H | 1 |
| A1 | H | 2 |
| A4 | H | 3 |
| A8 | H | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V8 Corruption and Loss of Data | H | 1 |
| V1 Falsified Timesheets | H | 2 |
| V2 Unauthorized Access | H | 3 |
| V11 Inadequate security of storage, database, and mainframe | H | 4 |

**Scenario 2:**

Considering proposed New Controls NC from new CISO, on Critical Assets where NC are applicable reduce TV probabilities or RI percentages. Estimating updated Residual Critical Asset Risks and rankings, Total Asset Risk, and Vulnerability Risk rankings.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | M | H | H | 0 |
| V2 on A2, A4, A8 | H | H | M | 0 |
| V8 on A1, A2, A4, A8 | 0 | M | 0 | H |
| V11 on A1, A2 | L | H | M | H |

**Residual Asset Security Risks**

Risk of asset A1: H\*(M+H+H+M+H+L+H+M+H) = H

Risk of asset A2:

H \* (M+H+H+H+H+M+M+H+L+H+M+H) = H

Risk of asset A4: H\* (M+H+H+M+H) = H

Risk of asset A8: H\* (H+H+M+M+H) = H

**Residual Vulnerability Security Risk**

Risk due to V1: [(H\*H) + (H\*H) + (H\*H)]= H

Risk due to V2: [(H\*H) + (H\*H) + (H\*H)] = H

Risk due to V8: [(H\*H) + (H\*H) + (H\*H) + (H\*H)] = H

Risk due to V11: [(H\*H) + (H\*H) + (H\*H)] = H

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A2 | H | 1 |
| A1 | H | 2 |
| A4 | H | 3 |
| A8 | H | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V8 Corruption and Loss of Data | H | 1 |
| V1 Falsified Timesheets | H | 2 |
| V2 Unauthorized Access | H | 3 |
| V11 Inadequate security of storage, database, and mainframe | H | 4 |

**Scenario 3 :**

**Considering Management-Operational-Technical MOT controls, in addition to Current and NC controls, where MOT controls are applicable reduce TV probabilities or RI percentages. Estimating updated Residual Critical Asset Risks and rankings, Total Asset**

**Risk, and Vulnerability Risk rankings**

|  |  |  |
| --- | --- | --- |
| **Management** | **Operational** | **Technical** |
| Policies(M1) | Preparing for Contingencies and Disasters(M5) | Identification and Authentication(M9) |
| Program Management(M2) | Incident Handling and Reporting(M6) | Logical Access Control(M10) |
| Risk Management(M3) | Awareness, Training and Education(M7) | Audit Trails(M11) |
| Assurance(M4) | Physical and Environmental Security(M8) | Cryptography(M12) |

|  |  |  |  |
| --- | --- | --- | --- |
| **Number** | **Category** | **Description** | **MOT Controls** |
| CSCP 1 | Security Manual | In compliance with federal and financial policies | 1 |
| CSCP 2 | General Use | Duties and privileges segregation of personnels | 2,3,5,6 |
| CSCP 3 | General | Security awareness training | 3,4,7 |
| CSCP 4 | General | Password selection and security policy | 1,3 |
| CSCP 5 | General | Access Control Mechanism | 4,6,9,10 |
| CSCP 6 | Payroll Frauds and Errors | Time and attendance application | 10,11 |
| CSCP 7 | Payroll Frauds and Errors | Sign and submit time sheet | 10,11 |
| CSCP 8 | Payroll Frauds and Errors | Data validation, verification, and authorization | 4,9,10,11 |
| CSCP 9 | Payroll Frauds and Errors | Access control and identification | 4,6,9,10 |
| CSCP 10 | Payroll Frauds and Errors | Containerization of the server | 5 |
| CSCP 11 | Payroll Frauds and Errors | Time sheet verification twice and sanity checks | 4 |
| CSCP 12 | Payroll Frauds and Errors | Segregation of personnel duties | 2 |
| CSCP 13 | Payroll Frauds and Errors | Digital signature for integrity | 4,12 |
| CSCP 14 | Payroll Frauds and Errors | Regular backup | 3,4,5 |
| CSCP 15 | Interruption of Operations | COG Contingency Planning and Testing | 3,4,6 |
| CSCP 16 | Interruption of Operations | Spare PCs, LAN server and cables, and drives in case of malfunctions | 3,5 |
| CSCP 17 | Interruption of Operations | Installation of licensed software and regular installation of patches | 1,2 |
| CSCP 18 | Interruption of Operations | Log Audit | 6,11 |
| CSCP 19 | Interruption of Operations | Division Contingency Planning | 3,4,6 |
| CSCP 20 | Disclosure or Brokerage of Information | Need to know policy | 1,3,9 |
| CSCP 21 | Disclosure or Brokerage of Information | Secure and guard physical and digital storage | 5,8 |
| CSCP 22 | Disclosure or Brokerage of Information | Policy on PC locks | 1,4,7,8,10 |
| CSCP 23 | Disclosure or Brokerage of Information | Group oriented access control | 10 |
| CSCP 24 | Disclosure or Brokerage of Information | Security awareness training | 3,7 |
| CSCP 25 | Network Threats | Filtered and restricted network activity | 4,12 |
| CSCP 26 | Network Threats | Packets monitoring | 11 |
| CSCP 27 | Network Threats | Restricted remote logins and dial-in access | 9,10 |
| CSCP 28 | Non-HGA Computer Systems | Policy for the HGA system components provided by external organization | 1,3,4 |

