Lecture 7:
Part 1:

Security Risk Measurement

Security Risk Management
Domain Model
Asset-related Concepts

- **Business asset**
  - Caveman’s ability to observe the surrounding world (to search for food)
- **IS asset**
  - Caveman
  - A cave (from which the caveman monitors the world)
- **Security criterion**
  - Availability of the caveman’s ability to observe the surrounding world
  - *Integrity of the* caveman’s ability to observe the surrounding world

Security Risk Management Domain Model

- **Security needs**
  - Security objective that characterizes the application of a *security criterion* on a *business asset*
- **Business asset Value**
  - Only business assets are estimated in terms of value
  - Business assets are involved to define and estimate security objectives and to assess the significance of risk
Measuring Assets

<table>
<thead>
<tr>
<th>Caveman’s ability to observe the surrounding world (to search for food)</th>
<th>Value</th>
<th>= 30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security need for availability</td>
<td>= 3</td>
<td></td>
</tr>
<tr>
<td>Security need for integrity</td>
<td>= 1</td>
<td></td>
</tr>
<tr>
<td>Security need for confidentiality</td>
<td>= 0</td>
<td></td>
</tr>
</tbody>
</table>

Risk-related Concepts

- **Risk**
  - Dino assaults through the cave hole because he is able to get through it, and eats the caveman thus leading to the extinct of cavemen

- **Impact**
  - Harms caveman;
  - The cave is not reliable;
  - Negates availability of the caveman
  - Leads to the extinct of cavemen (because nobody would feed the rest of the family)

- **Event**
  - Dino assaults through the cave hole because he is able to get through it, and eats the caveman

- **Vulnerability**
  - The cave hole is large enough for the Dino to get in

- **Threat**
  - Dino assaults through the cave hole and eats the caveman

- **Threat agent**
  - Dino, who has teeth, and is hungry

- **Attack method**
  - Assault through the cave hole;
  - Eat the caveman
Security Risk Management
Domain Model

**Risk level**
- Depends on event *potentiality* and *impact level*

**Potentiality**
- Is estimated through threat *likelihood* and *vulnerability level*

---

**Measuring Risk**

<table>
<thead>
<tr>
<th>Threat likelihood that Dino assaults through the cave hole and eats the caveman</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level of vulnerability: The cave hole is large enough for the Dino to get in</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>
Measuring Risk

- Potentiality of Event = likelihood + vulnerability level – 1
  - 3+2-1 = 4

- Maximum impact level of concerned impacts for the studied business assets; estimated from the security needs

<table>
<thead>
<tr>
<th>Impact level</th>
<th>Potentiality</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td></td>
</tr>
</tbody>
</table>

Risk Treatment-related Concepts

- Risk treatment decision
  - Risk reduction (reduce number of Dinos)
  - Security requirement
    - Smash Dino hard – bone-teeth
  - Control
    - A bludgeon with bone-teeth

- Risk treatment decision
  - Risk avoidance
  - Security requirement
    - Prevent access to caveman
  - Control
    - Metal bars on the cave hole
Security Risk Management
Domain Model

- **Cost**
  - Cost of buying a firewall
  - Cost of maintaining it by a security officer

- **Risk reduction**
  - Risk reduction, avoidance, and transfer treatment
  - For risk retention, risk reduction equals 0

Measuring Risk Treatment

<table>
<thead>
<tr>
<th>Risk treatment</th>
<th>Risk reduction</th>
<th>Risk avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security requirement</td>
<td>New vulnerability level</td>
<td>Smash Dino hard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prevent access to caveman</td>
</tr>
<tr>
<td>New Risk level</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Risk reduction</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>
# Measuring Risk Treatment

<table>
<thead>
<tr>
<th>Security requirement</th>
<th>New vulnerability level</th>
<th>Risk reduction</th>
<th>Risk avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smash Dino hard</td>
<td>1</td>
<td>Prevent access to caveman</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New Risk level</th>
<th>9</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk reduction</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

### Cost of
- A bludgeon with bone-teeth = 5 🍎
- Metal bars on the cave hole = 15 🍎

---

# Measuring Risk Treatment

<table>
<thead>
<tr>
<th>Security requirement</th>
<th>New vulnerability level</th>
<th>Risk reduction</th>
<th>Risk avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smash Dino hard</td>
<td>1</td>
<td>Prevent access to caveman</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New Risk level</th>
<th>9</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk reduction</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

