Module 6: Cyber-Physical Risk Assessment in Maritime Systems
The purpose of this module is

• To introduce the concepts of Risk and Risk Management

• To provide the basis for Risk-Based Decision Making and prioritization of risk mitigation projects
What is Risk?
The Concepts of Risk, Consequences, Vulnerability, Prioritization, and Mitigation

• Suppose a large insurance company is insuring thousands of ship voyages a year.
• Assume further that on the average, each ship and its cargo is worth $150M + $50M = $200M. Also assume that the probability of a ship being lost at sea is 1%.
• Assuming no loss of life nor environmental damage, the Consequences (C) of a loss of a ship is $200M. The probability (or Vulnerability, V) of the loss is 1%, or one in a hundred ship voyages
• So, if there are 100 voyages, and one ship is lost, the loss is $200M. Spreading this over the 100 voyages, each voyage must be covered for $200M/100 or $2M per ship voyage.
What is Risk?

The **quantitative** definition of Risk

- From the previous example, Risk may be defined mathematically (or **quantitatively**) as:
  - Risk = (Consequences of an Event) times (Probability of its Occurrence)
  
  This is a mathematical definition, and requires a lot of data to get meaningful values of Consequences, Probability, and Risk

- In insurance, financial, and other actuarial studies where there are large quantities of data, Risk can be calculated quantitatively with precision

- However, there have been relatively few maritime security incidents. Hence there is a relatively small amount of data on Consequences and Vulnerability due to security losses
What is Risk? (cont.)
The **qualitative** definition of Risk

- Due to the lack of data it’s difficult to make quantitative calculations of security Risk in maritime systems. Fortunately, we do not need precise numbers for decision making and prioritization of risk mitigation projects.

- For the purposes of understanding Risk and Mitigation, qualitative approaches will work.

- More generally, we may define Risk **qualitatively**, by using a qualitative scale like 1 to 10, for low to high values of Consequences and Vulnerability. We can then combine these values to get a quantitative value of Risk:

  - Risk = (Consequences) **combined with** (Vulnerability)

- We combine C and V in some way that makes sense for application.
Qualitative Risk-Based Decision Making

To Begin:

- Create an inventory of all systems including: Hardware (HW), Software (SW) (Versions and Patches), Malware Protection and Network Diagrams.
- Companies tend not to know these things. In the SolarWinds and Log4j exploits, entities did not know whether CISA-published patches applied to them or not.
- The documentation of which systems require risk improvement is the basis of a Facility Security Assessment.
Getting to the Facility Security Assessment and the Facility Security Plan

- **Consequence Score**
  - Determine the Consequences of the loss of all systems, and assign an importance to them in terms of a qualitative scale score, e.g., 3,2,1 or 5,4,3,2,1 from High to Low, and call this the Consequence Score for each system.

- **Vulnerability Score**
  - Determine the Vulnerability of these systems to successful attacks by setting a set of criteria and judging how well they are being met. Again, define a qualitative scale and determine a Vulnerability score.

- **Combine Consequence and Vulnerability**
  - Define a method to combine Consequence and Vulnerability scores and call that Risk. 
    - **Prioritize** relevant scenarios according to Risk. (This is the basis of a **Facility Security Assessment (FSA)**).

- **Mitigate**
  - Determine which systems in the prioritized list to **Mitigate** the Vulnerability (consistent with budget and executive experience).
  - This is the basis of a **Facility Security Plan (FSP)**. Requires organizational, educational, and technological initiatives to accomplish, since there is never enough resources to do everything.
Determining the Consequences

Identify All Systems of Concern, and All Attack Scenarios

Select an Attack Scenario

Determine Consequence, C Score

Determine Vulnerability, V Score

Determine Risk for Every Scenario

Create a Risk-Based Priority List

Qualitative Assessment of Consequences

• Determine the consequences of a successful attack
• Work with qualitative assessment levels, say a scale from 5 to 1, (where 5 is the highest consequence) depending...
• Define what we mean by the levels
• Consider the following charts:
## Determination of a Qualitative Consequence Score – An Example