**Threat Vulnerability pairs probabilities after implementing MOT controls**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | M | M | H | 0 |
| V2 on A2, A4, A8 | H | M | M | 0 |
| V8 on A1, A2, A4, A8 | 0 | M | 0 | M |
| V11 on A1, A2 | L | M | L | M |

**Residual Asset Security Risks**

Risk of asset A1: H\*(M+M+H+M+M+L+M+L+M) = H

Risk of asset A2:

H \* (M+M+H+H+M+M+M+M+L+M+L+M) = H

Risk of asset A4: H\* (M+M+H+H+M+M+M+M) = H

Risk of asset A8: H\* (H+M+M+M+M) = H

**Residual Vulnerability Security Risk**

Risk due to V1: [(H\*H) + (H\*H) + (H\*H)]= H

Risk due to V2: [(H\*H) + (H\*H) + (H\*H)] = H

Risk due to V8: [(H\*M) + (H\*M) + (H\*M) + (H\*M)] = H

Risk due to V11: [(H\*M) + (H\*M)] = H

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A2 | H | 1 |
| A1 | H | 2 |
| A4 | H | 3 |
| A8 | H | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V8 Corruption and Loss of Data | H | 1 |
| V1 Falsified Timesheets | H | 2 |
| V2 Unauthorized Access | H | 3 |
| V11 Inadequate security of storage, database, and mainframe | H | 4 |

**Prevention Strategy Step P1:**

The ranking above shows V8 – Corruption and Loss of Data is most prone to be exploited via threats. To reduce it, the organization should implement some counter measures. Recovery strategies and data quality checks can significantly improve the vulnerability risk.  
  
**Threat Vulnerability Pair for V8 after applying prevention strategy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | M | M | H | 0 |
| V2 on A2, A4, A8 | H | M | M | 0 |
| **V8 on A1, A2, A4, A8** | **0** | **L** | **0** | **L** |
| V11 on A1, A2 | L | M | L | M |

**Residual Asset Security Risks**

Risk of asset A1: H\*(M+M+H+L+L+L+M+L+M) = H

Risk of asset A2:

H \* (M+M+H+H+M+M+L+L+L+M+L+M) = H

Risk of asset A4: H\* (M+M+H+H+M+M+L+L) = H

Risk of asset A8: H\* (H+M+M+L+L) = H

**Residual Vulnerability Security Risk**

Risk due to V1: [(H\*H) + (H\*H) + (H\*H)]= H

Risk due to V2: [(H\*H) + (H\*H) + (H\*H)] = H

**Risk due to V8: [(H\*L) + (H\*L) + (H\*L) + (H\*L)] = M**

Risk due to V11: [(H\*M) + (H\*M)] = H

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A2 | H | 1 |
| A1 | H | 2 |
| A4 | H | 3 |
| A8 | H | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V2 Unauthorized Access | H | 1 |
| V1 Falsified Timesheets | H | 2 |
| V11 Inadequate security of storage, database, and mainframe | H | 3 |
| V8 Corruption and Loss of Data | M | 4 |

**Prevention Strategy Step P2:**

The ranking from P1 shows V2 – Unauthorized Access is most prone to be exploited via threats. To reduce it, the organization should implement some counter measures. Two factor and multi-factor authentication can significantly improve the vulnerability risk.

