A Practice-Based Pedagogy for Cybersecurity Education
Development of Practice-Based Education

Practice-Based Education (Higgs, 2013)

Pedagogy refers to a form of social practice that seeks to shape the educational development of learners. PBE is a pedagogy that prepares students for a practice or occupation.

PBE aims to realise the goals of developing students’ occupationally-relevant social, technical and professional capabilities, forming their occupational identities, and supporting their development as positively contributing global citizens.

Students’ prospective practice needs to be appraised and evaluated on an ongoing basis to provide a relevant frame of reference to situate students’ curriculum and pedagogical experiences.
From Practice-Based to Practice-Centered

Adapted Flow Channel Diagram

Certified Expertise
Adaptability Assessment
Ability Loop
Scenarios
Fail
Pass
Performance Assessment
Skill Loop
Exercise
Pass
Proficiency Assessment
Knowledge Loop
Instruction
START

VivoWorks
Accelerated Workforce Development

by Malcolm McCulloch — www.malcolmcc.com
(based on p74 of Flow by Csikszentmihalyi)
The Talent Crisis

- “Desperate shortage [of people with the skills] to design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts.”
  -- A Human Capital Crisis in Cybersecurity, CSIS, 2010

- “Only 15% of respondents are very confident that they have the security-related skill sets needed to meet evolving threat landscapes.”
  -- TEKsystems National Survey
A Vignette-Based Method

The collection of details that describe a critical incident:

- When the incident occurs (frequency or action sequence)
- What happens during the incident (problem or situation)
- Who is involved (entities or roles)
- Where the incident might happen (setting)
  - Optional:
  - Why it is important (Severity or priority of response)
  - How the critical incident is addressed (method, tools, or abilities that might be needed)
<table>
<thead>
<tr>
<th>Vignettes</th>
<th>Security Operations Center Role</th>
<th>IT Security Role</th>
<th>Network Administration Role</th>
<th>Incident Handling Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vignette: A new security vulnerability has been announced that affects your organization, such as a Microsoft vulnerability.</td>
<td>1. Update relevant detection mechanisms (e.g., IDS signatures)</td>
<td>1. Oversee patching process</td>
<td>1. Implement mitigating controls related to network infrastructure (e.g., potentially a firewall/proxy/router block)</td>
<td>1. Prepare to respond to any incidents related to exploitation of the vulnerability</td>
</tr>
<tr>
<td></td>
<td>2. Ensure operational procedures updated to respond to new alerts</td>
<td>2. Coordinate with application administrators, system administrators for patch testing and deployment.</td>
<td>2. Implement firewall blocks, router ACLs, ensure bandwidth SLAS, review router/firewall logs for suspicious traffic.</td>
<td>2. Respond to new compromises</td>
</tr>
<tr>
<td></td>
<td>3. Situational awareness of emerging threats related to the vulnerability</td>
<td>3. Assist in determining patch release timelines based on associated risk.</td>
<td>3. Implement new network mitigations related to this vulnerability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Coordinate with the firewall, network, antivirus and intrusion detection teams to understand the signature coverage, status of vulnerability scans, firewall blocks in place, etc.</td>
<td>4. Implement associated security mitigations, such as intrusion detection signatures, host-based intrusion detection signatures and controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Develop a notification / alert to be disseminated to all relevant parties.</td>
<td>5. Create new rules in security tools to watch for new compromises exploiting this new vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Monitor logs and IDS for new compromises that may be related to this new vulnerability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vignette: Data exfiltration: Company information / operations leaking to outside actor</td>
<td>1. Update relevant detection mechanisms (e.g., IDS signatures)</td>
<td>1. Evaluate recommendations in post mortem</td>
<td>1. Implement mitigating controls related to network infrastructure (e.g., potentially a firewall/proxy/router block)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Ensure operational procedures updated to respond to new alerts</td>
<td>2. Mitigate exfiltration and update security tools to monitor for exfiltration attempts</td>
<td>2. Assist in data gathering/monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Reviewing all sources of information relating to the data leakage to determine extent, time, location, etc.</td>
<td>3. Collect network information, netflow, router logs to assist in response.</td>
<td>3. Oversee remediation effort</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Monitor for exfiltration</td>
<td>4. Apply mitigations to firewalls and other network devices</td>
<td>4. Interface with law enforcement</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5. Determine root cause</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6. Coordinate with all other parties to identify, contain and mitigate the data loss.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7. Research how the attackers were able to compromise system to exfiltrate data, mitigate, and report findings on what information was exfiltrated</td>
<td></td>
</tr>
</tbody>
</table>
Typology of Task Complexity/ Difficulty