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Effect on MTS</th>
<th>Effect on Personnel and Business Operations</th>
<th>Effect on Economy or Security</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Long Term Significant Effect</td>
<td>Multiple Permanent Injuries/Death</td>
<td>Major Economic or Nat’l Security Impact</td>
<td>5</td>
</tr>
<tr>
<td>Major</td>
<td>Long Term Significant Effect</td>
<td>Few Permanent Injuries/Deaths</td>
<td>Major Local Disruption; Significant Damage to Critical Infrastruct.</td>
<td>4</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate Term Effect</td>
<td>Some Serious Injuries</td>
<td>Short Term Economic Disruption</td>
<td>3</td>
</tr>
<tr>
<td>Minor</td>
<td>Minor Disruptions</td>
<td>Business Disruptions Affecting Outside</td>
<td>Low Impact</td>
<td>2</td>
</tr>
<tr>
<td>Insignificant</td>
<td>No MTS Disruptions</td>
<td>Business Disruptions Within</td>
<td>None</td>
<td>1</td>
</tr>
</tbody>
</table>
A Way of Determining a Vulnerability Score

• Create a Consequence priority list of systems in decreasing order of Consequences

• Develop checklist of cyber vulnerability areas for each system

• Assign Vulnerability Score by virtue of compliance with checklist, or lack thereof, working down the Consequence priority list

• Determine required Mitigations

• Assess Mitigation effectiveness and cost, as far down the list as possible

• See also: NIST SP 800-82 Version 2
Vulnerability Assessment

Some things to consider:

1. Is the system exposed to an external threat, an internal threat?
2. Is the system vulnerable to a “lateral” attack, i.e., can an intrusion into one system lead to an intrusion into another?
3. Is there adequate segmentation and segregation?
4. Are there strong authentication, access control, least privilege, encryption capabilities?
5. Is SW (software) up to date, is there a patch management policy?* (*see next slide for discussion of patch management)
6. Are there adequate backups for each system (e.g., resilience to a ransomware attack)?
7. Is staff adequately trained in cybersecurity hygiene, i.e., portable media, strong password, Multi-factor Authentication, social engineering...

Plus many more. See, for example:

- CISA Alert (AA20-049A), Ransomware Impacting Pipeline Operations
- NIST Special Publication 800-82 Rev 2
Patch Management Policy

- Patch management is a method of repairing vulnerabilities to attack in software operating systems and applications.

- In modern operating systems, patches are regularly downloaded and installed, especially in IT systems.

- OT systems may, however, be decades old with many vintages, legacy systems, proprietary protocols, with out-of-date SW and patches. Hard to patch on-the-fly.

- Systems may not have been designed with Cybersecurity in mind.

- OT patches might not be administrable while a ship is underway.

- So, patch management plans may be case-by-case, and scheduled outages may be necessary.

Discussion: What’s the debate about planned outages and patch deployment?
Create a Vulnerability Score for System X

For every system of interest, assess a Vulnerability Score. Here’s an example of a qualitative Vulnerability computation:

<table>
<thead>
<tr>
<th>Vulnerability of System X</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Strength/Mitigation</strong></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
</tr>
<tr>
<td><strong>Segregation</strong></td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
</tr>
<tr>
<td><strong>Hygiene/Training</strong></td>
</tr>
<tr>
<td><strong>VULNERABILITY SCORE:</strong></td>
</tr>
</tbody>
</table>
Create a Risk-Based Mitigation Priority List to Reduce Cyber Risk

• For each system, combine Consequence Score with Vulnerability Score as is best for the application. Call that Risk.
• Create ordered priority list for all systems according to Risk, highest first.
• Determine appropriate mitigations to improve system risk to acceptable levels
• Continue until agreed threshold is reached, or until the money runs out.
Risk-Based Priority List

Shown is an example priority list for four systems. The budget is exhausted after System Z is mitigated. *How is the tie with System Q broken?*

<table>
<thead>
<tr>
<th></th>
<th>C-Score</th>
<th>V-Score</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>System X</td>
<td>5</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>System Y</td>
<td>4</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>System Z</td>
<td>4</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>System Q</td>
<td>3</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>

Budget
Module 6 Summary

• In this module, we introduced the key building blocks and concepts of Risk and Risk Management

• This included the concepts of Risk, Consequences, Vulnerability, Prioritization, and Mitigation.

• An example was given as to how the concepts could be applied to the creation of a cybersecurity FSA and FSP

• However, a specific plan was not prescribed, as different facilities, different industries, and different vessels have different circumstances to manage.
This material is based upon work supported by the U.S. Department of Homeland Security under Cooperative Agreement No. 2014-ST-061-ML0001.

MSC@stevens.edu
www.stevens.edu/MSC