**Threat Vulnerability Pair for V8 after applying prevention strategy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | M | M | H | 0 |
| **V2 on A2, A4, A8** | **L** | **L** | **L** | **0** |
| V8 on A1, A2, A4, A8 | 0 | L | 0 | L |
| V11 on A1, A2 | L | M | L | M |

**Residual Asset Security Risks**

Risk of asset A1: H\*(M+M+H+L+L+L+M+L+M) = H

Risk of asset A2:

H \* (M+M+H+L+M+L+L+L+L+M+L+M) = H

Risk of asset A4: H\* (M+M+H+L+L+L +L+L) = H

**Risk of asset A8: H\* (L+L+L+L+L) = M**

**Residual Vulnerability Security Risk**

Risk due to V1: [(H\*H) + (H\*H) + (H\*H)]= H

**Risk due to V2: [(H\*L) + (H\*L) + (H\*L)] = M**

Risk due to V8: [(H\*L) + (H\*L) + (H\*L) + (H\*L)] = M

Risk due to V11: [(H\*M) + (H\*M)] = H

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A2 | H | 1 |
| A1 | H | 2 |
| A4 | H | 3 |
| **A8** | **M** | **4** |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V1 Falsified Timesheets | H | 1 |
| V11 Inadequate security of storage, database, and mainframe | H | 2 |
| **V2 Unauthorized Access** | **M** | **3** |
| V8 Corruption and Loss of Data | M | 4 |

**Response (Resilience) Strategy Step RE1**

|  |  |  |
| --- | --- | --- |
| **Management** | **Operational** | **Technical** |
| Policies(M1) | Preparing for Contingencies and Disasters(M5) | Identification and Authentication(M9) |
| Program Management(M2) | Incident Handling and Reporting(M6) | Logical Access Control(M10) |
| Risk Management(M3) | Awareness, Training and Education(M7) | Audit Trails(M11) |
| Assurance(M4) | Physical and Environmental Security(M8) | Cryptography(M12) |

After applying MOT controls in the preventive strategy steps for other remaining vulnerabilities. After completing the calculations, the last Threat Vulnerability pair matrices look as:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | M | M | H | 0 |
| V2 on A2, A4, A8 | L | L | L | 0 |
| V8 on A1, A2, A4, A8 | 0 | L | 0 | L |
| V11 on A1, A2 | L | M | L | M |

**Updated Risk Impacts**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T4xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | H | 0 | 0 | H | H | 0 | H | H | H | 0 | H | H | 0 | 0 | H | H |
| A2 | H | H | 0 | H | H | H | H | H | H | H | H | H | 0 | 0 | H | H |
| A4 | H | H | 0 | 0 | H | H | H | 0 | H | H | H | H | 0 | 0 | H | 0 |
| A8 | 0 | H | 0 | 0 | 0 | H | H | 0 | 0 | H | H | 0 | 0 | 0 | H | 0 |

**Residual Asset Security Risks**

Risk of asset A1: H\*(H\*M + H\*L + H\*M + H\*L + H\*M + H\*H + H\*L + H\*L + H\*M) = H

Risk of asset A2:

H \* (H\*M + H\*L + H\*L + H\*M + H\*L + H\*L + H\*M + H\*H + H\*L + H\*L + H\*L + H\*M) = H

Risk of asset A4: H\* (H\*M + H\*L + H\*M + H\*L + H\*L + H\*H + H\*L + H\*L + H\*L) = H

Risk of asset A8: H\* (H\*L + H\*L + H\*L + H\*L + H\*L) = H

**Residual Vulnerability Security Risk**

Risk due to V1: H\*(H\*M+H\*M+H\*H) + H\*(H\*M+H\*M+H\*H) + H\*(H\*M+H\*M+H\*H) = H

Risk due to V2:H\*(H\*L+H\*L+H\*L) + H\*(H\*L+H\*L+H\*L) + H\*(H\*L+H\*L+H\*L) = H

Risk due to V8: H\*(H\*L+H\*L+H\*L) + H\*(H\*L+H\*L+H\*L) + H\*(H\*L+H\*L+H\*L) + H\*(H\*L+H\*L+H\*L) = H