Table 3
Complex Task Classifications

<table>
<thead>
<tr>
<th>Task Type</th>
<th>Complexity Sources</th>
<th>Examples</th>
<th>Task Type</th>
<th>Complexity Sources</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Decision Tasks (Types 3, 7, 9, 12)</td>
<td>Number of desired outcomes to attain; Conflicting interdependence among outcomes; Uncertainty. (Path multiplicity irrelevant).</td>
<td>Employee selection: Choosing a house; Selecting a building site.</td>
<td>C. Problem Tasks (Types 2, 8, 10, 13)</td>
<td>Path multiplicity to single desired outcome; Conflicting interdependence among paths; Uncertainty. (Outcome multiplicity irrelevant).</td>
<td>Chess problems: Personnel scheduling: Personnel placement.</td>
</tr>
<tr>
<td>B. Judgment Tasks (Types 4, 5, 6)</td>
<td>Conflicting and probabilistic nature of task information; Uncertainty. (Multiplicity of desired outcomes and multiplicity)</td>
<td>Intelligence analysis: Stock market analysis; Multiple case probability learning.</td>
<td>D. Fuzzy Tasks (Types 11, 14, 15, 16)</td>
<td>Outcome multiplicity; Path multiplicity; Conflicting interdependence; Uncertainty.</td>
<td>Business ventures.</td>
</tr>
</tbody>
</table>
Decision Task Types

- Number of desired outcomes to attain
- Conflicting interdependence among outcomes
- Uncertainty
- Path multiplicity irrelevant
- EX: Employee selection, choosing a house, selecting a building site
Decision-Based Practice

● Incident Response
● Scanning

More Examples?
Judgement Task Types

- Conflicting and probabilistic nature of task information
- Uncertainty
- Multiplicity of desired outcomes
- Multiplicity of paths irrelevant
- EX: Intelligence Analysis, Stock Market Analysis, Multiple Cue Probability Learning
Judgement-Based Practice

● Diagnostics
  ○ Where are we vulnerable?
  ○ When did they get in?
  ○ What did they take?

● Network Forensics

● Intrusion Analysis

More Examples?

http://upload.wikimedia.org/wikipedia/commons/c/c6/Botnet.svg
Problem Task Types

- Path multiplicity to a single desired outcome
- Conflicting interdependence among paths
- Uncertainty
- Outcome multiplicity irrelevant
- EX: Chess problems, Personnel scheduling, Personnel placement
Problem-Based Practice

- Triage
- Incident Response
- Project Management
- Staffing
- Downtime
- Policies

More Examples?
Fuzzy Task Types

- Outcome multiplicity
- Path multiplicity
- Conflicting interdependence
- Uncertainty
- EX: Business Ventures
Fuzzy-Based Practice

- Zero-Day
- Inherited Networks

More Examples?

http://upload.wikimedia.org/wikipedia/commons/a/a4/PROSTAGLANDIN_H2_SYNTHASE-1_COMPLEX.png
Supporting Engagement

NCL Bracketing System

Bronze: Decision Tasks
Silver: Judgment/Problem
Gold: Problem/Fuzzy

VivoWorks
Accelerated Workforce Development
Questions and Discussion

Contact Information:

David H. Tobey  
Indiana University South Bend  
Email: dhtobey@indiana.edu

Portia Pusey  
VivoWorks, Inc.  
Email: portia@vivoworks.com