|  |  |
| --- | --- |
|  | CIS-1290 Principles of Information Security |

Topic 4 Part 3

|  |  |
| --- | --- |
| To: | Mike MacDonald |
| From: | Christopher Sigouin |
| Date: | February 25, 2015 |
| Subject: | Risk Management Class Activity ( Part 3 ) |
|  |  |

This assignment assesses the “Risk Control” phase of the Risk Management process utilizing a pharmacy company profile. The prior stages of “Risk Identification” and “Risk Assessment” have been completed in order to produce the following data below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Safeguard Determination Table** | | | | | |
| TVA Name | Control Strategy | Recommended Safeguard Description | Residual Likelihood of Occurence | Residual Impact Severity | Residual Risk Level |
| (a) Human error or failure / Data entry errors / Pharmacist | Defend | Quarterly training sessions on usage of systems | Very Low (0.3) | Damaging (2) | Low(0.6) |
| (b) Human error or failure / Data entry errors / Pharmacist | Transfer | Increased system confirmation of data entries implemented by vendor for increased integrity | Very Low (0.3) | Damaging (2) | Low(0.6) |
| Human error or failure / Data entry errors / Student Temp Employee | Defend | Strong mentorship program | Low (0.4 ) | Significant (1.5) | Low(0.6) |
| Human error or failure / Data entry errors/ Prescription delivery personnel | Accept | Data entry errors for the nature of the asset are acceptable | High (0.8) | Minor (1) | Low(0.8) |
| Quality of Service deviations from service providers / No access to assets / Process of interaction with HIAL ( Pharmacy Network ) | Transfer | Service provider ensures reliable business class networking services and backup services in the event of an outage | Low (0.4) | Damaging(2) | Low(0.8) |
| (a) Software attacks / Malware infections / Process of interaction with HIAL ( Pharmacy Network ) | Defend | All data scanned prior to entry into the local system. | Low (0.4) | Critical (3) | Moderate(1.2) |
| (b) Software attacks / Malware infections / Process of interaction with HIAL ( Pharmacy Network ) | Mitigate | Processes implemented through IRP and DRP in the case of infection | Medium (0.6)  \*does not change occurrence | Damaging (2) | Moderate(1.2) |
| Missing, inadequate or imcomplete organizational policy or planning / Improper exchange of information / Process with PoS: Initiating client transaction and client usage | Transfer | Vendor ensures proper safeguards in place with PoS system in the event that information is provided to an unauthorized individual | Very Low (0.3) | Minor (1) | Low(0.3) |
| Human error or failure / Data handling issues / Local Database: Patient Information, prescriptions, inventory, orders, professional info bulletins | Transfer | Responsibility of IT service contractor to complete backup procedures properly and ensures their integrity | Low (0.4) | Damaging (2) | Low(0.8) |
| Missing, inadequate or incomplete organizational policy or planning / Backup procedures / Local Database: PoS ( includes inventory, accounting , sales trends, pricing ) | Transfer | Responsibility of IT service contractor to complete backup procedures properly and ensure their integrity | Low (0.4) | Damaging (2) | Low(0.8) |
| Information extortion / Configuration issues / TELUS Assyst Rx software ( local system ) | Transfer | Vendor of TELUS Assyst Rx software is responsible for the configurations of the system. SLA and insurance of confidentiality provided | Very Low ( 0.3) | Damaging (2) | Low(0.6) |
| Missing, inadequate or incomplete controls / Unsecured access / TELUS Assyst PoS system software | Transfer | Service contract with vendor TELUS Assyst PoS system ensures confidentiality | Very Low (0.3) | Damaging (2) | Low(0.6) |
| Software attacks / Email systems / Miscellaneous applications ( Office suites, email systems, etc ) | Defend | Antivirus software enabled on all email available systems. Also regular training sessions on email handling | Low (0.4) | Serious (2.5) | Moderate(1.0) |
| Technical hardware failures or errors / Firmware failures / Servers ( Both TELUS Assyst Rx software and TELUS Assyst PoS system ) | Transfer | Services provided by the vendor of the TELUS Assyst Rx software solution to restore in the event of failure | Very Low ( 0.3) | Serious (2.5) | Low(0.75) |
| Forces of Nature / Destruction of hardware / Networking Equipment / | Mitigate | Implement IR and DR plans to restore services as soon as possible | Low (0.4)  \*does not change occurrence | Significant (1.5) | Low(0.6) |
| Theft / Risk of being stolen / Removable Media ( Backups, documentation, etc ) | Terminate | Due to the nature of the asset being easily concealable, this asset will be terminated | Negligible  (0.1) | Insignificant (0.5) | Low(0.05) |

The following notes below show the change from a ”High or Moderate” to” Low” risk level.

Pharmacist – **Moderate (1.2) to Low (0.6)**

Student – **Moderate (1.2) to Low (0.6)**

Prescription Delivery Personnel – **Moderate (1.6) to Low (0.8)**

Process with PoS: Initiating client transaction and client usage – **Moderate (1.0) to Low (0.3)**

Local Database: Patient Information, prescriptions, inventory, orders, professional info bulletins

**Moderate (1.2) to Low (0.8)**

Local Database: PoS (includes inventory, accounting, sales trends, pricing) –

**Moderate (1.0) to Low (0.8)**

TELUS Assyst Rx software (local system) – **Moderate (1.5) to Low (0.6)**

TELUS Assyst PoS system software – **Moderate (1.0) to Low (0.6)**

Servers (Both TELUS Assyst Rx software and TELUS Assyst PoS system) -

**Moderate (1.0) to Low (0.75)**

Networking Equipment – **Moderate (1.0) to Low (0.6)**

Removable Media (Backups, documentation, etc.) – **Moderate (1.6) to Low (0.05)**

Main reasoning for the large amount of risk level change is due to the fact that most of the controls implemented involved “transfer”. This moved the responsibility to another provider so that it lessened the impact severity somewhat.