Risk due to V11: H\*(H\*L+H\*M+H\*L+H\*M) + H\*(H\*L+H\*M+H\*L+H\*M) = H

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A2 | H | 1 |
| A1 | H | 2 |
| A4 | H | 3 |
| A8 | H | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V1 Falsified Timesheets | H | 1 |
| V11 Inadequate security of storage, database, and mainframe | H | 2 |
| V2 Unauthorized Access | H | 3 |
| V8 Corruption and Loss of Data | H | 4 |

**Response (Resilience) Strategy Step RE2**

In the Response Resilience Strategy RE1, the highest ranking for asset risk is **A2 Personnel Information.** To safeguards personnel information, encryption and cryptography helps to reduce the risk asserted on the asset.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | M | M | H | 0 |
| V2 on A2, A4, A8 | L | L | L | 0 |
| V8 on A1, A2, A4, A8 | 0 | L | 0 | L |
| V11 on A1, A2 | L | M | L | M |

**Updated Risk Impacts**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T4xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | H | 0 | 0 | H | H | 0 | H | H | H | 0 | H | H | 0 | 0 | H | H |
| **A2** | **0** | **L** | **0** | **L** | **0** | **L** | **L** | **0** | **0** | **L** | **L** | **L** | **0** | **0** | **L** | **0** |
| A4 | H | H | 0 | 0 | H | H | H | 0 | H | H | H | H | 0 | 0 | H | 0 |
| A8 | 0 | H | 0 | 0 | 0 | H | H | 0 | 0 | H | H | 0 | 0 | 0 | H | 0 |

**Residual Asset Security Risks**

Risk of asset A1: H\*(H\*M + H\*L + H\*M + H\*L + H\*M + H\*H + H\*L + H\*L + H\*M) = H

Risk of asset A2:

H \* (L\*L + L\*L + L\*L + L\*L+ L\*L + L\*L + L\*L) = M

Risk of asset A4: H\* (H\*M + H\*L + H\*M + H\*L + H\*L + H\*H + H\*L + H\*L + H\*L) = H

Risk of asset A8: H\* (H\*L + H\*L + H\*L + H\*L + H\*L) = H

**Residual Vulnerability Security Risk**

Risk due to V1: H\*(H\*M+H\*M+H\*H) + H\*(H\*M+H\*M+H\*H) + H\*(H\*M+H\*M+H\*H) = H

Risk due to V2: H\*(L\*L+L\*L+L\*L) + H\*(H\*L+H\*L+H\*L) + H\*(H\*L+H\*L+H\*L) = H

Risk due to V8: H\*(H\*L+H\*L+H\*L) + H\*(L\*L+L\*L) + H\*(H\*L+H\*L+H\*L) + H\*(H\*L+H\*L+H\*L) = H

Risk due to V11: H\*(H\*L+H\*M+H\*L+H\*M) + H\*(H\*L+H\*L) = H

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A1 | H | 1 |
| A4 | H | 2 |
| A8 | H | 3 |
| A2 | M | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V1 Falsified Timesheets | H | 1 |
| V11 Inadequate security of storage, database, and mainframe | H | 2 |
| V2 Unauthorized Access | H | 3 |
| V8 Corruption and Loss of Data | H | 4 |

**Mixed Strategy Step 1: Start with TV and RI from Scenario 3 and apply 2-Factor**

**Authentication. The results should be the same as above.**

Taking initial TV matrix from Scenario 3 where resilience is considered to be 0 and likelihood to be 100%.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | M | M | H | 0 |
| V2 on A2, A4, A8 | H | M | M | 0 |
| V8 on A1, A2, A4, A8 | 0 | M | 0 | M |
| V11 on A1, A2 | L | M | L | M |

Applying 2-Factor Authentication,

**Updated Threat Vulnerability pair values**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | L | M | L | 0 |
| V2 on A2, A4, A8 | M | L | L | 0 |
| V8 on A1, A2, A4, A8 | 0 | M | 0 | M |
| V11 on A1, A2 | L | L | 0 | L |

**Updated Risk Impact Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T4xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | M | 0 | 0 | L | M | 0 | M | L | M | 0 | M | L | 0 | 0 | M | L |
| A2 | M | L | 0 | L | M | L | M | L | M | L | M | L | 0 | 0 | M | L |
| A4 | M | L | 0 | 0 | M | L | M | 0 | M | L | M | M | 0 | 0 | M | 0 |
| A8 | 0 | M | 0 | 0 | 0 | M | M | 0 | 0 | M | M | 0 | 0 | 0 | M | 0 |

