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 20, 2024
Block 1

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

Risks, Threats, and Vulnerabilities

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood that something bad will happen to an asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Any action that could damage an asset</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>A weakness that allows a threat to be realized or to have an effect on an asset</td>
</tr>
</tbody>
</table>

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 generative AI 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.
  • Regarding generative AI technologies, 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)
Risks, Threats, and Vulnerabilities

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

Adapted from Kim and Solomon (2018)
The Risk Management Process

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