# *IT Security (420-F30-HR)*

# *Lab 02b –* *Threat, Vulnerabilities, Risk, Cost*

Date assigned: Friday, January 31

Date Due: Friday, January 31 (end of lab)

**Objectives:**

Learn:

1. Understand Threat, Vulnerability, Risk and Cost consideration
2. Understand Threat Actors

**References:** S0101-Foundations\_CIA, S0201\_Threat

# Theory – (Individual Lab)

## Threat Analysis – non-cybersecurity

**Objectives:** Understand the definitions of the terms (threat, vulnerability, risk and cost) via non-cybersecurity use case

**To Do:**

## Threat Analysis – CIA Scenarios

For each of the cases below indicate whether Confidentiality, Integrity or Availability is violated. Discuss and agree as a group:

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Confidentiality | Integrity | Availability |
| Ellen is buying a laptop from an online site and finds a way to change the price from $800 to $80. |  |  |  |
| Steve is on an online auction site trying to bid for a new mountain bike. As he makes his bid, the website crashes. |  |  |  |
| Alice is checking her grades and forgets to logout before she leaves. Bob gets on the computer and sees her grades. |  |  |  |
| Jane discovers she can change the website of the college news. She edits the website. |  |  |  |

# Case Study – (Group Lab)

Groups of 4 students. That’s 3 cases for part B, 1 case for Part C. Everybody gets a case to present.

Each group must find a case study for the 3 kinds of threats. (Use whiteboard to avoid conflicts/duplicates).

|  |  |  |  |
| --- | --- | --- | --- |
|  | Natural Event | Human error/accident | Attack (Malicious intent) |
| Group 1 |  |  |  |
| Group 2 |  |  |  |
| Group 3 |  |  |  |
| Group 4 |  |  |  |

## Find a real-world case for each type.

1. Fill in the Case Study Template. In the Attack section, define the definition of your threat actor type (i.e. “Nation state, Acts of God”, etc.).
2. Be prepared to present your case study later.
   1. Every group member should have a portion to present. 4-6 minutes per case
   2. Clearly define each of your **threat actor types** and **motivations** and explain which one your case study covers.

# Case Study – (Group Lab)

Using a highly advanced matching algorithm, the following groups are assigned

|  |  |
| --- | --- |
|  | Threat Actors (pick one) |
| Group 1 | Acts of God, hacktivists |
| Group 2 | Accidental/human error |
| Group 3 | Nation States, terrorist group |
| Group 4 | Cybercriminals, thrill-seekers |
| Group 5 | Insider threat |

## Find a real-world case for one of your threat actors.

1. Fill in the Case Study Template. In the Attack section, define the definition of your threat actor type (i.e. “Nation state, Acts of God”, etc.).
2. Be prepared to present your case study later.
   1. Clearly define each of your **threat actor types** and **motivations** and explain which one your case study covers.

# Impact, Likelihood & Risk (Individual lab)

## Risk Rating

Study the OWASP Risk Rating Methodology:

<https://owasp.org/www-community/OWASP_Risk_Rating_Methodology>

## Research the Ashley Madison use case. Start [here](https://www.pandasecurity.com/en/mediacenter/security/lessons-ashley-madison-data-breach/) and [here](https://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/?sh=284afb404c82). There are lots of others to find.

Perform the OWASP Risk Rating. Show me your rating for all the component elements. Use <https://www.owasp-risk-rating.com/> and provide screen shot below:

<screen shot>

What are the two key factors for determining risk in the OWASP model:

<answer here>

Explain your reasoning for each of the factors:

**Likelihood factors**

Threat Agent Factors

|  |  |  |
| --- | --- | --- |
|  | Rating | Reasoning |
| Skill Level |  |  |
| Motive |  |  |
| Opportunity |  |  |
| Size |  |  |

Vulnerability Factors

|  |  |  |
| --- | --- | --- |
|  | Rating | Reasoning |
| Ease of Discovery |  |  |
| Ease of Exploit |  |  |
| Awareness |  |  |
| Intrusion Detection |  |  |

**Impact factors**

Technical Impact Factors

|  |  |  |
| --- | --- | --- |
|  | Rating | Reasoning |
| Loss of Confidentiality |  |  |
| Loss of Integrity |  |  |
| Loss of Availability |  |  |
| Loss of Accountability |  |  |

Business Impact Factors

|  |  |  |
| --- | --- | --- |
|  | Rating | Reasoning |
| Financial Damage |  |  |
| Reputation Damage |  |  |
| Non-compliance |  |  |
| Privacy Violation |  |  |

What are the two key factors for determining risk in the OWASP model:

<answer here>

## Risk vs Cost/Counter-measures

***Purpose:*** Gauge Risk and consider counter-measures if necessary

***To Do: Given Risk vs Cost grid***

Identify examples (either in your personal life or in general) for each quadrant of the grid below.

For each example, specify:

* Scenario
* Risk (high/med/low)
* Suggested Mitigation/Counter-measures

|  |  |  |
| --- | --- | --- |
|  | Low Likelyhood | High Likelyhood |
| High Impact |  |  |
| Low Impact |  |  |

**Marking Scheme**

|  |  |  |
| --- | --- | --- |
|  | **Mark** | **Out of** |
|  |  |  |
| **Part A: Theory - Individual** |  |  |
| CIA Scenarios |  | 4 |
|  |  |  |
|  |  |  |
| **Part B,C: Case Study -Group** |  |  |
| Case (x 4) |  |  |
| Scenario (clearly described) |  | 2 |
| Attack (threat, threat actor, vulnerability) |  | 8 |
| Impact |  | 2 |
| Response |  | 2 |
| Lessons Learned |  | 2 |
| Counter Measures |  | 2 |
|  |  |  |
| Individual – presentation & contribution |  | 8 |
|  |  |  |
| **Part D: Risk vs Cost** |  |  |
| Risk vs Cost grid |  | 8 |
| Risk metrics (0.5 each) |  | 8 |
|  |  |  |
| Handed in properly |  | 4 |
| **Total** |  | **46** |