**Residual Asset Security Risks**

Risk of asset A1: H\*(M\*L+L\*L+M\*M+M\*M+M\*L+M\*M) = H

Risk of asset A2:

H \* (M\*L+L\*M+L\*L+M\*M+L\*L+M\*M+L\*L+M\*L+L\*L+M\*M) = H

Risk of asset A4: H\* (M\*L+L\*M+M\*M+L\*L+M\*M+M\*L+L\*L+M\*M) = H

Risk of asset A8: H\* (M\*M+M\*L+M\*M+M\*L+M\*M) = H

**Residual Vulnerability Security Risk**

Risk due to V1: H\*(M\*M+M\*L+M\*M) + H\*(M\*M+M\*L+M\*M) + H\*(M\*M+M\*L+M\*M) = H

Risk due to V2:H\*(L\*M+L\*L+L\*L) + H\*(L\*M+L\*L+L\*L) + H\*(L\*M+L\*L+L\*L) = H

Risk due to V8: H\*(M\*M+M\*M) + H\*(M\*M+M\*M) + H\*(M\*M+M\*M) + H\*(M\*M+M\*M) = H

Risk due to V11: H\*(L\*L+L\*L+L\*L) + H\*(L\*L+L\*L+L\*L) = M

**Mixed Strategy Step 2: Start with TV and RI from Scenario 3 and apply VPN.**

**Estimate updated Residual Critical Asset Risk rankings, Total Asset Risk, and**

**Vulnerability Risk rankings.**

**Updated Threat Vulnerability pair values**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | L | L | L | 0 |
| V2 on A2, A4, A8 | L | 0 | L | 0 |
| V8 on A1, A2, A4, A8 | 0 | M | 0 | M |
| V11 on A1, A2 | L | L | 0 | L |

**Updated Risk Impact Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T4xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | L | 0 | 0 | L | L | 0 | L | L | L | 0 | L | L | 0 | 0 | L | L |
| A2 | L | 0 | 0 | L | L | L | L | L | L | L | L | L | 0 | 0 | L | L |
| A4 | L | L | 0 | 0 | M | L | M | 0 | M | L | M | M | 0 | 0 | M | 0 |
| A8 | 0 | L | 0 | 0 | 0 | M | M | 0 | 0 | M | M | 0 | 0 | 0 | M | 0 |

**Residual Asset Security Risks**

Risk of asset A1: H\*(L\*L+\*L\*L+L\*L+L\*M+L\*L+L\*L+L\*M+L\*L) = H

Risk of asset A2:

H \* (L\*L+L\*L+L\*L+L\*M+L\*L+L\*L+L\*L+L\*M+L\*L) = H

Risk of asset A4: H\* (L\*L+L\*L+M\*L+M\*M+M\*L+L\*L+M\*M) = H

Risk of asset A8: H\* (L\*L+M\*M+M\*L+M\*M) = H

**Residual Vulnerability Security Risk**

Risk due to V1: H\*(L\*L+L\*L+L\*L) + H\*(L\*L+L\*L+L\*L) + H\*(L\*L+M\*L+M\*L) = H

Risk due to V2:H\*(L\*L+L\*L) + H\*(L\*L+L\*L) + H\*(L\*L+L\*L) + H\*(L\*L+M\*L) = H

Risk due to V8: H\*(L\*L+L\*L) + H\*(L\*L+L\*L) + H\*(M\*M+M\*M) + H\*(M\*M+M\*M) = H

Risk due to V11: H\*(L\*L+L\*L+L\*L) + H\*(L\*L+L\*L+L\*L) = M

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A1 | H | 1 |
| A4 | H | 2 |
| A8 | H | 3 |
| A2 | H | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V1 Falsified Timesheets | H | 1 |
| V2 Unauthorized Access | H | 2 |
| V8 Corruption and Loss of Data | H | 3 |
| V11 Inadequate security of storage, database, and mainframe | M | 4 |

**Mixed Strategy Step 3: Start with TV and RI from Scenario 3 and apply Redudant Server. Estimate updated Residual Critical Asset Risk rankings, Total Asset Risk, and Vulnerability Risk rankings.**

