Class Activity: Risk Management, Part 1

## *Objective: Using the company profile provided (see SAM), and your imagination where necessary, complete tasks associated with Risk Management.*

Recall the following figure from pg. 120 in the textbook:

### **Note on Health Laws Security**

Health Acts/Laws, such as HIPAA or Canadian provincial or federal statutes, and related frameworks call for due diligence based on good business practices, for systems handling electronic protected health information (EPHI). Creating an Information Risk Assessment Report satisfies these requirements to analyze risks, formulate appropriate safeguards, and document the risk management decision-making process.

# Part 1: Risk Identification – Tasks include: Asset Identification, Asset Classification, and Vulnerability Assessment

## Identify & inventory assets

Conduct an inventory of all the information assets for use in Table 1 (or similar table).   
(Add rows if necessary).

Table 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Information Asset Valuation and Prioritization** | | | | | |
| **Asset Name** | **Data classification  (Confidential, Private, Public)** | **Confidentiality (1-3)** | **Integrity (1-3)** | **Availability (1-3)** | **Score (average)** |
| Pharmacist ( Employee ) |  |  |  |  |  |
| Pharmacy Assistant ( Employee ) |  |  |  |  |  |
| Computer Technician ( Non-Employee ) |  |  |  |  |  |
| Student ( Temp Employee / Employee ) |  |  |  |  |  |
| Sales Employee |  |  |  |  |  |
| Suppliers ( Non-Employee ) |  |  |  |  |  |
| Homecare Employees |  |  |  |  |  |
| Prescription Delivery Personnel ( Employee or Non-Employee ) |  |  |  |  |  |
| Process of interaction with HIAL ( Pharmacy Network ) | Confidential | 3 | 3 | 1 | 7 |
| Process of interaction with TELUS Assyst Rx ( Local software solution ) | Confidential | 3 | 3 | 3 | 9 |
| Process of providing information during prescription deliveries | Private | 1 | 2 | 1 | 4 |
| Process of updating information regarding deliveries completed | Private | 2 | 3 | 2 | 7 |
| Process of providing information during homecare sessions | Private | 1 | 2 | 1 | 4 |
| Process of updating homecare session completion | Private | 2 | 3 | 2 | 7 |
| Process of providing general information with customers / clients | Public | 1 | 1 | 1 | 3 |
| Process of updating shipping / receiving / pricing / inventory for diabetic supplies | Private | 2 | 3 | 2 | 7 |
| Process with PoS: Initiating client transaction and client usage | Public | 3 | 3 | 3 | 9 |
| Process with PoS: Backend configurations, updates, etc | Private | 3 | 3 | 1 | 7 |
| Process with PoS: Managing Inventory | Private | 2 | 3 | 2 | 7 |
| Process with PoS: Accounting and Reports (may include salaries?) | Confidential | 3 | 3 | 3 | 9 |
| Local Database / Electronic Documents: Patient information, prescriptions, Inventory, orders, Professional info Bulletins ( includes consultation information ) | Confidential | 3 | 3 | 3 | 9 |
| Local Database / Electronic Documents: PoS ( includes inventory, accounting, sales trends, Pricing ) | Confidential  ( because it also includes sales, accounting, etc ) | 3 | 3 | 3 | 9 |
| Local Database / Electronic Documents: Homecare and Prescription Deliveries | Private | 2 | 2 | 2 | 6 |
| Local Database / Electronic Documents: Shipping and Receiving | Private | 2 | 2 | 2 | 6 |
| TELUS Assyst Rx software ( local system ) | Confidential | 3 | 3 | 3 | 9 |
| TELUS Assyst Point of Sale system | Confidential | 3 | 3 | 3 | 9 |
| Application(s) used with Prescription Delivery service ( signature verification, delivery completion, etc ) | Private | 2 | 2 | 2 | 6 |
| Application(s) used with Homecare service ( signature verification, homecare session completion, etc ) | Private | 2 | 2 | 2 | 6 |
| Applications and/or software used for accessing & updating information regarding diabetic supplies | Private | 2 | 2 | 2 | 6 |
| Operating System software | Private | 2 | 3 | 3 | 8 |
| Miscellaneous applications  ( Office suites, etc ) | Private | 1 | 2 | 2 | 5 |
| Servers ( Both for TELUS Assyst Rx software and TELUS Assyst Point of Sale system ) | Confidential | 3 | 3 | 3 | 9 |
| Terminals ( x2, TELUS Assyst Rx software ) | Private | 2 | 3 | 2 | 7 |
| Terminals ( x2, TELUS Assyst Point of Sale system ) | Private | 2 | 3 | 2 | 7 |
| Networking Equipment | Confidential | 3 | 3 | 3 | 9 |
| Peripherals used through both Prescription Deliveries and/or Homecare Sessions | Private | 2 | 2 | 2 | 6 |

