**IT2522 Risk and Incident Management**

**2013/2014 Semester 1**

**Tutorial 2 – Qualitative Risk Assessment**

**Learning Objective**

Able to perform the following tasks

* Assets, threats and vulnerabilities identification
* Qualitative risk assessment

# Instructions

1. Form groups with 2 persons in each group.
2. Google and state the **mission** of the company [www.amazon.com](http://www.amazon.com) (5 mins)
3. List **TEN information assets** that support the business objectives of amazon.com in the page 3 of this tutorial (5 mins).

|  |  |
| --- | --- |
| **Asset ID** | **Asset** |
| 1 | Customers’ information |
| 2 | Suppliers’ information |

1. Go to blackboard and download a copy of “CSI Computer Crime and Security Survey 2010”.
2. Refer to the page 17 of the survey and other Internet resources, fill in the **TEN threats** that may affect the business objectives of amazon.com in the Risk Assessment Table in the page X of this tutorial. (5 mins)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat ID** | **Threat** | **Threat Impact** | **Threat Likelihood** | **Risk Level** |
| 1 | Denial of service attack |  |  |  |
| 2 |  |  |  |  |

1. Download a copy of “NIST SP800-30 Risk Management Guide for Information Technology Systems” from <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Refer to the “Table 3-5. Magnitude of Impact Definitions” in page 23. Discuss and define a magnitude of impact definitions for amazon.com with the consideration of their business objectives and identified threats in (5) above. Fill in the Threat Impact Definition in page Y of this tutorial. (5 mins)

|  |  |
| --- | --- |
| **Magnitude of Impact** | **Threat Impact Definition** |
| High | e.g. Interruption of all online business transactions for more than a day |
| Medium |  |
| Low |  |

1. Assess the impact of each threat and fill in the respective threat impact level in the risk assessment table.

For an example

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat ID** | **Threat** | **Threat Impact** | **Threat Likelihood** | **Risk Level** |
| 1 | Denial of service attack | High |  |  |
| 2 |  |  |  |  |

1. Search Internet for key words like “Amazon Security Issue” and read up the vulnerabilities that could be exploited by attackers (threat-source). Study the effectiveness of the current security controls that reduce the vulnerabilities. (5 mins)
2. Assess the vulnerabilities of the ten assets, the effectiveness of the current security controls and consider the type of attacks experience by percentage of respondents in the page 8 of the CSI survey, fill in the threat likelihood of each of the threats in the Risk Assessment Table. (5 mins)

For an example

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat ID** | **Threat** | **Threat Impact** | **Threat Likelihood** | **Risk Level** |
| 1 | Denial of service attack | High | Medium | Medium |
| 2 |  |  |  |  |

1. Base on the following risk level matrix table and determine the risk level of each of the threats. Fill in the Risk Level of each of the threats in the Risk Assessment Table.

Risk Level Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Threat Impact** | | |
| **Threat Likelihood** | Low | Medium | High |
| Low | ***Low*** | ***Low*** | ***Low*** |
| Medium | ***Low*** | ***Medium*** | ***Medium*** |
| High | ***Low*** | ***Medium*** | ***High*** |

For an example

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat ID** | **Threat** | **Threat Impact** | **Threat Likelihood** | **Risk Level** |
| 1 | Denial of service attack | Low | Medium | Low |
| 2 |  |  |  |  |

1. Submit your answer sheet to your tutor at the end of this tutorial.

**Answer Sheet**

**Group Member Names :**  Hung Dejian, Daryl

See yat cheung peter

**The business objectives of amazon.com:**

Our vision is to be earth's most customer centric company; to build a place where people can come to find and discover anything they might want to buy online.

**Ten information assets:**

|  |  |
| --- | --- |
| **Asset ID** | **Asset** |
| 1 | Customer information |
| 2 | Supplier information |
| 3 | Staff information |
| 4 | Product information |
| 5 | Website |
| 6 | Server |
| 7 | Customer credit card information |
| 8 | Shareholders information |
| 9 | Customer Feedback information |
| 10 | Internet connection |

**Threat Impact Definition:**

|  |  |
| --- | --- |
| **Magnitude of Impact** | **Threat Impact Definition** |
| High | Interruption of all online business transactions for more than a day or total destruction of business transaction records |
| Medium | Interruption of all online business transaction for more than an hour or partial destruction of business transaction records |
| Low | Interruption of all online business transaction for less than an hour or destruction of less than 100 business transaction records |

**Risk Assessment Table:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat ID** | **Threat** | **Threat Impact** | **Threat Likelihood** | **Risk Level** |
| 1 | Malware infections | Medium | High | High |
| 2 | Password sniffing | High | Medium | High |
| 3 | Financial fraud | High | Low | Low |
| 4 | Denial of Service | High | Medium | Medium |
| 5 | Exploit of wireless network | High | Medium | Medium |
| 6 | Bots | Low | Low | Low |
| 7 | Exploit of DNS | High | Low | Medium |
| 8 | Instant messaging abuse | Low | Medium | Low |
| 9 | System penetration by outsider | High | Low | Low |
| 10 | Laptop or mobile hardware theft | Low | Low | Low |