**Updated Threat Vulnerability pair values**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | L | L | L | 0 |
| V2 on A2, A4, A8 | L | 0 | L | 0 |
| V8 on A1, A2, A4, A8 | 0 | L | 0 | L |
| V11 on A1, A2 | L | 0 | 0 | 0 |

**Updated Risk Impact Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T4xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | L | 0 | 0 | L | L | 0 | L | L | L | 0 | L | L | 0 | 0 | 0 | 0 |
| A2 | L | 0 | 0 | L | L | L | L | L | L | L | L | L | 0 | 0 | 0 | 0 |
| A4 | L | L | 0 | 0 | M | L | L | 0 | M | L | L | L | 0 | 0 | L | 0 |
| A8 | 0 | L | 0 | 0 | 0 | M | L | 0 | 0 | L | L | 0 | 0 | 0 | L | 0 |

**Residual Asset Security Risks**

Risk of asset A1: H\*(L\*L+L\*L+L\*L+L\*L+L\*L) = M

Risk of asset A2:

H \* (L\*L+ L\*L+L\*L+L\*L+L\*L+L\*L) = M

Risk of asset A4: H\* (L\*L+L\*L+M\*L+L\*L+M\*L+L\*L+L\*L) = H

Risk of asset A8: H\* (L\*L+ L\*L+L\*L+L\*L+L\*L) = M

**Residual Vulnerability Security Risk**

Risk due to V1: H\*(L\*L+L\*L+L\*L) + H\*(L\*L+L\*L+L\*L) + H\*(L\*L+M\*L+M\*L) = H

Risk due to V2:H\*(L\*L+L\*L) + H\*(L\*L+L\*L) + H\*(L\*L+L\*L) + H\*(L\*L+M\*L) = H

Risk due to V8: H\*(L\*L) + H\*(L\*L) + H\*(L\*L+L\*L) + H\*(L\*L+L\*L) = M

Risk due to V11: H\*(L\*L) + H\*(L\*L) = M

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A4 | H | 1 |
| A1 | M | 2 |
| A8 | M | 3 |
| A2 | M | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V1 Falsified Timesheets | H | 1 |
| V2 Unauthorized Access | H | 2 |
| V8 Corruption and Loss of Data | M | 3 |
| V11 Inadequate security of storage, database, and mainframe | M | 4 |

**Mixed Strategy Step 4: Start with TV and RI from Scenario 3 and apply Mirror Site. Estimate updated Residual Critical Asset Risk rankings, Total Asset Risk, and Vulnerability Risk rankings.**

**Updated Threat Vulnerability pair values**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | L | L | L | 0 |
| V2 on A2, A4, A8 | L | 0 | L | 0 |
| V8 on A1, A2, A4, A8 | 0 | 0 | 0 | 0 |
| V11 on A1, A2 | L | 0 | 0 | 0 |

**Updated Risk Impact Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T4xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | L | 0 | 0 | L | L | 0 | L | L | L | 0 | L | L | 0 | 0 | 0 | 0 |
| A2 | L | 0 | 0 | L | L | L | L | L | L | L | L | L | 0 | 0 | 0 | 0 |
| A4 | L | L | 0 | 0 | M | L | L | 0 | M | L | L | L | 0 | 0 | L | 0 |
| A8 | 0 | L | 0 | 0 | 0 | M | L | 0 | 0 | L | L | 0 | 0 | 0 | L | 0 |

**Residual Asset Security Risks**

Risk of asset A1: H\*(L\*L+L\*L+L\*L+L\*L) = M

Risk of asset A2:

H \* (L\*L+ L\*L+L\*L+L\*L+L\*L) = M

Risk of asset A4: H\* (L\*L+L\*L+M\*L+L\*L+M\*L+L\*L+L\*L) = H

Risk of asset A8: H\* (L\*L+ L\*L+L\*L) = M

**Residual Vulnerability Security Risk**

Risk due to V1: H\*(L\*L+L\*L) + H\*(L\*L+L\*L) + H\*(L\*L+M\*L) = H

Risk due to V2: H\*(L\*L) + H\*(L\*L+L\*L) + H\*(L\*L+L\*L) = M

Risk due to V8: H\*(L\*L) + H\*(L\*L) + H\*(L\*L) + H\*(L\*L) = M

Risk due to V11: H\*(L\*L) + H\*(L\*L) = M

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A4 | H | 1 |
| A1 | M | 2 |
| A8 | M | 3 |
| A2 | M | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V1 Falsified Timesheets | H | 1 |
| V2 Unauthorized Access | M | 2 |
| V8 Corruption and Loss of Data | M | 3 |
| V11 Inadequate security of storage, database, and mainframe | M | 4 |