### Cost of
- A bludgeon with bone-teeth = 5 🍎
- Metal bars on the cave hole = 15 🍎
Return on Security Investment

\[
ROSI = \frac{(RiskExposure \times RiskMitigated) - SolutionCost}{SolutionCost} \times 100\%
\]

- A bludgeon with bone-teeth
  - Risk exposure = 30
  - Risk mitigated = Risk reduction / Risk level = 3/12
  - Solution cost = 5
    \[\text{ROSI (A bludgeon with bone-teeth)} = 50\%\]

- Metal bars on the cave hole
  - Risk exposure = 30
  - Risk mitigated = Risk reduction / Risk level = 6/12
  - Solution cost = 15
    \[\text{ROSI (Metal bars on the cave hole)} = 0\%\]

A case of
Airline Turnaround
(Matulevičius, Norta et al, 2016)

- Catering
- Ramp service
  - Luggage handling
  - Refueling
  - Air cargo handling
- Passenger service
  - Check-in
  - Gate arrival
- Field operation service
... lead to severe results ...
US Airways Express Flight 5481 stalled after take-off (January 8, 2003), crashed into a US Airways hangar and burst into flames 37 seconds after leaving Charlotte/Douglas International Airport. Although the pilots had totaled up the take-off weight of the aircraft before the flight and determined it to be within limits, the plane was actually overloaded and out of balance ...

Security Risk Management in Airline Turnaround Sector

- **Check-in passenger information**
  - **Risk1**: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed
  - **Risk2**: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight

- **Luggage information**
  - **Risk3**: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft
  - **Risk4**: The personnel accepts luggage and adds contraband items to a passenger’s luggage

- **Fuel slip**
  - **Risk5**: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip
  - **Risk6**: The attacker intercepts the fuel slip, changes the data contained and sends it to the supplier

- **Cargo assignment**
  - **Risk7**: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider
  - **Risk8**: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider
Security Risk Management in Airline Turnaround Sector

- **Check-in passenger information**
  - **Risk1**: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed
  - **Risk2**: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight

- **Luggage information**
  - **Risk3**: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft
  - **Risk4**: The personnel accepts luggage and adds contraband items to a passenger's luggage

- **Fuel slip**
  - **Risk5**: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip
  - **Risk6**: The attacker intercepts the fuel slip, changes the data contained and sends it to the supplier

- **Cargo assignment**
  - **Risk7**: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider
  - **Risk8**: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider

<table>
<thead>
<tr>
<th>Risk</th>
<th>Vulnerability level</th>
<th>Threat likelihood</th>
<th>Event potentiality</th>
<th>Impact level</th>
<th>Risk level</th>
<th>Vulnerability level</th>
<th>Threat likelihood</th>
<th>Event potentiality</th>
<th>Risk level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk1</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Risk2</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Risk3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Risk4</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>3</td>
<td>15</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Risk5</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>20</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Risk6</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>16</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Risk7</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Risk8</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>

Priority = A* Risk reduction level + B* 1/Cost of countermeasure + C* Business asset value
Security Risk Management in Airline Turnaround Sector

- **Check-in passenger information**
  - **Risk1**: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed.
  - **Risk2**: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight.

- **Luggage information**
  - **Risk3**: Personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft.
  - **Risk4**: Personnel accepts luggage and adds contraband items to a passenger’s luggage.

- **Fuel slip**
  - **Risk5**: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip.
  - **Risk6**: Attacker intercepts the fuel slip, changes the data contained and sends it to the supplier.

- **Cargo assignment**
  - **Risk7**: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider.
  - **Risk8**: Attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider.

Security Risk Management in Airline Turnaround Sector

- **Fuel slip**
  - **Risk5**: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip.
  - **Risk6**: Attacker intercepts the fuel slip, changes the data contained and sends it to the supplier.

- **Cargo assignment**
  - **Risk7**: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider.
  - **Risk8**: Attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider.
Security Risk Management in Airline Turnaround Sector

- Check-in passenger information
  - Risk1: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed
  - Risk2: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight

- Luggage information
  - Risk3: Personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft
  - Risk4: Personnel accepts luggage and adds contraband items to a passenger’s luggage

- Fuel slip
  - Risk5: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip
  - Risk6: The attacker intercepts the fuel slip, changes the data contained and sends it to the supplier

- Cargo assignment
  - Risk7: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider
  - Risk8: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider

Message to Take Home

If you do not measure – you do not control