A Practice-Based Pedagogy for Cybersecurity Education

Development of Practice-Based Education

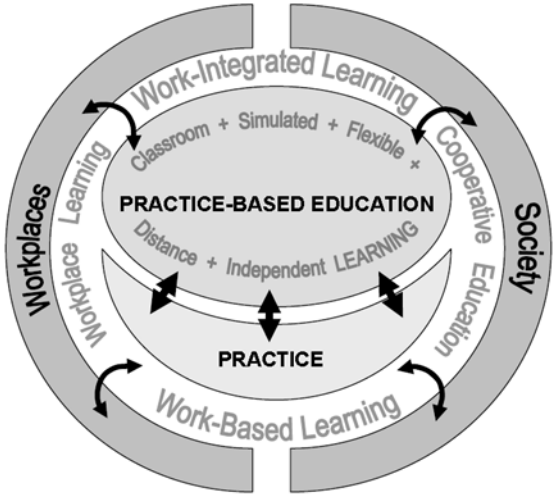
> *No reception without reaction, no impression without correlative expression — that is the great maxim which the teacher ought never to forget*
>
> *-- William James (1892) "Talks to Teachers"*

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.

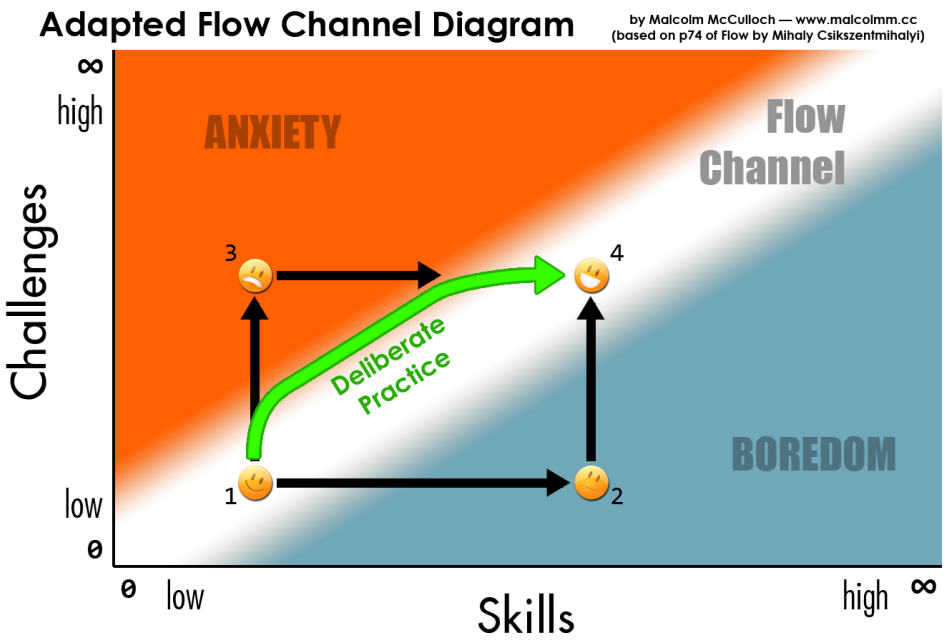
PBE aims to realise the goals of developing students' occupationally-relevant social, technical and professional capabilities, forming their occupational identities, and supporting their development as positively contributing global citizens.