**Summary**

Heat chart of Scenario 1 showing Threat/Vulnerability likehood with Asset Risk Impact.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Asset Risk  Impact |  |
|  |  | L | M | H |
|  | H |  |  | A1,A2,A4,A8 |
| T/V likelihood | M |  |  |  |
|  | L |  |  |  |

With the reference of HGA case study, the subsets of the 4 selected assets, threat and vulnerabilities are as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Number** | **Asset** | **Description** | **Value** |
| A1 | Financial Resources | Includes paychecks, transfers, and balances | H |
| A2 | Personnel Information | Includes information about the employees like name, email addresses, paycheck details etc. | H |
| A4 | PC | Hardware entity for personnels of HGA for their duties like submitting timesheets. | H |
| A8 | LAN Server | Central network component between PCs and other hardware entities and shared programs, storage etc. | H |

|  |  |
| --- | --- |
| **Number** | **Threat** |
| T1 | Payroll Frauds |
| T3 | Interruption of Operations |
| T4 | Disclosure and Brokerage of Information |
| T9 | Natural Disaster |

|  |  |
| --- | --- |
| **Number** | **Vulnerability** |
| V1 | Falsified Timesheets |
| V2 | Unauthorized Access |
| V8 | Corruption and Loss of Data |
| V11 | Inadequate security of storage, database, and mainframe |

Using arbitrary values of asset values, TV matrix is created with the consideration of the crucialness, and significance of the assets and threat and vulnerability might affect it. Additionally, for starters Risk Impact for the applicable assets was considered 100% taking resilience as zero. Thus, initial matrix are as follows:

**Initial TV pair matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | H | H | H | 0 |
| V2 on A2, A4, A8 | H | H | H | 0 |
| V8 on A1, A2, A4, A8 | 0 | H | L | H |
| V11 on A1, A2 | M | H | H | H |

**Initial Risk Impact matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T4xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | H | 0 | 0 | H | H | 0 | H | H | H | 0 | H | H | 0 | 0 | H | H |
| A2 | H | H | 0 | H | H | H | H | H | H | H | H | H | 0 | 0 | H | H |
| A4 | H | H | 0 | 0 | H | H | H | 0 | H | H | H | H | 0 | 0 | H | 0 |
| A8 | 0 | H | 0 | 0 | 0 | H | H | 0 | 0 | H | H | 0 | 0 | 0 | H | 0 |

Applying Scenario 1, Scenario 2, Scenario 3, P1, P2, RE1, RE2 the matrixes were:

**Updated TV matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | M | M | H | 0 |
| V2 on A2, A4, A8 | L | L | L | 0 |
| V8 on A1, A2, A4, A8 | 0 | L | 0 | L |
| V11 on A1, A2 | L | M | L | M |

**Updated RI matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T4xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | H | 0 | 0 | H | H | 0 | H | H | H | 0 | H | H | 0 | 0 | H | H |
| A2 | 0 | L | 0 | L | 0 | L | L | 0 | 0 | L | L | L | 0 | 0 | L | 0 |
| A4 | H | H | 0 | 0 | H | H | H | 0 | H | H | H | H | 0 | 0 | H | 0 |
| A8 | 0 | H | 0 | 0 | 0 | H | H | 0 | 0 | H | H | 0 | 0 | 0 | H | 0 |

Here in each scenarios we used the approach of applying existing and new recommended security policies in iterative manner. After, asset and vulnerability hardening were performed where in Prevention strategy, highest vulnerability was targeted and appropriate measures were implemented and calculations were done. Later, the highest asset risk was selected and same as Prevention strategy was performed resulting in the reduction of asset and vulnerability risk both.

Thus, application of Current Security Control Policies, New Security Policies recommended by CISO team, MOT controls, 2 factor authentication, VPN, encryption, and cryptography resulted in the reduction of asset and vulnerability residual risk along with the likelihood of the exploitation.

**Do you agree with HGA new CISO’s risk management recommendations and why?**

My view weighs on both sides. The CISO’s risk management recommendations reduces the risk of threat exploiting vulnerabilities very highly. The recommendations covers broad range of assets in the HGA. However, there could be some more enhancements in the security recommendations and countermeasures. For example, physical security was an issue that was addressed. But it can be more strictly implemented and tightened. Thus, I agree with the recommendations with addition to make it more robust.

