Human Behavior and the Organizational Context of Information Security

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

Julia Stachofsky
PhD Student — Information Systems

Workshop Date: May 24, 2022
Block 1

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk</strong></td>
<td>Likelihood that something bad will happen to an asset</td>
</tr>
<tr>
<td><strong>Threat</strong></td>
<td>Any action that could damage an asset</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td>A weakness that allows a threat to be realized or to have an effect on an asset</td>
</tr>
</tbody>
</table>
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?
Weakest Link in the Security of an IT Infrastructure

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)
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

| Business impact analysis (BIA) | Business continuity plan (BCP) | Disaster recovery plan (DRP) |

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**

**Hot site**
- Has environmental utilities, hardware, software, and data like original data center

**Warm site**
- Has environmental utilities and basic computer hardware

**Cold site**
- Has basic environmental utilities but no infrastructure components

**Mobile site**
- Trailer with necessary environmental utilities, can operate as warm or cold site

Adapted from Kim and Solomon (2018)
Block 3

Beyond Organizational Borders: Cyberwarfare
Cyberwarfare is happening now

Destructive malware circulating in Ukraine has hit hundreds of computers - ESET researchers

Russian Cyberattacks Increase on Ukraine’s Critical Infrastructure: Report

Hacked News Channel and Deepfake of Zelenskyy Surrendering Is Causing Chaos Online
Internet of Things

Group Activity 3

• In groups of 2 or 3 answer the following questions from a national security perspective. Be prepared to share your answers.
  • What risks are introduced at the individual level? (IoT Devices in Home)
  • What risks are introduced at the organizational level? (IoT Devices in Business)
  • What risks are introduced at the government level? (IoT Devices in Government Infrastructure)
  • What can be done to mitigate these risks?
Group Activity 4

• In groups of 2 or 3 answer the following questions. Be prepared to share your answers.
  • Should we be using cyberwarfare attacks?
  • When is it acceptable?
  • Are cyberwarfare attacks preferable to conventional warfare?
What can we do?

- A lot of the same security principles apply even if your adversary is a nation state
- Public awareness reduces support for cyber warfare escalation (Shandler et al., 2021)
- Educating key military and political personnel on cybersecurity (Hare, 2019, Shandler et al., 2021)
  - Through programs like CySER!
- Cultivating cyber resilience (Clarke and Knake, 2019)
  - Not one nationalized solution to the problem
Questions/Comments?