STSD-CSTE

A Socio-Technical Framework to Improve cyber security training: A Work in Progress

Grethe Østby  
*PhD researcher*  
*NTNU*

Lars Berg  
*Lawyer*  
*Telenor*

Mazaher Kianpour  
*PhD researcher*  
*NTNU*

Basel Katt  
*Associate professor*  
*NTNU*

Stewart James Kowalski  
*Professor*  
*NTNU*
Problem: Lack of trained personnel

• According to the Cisco 2018 annual Cyber Security report, the lack of trained cyber security personnel is one of the key issue challenging security management (Cisco, 2018).
“The focus is no longer prevention: you can’t stop attacks. It’s now about better detection and readiness for the inevitable in order to survive in today’s complex world.”

www.ey.com
Naive inductivist Approach
“A characteristic of inductive arguments that distinguishes them from deductive ones is that, by proceeding as they do from statements about some to statements about all events of a particular kind, they go beyond what is contained in the premises.”

Alan Chalmers
Table 2. Three Kinds of Inference

<table>
<thead>
<tr>
<th></th>
<th>Abduction</th>
<th>Deduction</th>
<th>Induction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premiss</td>
<td>Fact</td>
<td>Rule</td>
<td>Case</td>
</tr>
<tr>
<td>Premiss</td>
<td>Rule</td>
<td>Case</td>
<td>Fact</td>
</tr>
<tr>
<td>Outcome</td>
<td>Case</td>
<td>Fact</td>
<td>Rule</td>
</tr>
</tbody>
</table>

Design Science Research

“Design science research in information systems (DSRIS) uses artifact design and construction (learning through building) to generate new knowledge and insights into a class of problems.”

Kuechler & Vaishnavi, 2012
Design Science Research – practical approach

Karokola 2012, modified
Use Real Cases to Design Scenarios for Exercises

Use different ST-analyzis to approach different exercises
Practical testing NCR

Knowledge Flows

Proper steps
- Awareness of Problem
- Suggestion
- Development
- Evaluation
- Conclusion

Logical formalism
- Induction
  - Proposal
  - Tentative design
  - Artifact
  - Performance measures
  - Results

Deduction

Circumscription

Karokola 2012, modified
Socio-technical exercises to meet the demand of trained personnel
Case: Advanced Persistent Threat (APT)

“Advanced Persistent Threat (APT) is a term for a breed of insidious threats that use multiple attack techniques and vectors and that are conducted by stealth to avoid detection so that hackers can retain control over target systems unnoticed for long periods of time.”

Colin Tankard, 2011
Operation Socialist – GCHQ infiltration on Belgacom
## Root cause analysis – models used

<table>
<thead>
<tr>
<th>Withford</th>
<th>SBC-model</th>
<th>Kowalski</th>
<th>BSE-model</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human-centered</strong></td>
<td><strong>Synchronized</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Equity</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Sustainability</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Flexibility</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Validity</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>User involvement</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Innovation</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Communication</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Transparency</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Effects on the user</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Feedback</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Stakeholders</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Interaction</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Design</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Evaluation</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Testing</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Deployment</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
<tr>
<td><strong>Feedback and improvement</strong></td>
<td><strong>Scheduling</strong></td>
<td><strong>Sustainable</strong></td>
<td><strong>Sociocultural</strong></td>
</tr>
</tbody>
</table>

---

**BSE-model**

- **Scheduling**
- **Sustainable**
- **Sociocultural**

**Scheduling**

- **Sustainable**
- **Sociocultural**

**Sustainable**

- **Scheduling**
- **Sociocultural**

**Sociocultural**

- **Scheduling**
- **Sustainable**
Socio-technical modelling exercises
Future work

• Test at Norwegian Cyber Range (NCR)

“NCR will be an arena where testing, training, and exercise will be used to expose individuals, public and private organizations and government agencies to simulate socio-technical cyber security events and situations in a realistic but safe environment.”
Other future options

• Other socio-technical models?
• Ethical-Machine exercises?
• Capacity levels exercises – financial?
“Almost every crisis contains within itself the seeds of success as well as the roots of failure.” Harvard Business Review

THANK YOU

Grethe Østby
grethe.ostby@ntnu.no