## Classify & prioritize assets

Classify the information assets in Column 2 of Table 1 (above).

Rank the inventoried and classified data assigning a number to each CIA column according to the **financial impact it would have and how much trust (integrity) you place in the data as being reliable to the business, if compromised and not being available for a period of time**. Understand that any data has a financial impact to a business if Confidentiality, Integrity or Availability is compromised and each should have a number assigned.

## Identify and Prioritize Threats

Identify threats that could exploit vulnerabilities. For convenience, use the threat categories referenced in the textbook (see pg. 44, 134, & 141). Not all threat categories may apply to all assets.

***You should end up with a separate table for EACH asset.***

Next, consider the potential vulnerabilities associated with each threat, to produce a threat-vulnerability pair (TV pair). A vulnerability can be associated with one or more threats. Collect input from previous risk assessments, audits, system deficiency reports, security advisories, scanning tools, security test results, system development testing, industry and government listings, such as sans.org, securityfocus.com, vendor advisories, and the NIST vulnerability database at <http://nvd.nist.gov/>.

Table 2 (separate table for EACH asset)

|  |  |
| --- | --- |
| **Asset Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Vulnerability Assessment** | |
| **Threat category** | **Possible Vulnerabilities** |
| Compromises to intellectual property |  |
| Espionage or trespass |  |
| Forces of Nature |  |
| Human error or failure |  |
| Information extortion |  |
| Missing, inadequate, or incomplete controls |  |
| Missing, inadequate, or incomplete organizational policy or planning |  |
| Quality of Service deviations from service providers |  |
| Sabotage or vandalism |  |
| Software attacks |  |
| Technical hardware failures or errors |  |
| Technical software failures or errors |  |
| Technological obsolescence |  |
| Theft |  |

|  |  |
| --- | --- |
| **Asset Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Vulnerability Assessment** | |
| **Threat category** | **Possible Vulnerabilities** |
| Compromises to intellectual property |  |
| Espionage or trespass |  |
| Forces of Nature |  |
| Human error or failure |  |
| Information extortion |  |
| Missing, inadequate, or incomplete controls |  |
| Missing, inadequate, or incomplete organizational policy or planning |  |
| Quality of Service deviations from service providers |  |
| Sabotage or vandalism |  |
| Software attacks |  |
| Technical hardware failures or errors |  |
| Technical software failures or errors |  |
| Technological obsolescence |  |
| Theft |  |

# Part 2: Risk Assessment – Tasks to be determined (see separate document)

# Part 3: Risk Control – Tasks to be determined (see separate document)

#### Sources:

A Risk Assessment Checklist For Small Business (<http://www.comptia.org/Libraries/ME-Misc/The_Purpose_of_Developing_Security_Checklists.sflb.ashx>)

Information **Security Risk** Assessment Project (<http://www.mass.gov/anf/docs/itd/policies-standards/it-security-risk-assessment-guidelines.rtf>)

Principles of Information Security, 4th Edition textbook

NIST SP800-60\_Vol1-Rev1 (<http://csrc.nist.gov/publications/PubsSPs.html>)