Human Behavior and the Organizational Context of Information Security

Robert E. Crossler
Department Chair — Management, Information Systems, and Entrepreneurship
Associate Professor — Information Systems

Workshop Date: May 23, 2023
Block 1

Understanding the Human and Organizational Security Context
Risks, Threats, and Vulnerabilities

- **Risk**: Likelihood that something bad will happen to an asset
- **Threat**: Any action that could damage an asset
- **Vulnerability**: A weakness that allows a threat to be realized or to have an effect on an asset

Adapted from Kim and Solomon (2018)
Internet of Things (IoT)

• What is it?

Group Activity 1

• In groups of 2 or 3 answer the following questions. Be prepared to share your answers.
  • Identify one or two IoT technologies and discuss the benefits and risks associated with each.
  • Who receives the benefit and who is threatened by the risk?
User is weakest link in security

Group Activity 2

- In groups of 2 or 3 answer the following questions. Be prepared to share your answers.
  - Identify possible threats caused by individuals.
  - For each threat, indicate what could be done to mitigate that threat.
Tenets of Information Systems Security

Adapted from Kim and Solomon (2018)
New Challenges Created by the IoT

- Security
- Privacy
- Interoperability
- Legal and regulatory compliance
- E-commerce and economic dev issues

Adapted from Kim and Solomon (2018)
Personnel Security Principles

- Limiting Access
- Separation of duties
- Job rotation
- Mandatory vacations
- Security training
- Security awareness
- Social engineering

Adapted from Kim and Solomon (2018)
Block 2

Risk Management and Business Continuity
Risks, Threats, and Vulnerabilities

Seek a balance between the utility and cost of various risk management options

Adapted from Kim and Solomon (2018)
Quantitative Risk Assessment

Individual Activity 1

• Complete the quantitative risk worksheet.
The Risk Management Process

Adapted from Kim and Solomon (2018)
Implementing a BIA, a BCP, and a DRP

Protecting an organization’s IT resources and ensuring that events do not interrupt normal business functions

<table>
<thead>
<tr>
<th>Business impact analysis (BIA)</th>
<th>Business continuity plan (BCP)</th>
<th>Disaster recovery plan (DRP)</th>
</tr>
</thead>
</table>

Adapted from Kim and Solomon (2018)
BIA Recovery Goals and Requirements

- Recovery point objective (RPO)
- Recovery time objective (RTO)
- Business recovery requirements
- Technical recovery requirements

Adapted from Kim and Solomon (2018)
Disaster Recovery Plan (DRP)

- **Threat analysis**
- **Impact scenarios**
- **Recovery requirement documentation**
- **Disaster recovery**

<table>
<thead>
<tr>
<th>Site Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hot site</strong></td>
<td>Has environmental utilities, hardware, software, and data like original data center</td>
</tr>
<tr>
<td><strong>Warm site</strong></td>
<td>Has environmental utilities and basic computer hardware</td>
</tr>
<tr>
<td><strong>Cold site</strong></td>
<td>Has basic environmental utilities but no infrastructure components</td>
</tr>
<tr>
<td><strong>Mobile site</strong></td>
<td>Trailer with necessary environmental utilities, can operate as warm or cold site</td>
</tr>
</tbody>
</table>

Adapted from Kim and Solomon (2018)
Questions/Comments?