**Was the M-O-T model used effectively by HGA? Did HGA’s security policies cover the policies recommended by the M-O-T model?**

No, MOT model provided was not implemented as per required in the HGA’s security policy. There were many domains of security which could have been more effective if the MOT model had been used to cover the policies of the HGA. Taking a scenario, it lacked authentication measures, which would have reduced some of the biggest threats like failure to maintain confidentiality and integrity of the financial asset and sensitive information. For example, biometrics for extensive authentication. Therefore, MOT controls could have been implemented more precisely keeping labor and technical cost, efficiency and time in mind.

**Now compare Risk strategies. Do you recommend a Risk Prevention Strategy, a Risk Response (Resilience) Strategy, or a Mixed Strategy as combination of both? Clearly explain your analysis and recommendations.**

According to me and what I have analyzed, my recommendation would be Mix Strategy. Although, Risk Prevention and Resilience strategy reduce the risk same or maybe more than mixed strategy, time and cost are the two aspects to be considered. Mixed strategy implements both Prevention and Response strategy at the same time. This can be important at a crucial time while identifying, managing, and mitigating threats and vulnerabilities. If the cost and efficiency proves out to be the same in both strategies, it depends on the organization which type of strategy to implement it according to their needs, infrastructures and exposure.

**Self-Assessment Questionnaire**

Management Controls

**• Is risk periodically assessed?**

Yes, the risk assessment is done periodically.

**• Do program managers understand the risk to systems under their control and determine the acceptable level of risk?**

Yes, new CISO recommendations enhances the risk identification and control.

**• Have the security controls of the system and interconnected systems been reviewed?**

Yes

**• Does management ensure that corrective actions are effectively implemented?**

Yes

**• Has a system development life cycle methodology been developed?**

No

**• Has the system been certified/recertified and authorized to process (accredited)?**

No

**• Is the system operating on an interim authority to process in accordance with specified agency procedures?**

No

**• Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?**

No

**• Is the plan kept current?**

Yes

**Operational Controls**

**• Are duties separated to ensure least privilege and individual accountability?**

Yes, the duties are separated to guarantee least privilege and individual accountability.

**• Is appropriate background screening for assigned positions completed prior to granting access?**

No

**• Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?**

No

**• Is data protected from interception?**

Yes, encryption was recommended by the CISO recommendation.

**• Are mobile and portable systems protected?**

No, mobile and portable systems are not protected.

**• Is there user support?**

No

**• Are there media controls?**

No

**• Have the most critical and sensitive operations and their supporting computer resources been identified?**

Yes, they have been identified in the risk assessment.

**• Has a comprehensive contingency plan been developed and documented?**

Yes

**• Are tested contingency/disaster recovery plans in place?**

Yes, but it requires more work.

**• Is access limited to system software and hardware?**

Yes

**• Are all new and revised hardware and software authorized, tested and approved before implementation?**

No

**• Are systems managed to reduce vulnerabilities?**

Yes, incident response and IAM has been implemented.

**• Is virus detection and elimination software installed and activated?**

Yes

**• Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?**

Yes

**• Is there sufficient documentation that explains how software/hardware is to be used?**

Yes

**• Are there formal security and operational procedures documented?**

Yes

**• Have employees received adequate training to fulfill their security responsibilities?**

Yes, employees receive proper training along with fresher courses.

**• Is there a capability to provide help to users when a security incident occurs in the system?**

Yes, support measures are in place for the users.

**• Is incident related information shared with appropriate organizations?**

No, this practice is not followed

**Technical Controls**

**• Are users individually authenticated via passwords, tokens, or other devices?**

Yes, OTP using smart token are used for authentication.

**• Are access controls enforcing segregation of duties?**

Yes, the segregation of duties are enforced for restricted access and minimal exposure.

**• Do the logical access controls restrict users to authorized transactions and functions?**

Yes, only timesheets transactions and emails are being allowed.

**• Are there logical controls over network access?**

Yes, firewall, IDS and IPS is implemented.

**• If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?**

No, public access has not been considered.

**• Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?**

Yes, IDS and IPS, IAM, access controls and all ensures restricted access with continuous monitoring, identification, and mitigation.