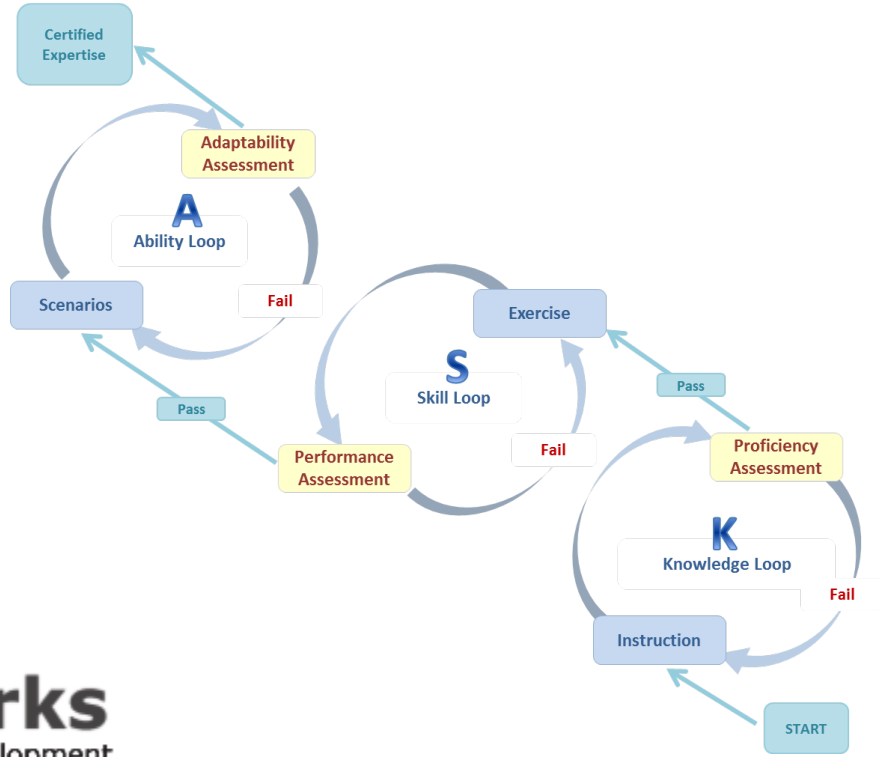
Students' prospective practice needs to be appraised and evaluated on an ongoing basis to provide a relevant frame of reference to situate students' curriculum and pedagogical experiences.



VivoWorks
Accelerated Workforce Development

From Practice-Based to Practice-Centered





VivoWorks
Accelerated Workforce Development

Importance of Practice-Centered Education

The Talent Crisis

- “Desperate shortage [of people with the skills] to 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

VivoWorks
Accelerated Workforce Development

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**

VivoWorks
Accelerated Workforce Development

Vignette

Vignettes	Security Operations Center Role	IT Security Role	Network Administration Role	Incident Handling Role
START HERE >>> **Vignette: A new security vulnerability has been announced that affects your organization, such as a Microsoft vulnerability.**	1. Update relevant detection mechanisms (eg IDS signatures) 2. Ensure operational procedures updated to respond to new alerts 3. Situational awareness of emerging threats related to the vulnerability 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. 5. Develop a notification / alert to be disseminated to all relavant parties. 6..Monitor logs and IDS for new compromises that may be related to this new vulnerability	1. Oversee patching process 2. Coordinate with application administrators, system administrators for patch testing and deployment. 3. Assist in determining patch release timelines based on associated risk. 4. Implement associated security mitigations, such as intrusion detection signatures, host-based intrusion detection signatures and controls 5.Create new rules in security tools to watch for new compromises exploiting this new vulnerability	1. Implement mitigating controls related to network infrastructure (eg, potentially a firewall/proxy/router block) 2. Implement firewall blocks, router ACLs, ensure bandwidth SLAs, review router/firewall logs for suspicious traffic 3.Implement new network mitigations related to this vulnerability	1. Prepare to respond to any incidents related to exploitation of the vulnerability 2. Respond to new compromises
Vignette: Data exfiltration: Company information / operations leaking to outside actor	1. Update relevant detection mechanisms (eg IDS signatures) 2. Ensure operational procedures updated to respond to new alerts 3. Reviewing all sources of information relating to the data leakage to determine extent, time, location, etc. 4 Monitor for exfiltration	1. Evaluate recommendations in post mortem 2.Mitigate exfiltration and update security tools to monitor for exfiltration attempts	1. Implement mitigating controls related to network infrastructure (eg, potentially a firewall/proxy/router block) 2. Assist in data gathering/monitoring 3.Collect network information, netflow, router logs to assist in response. 4.Apply mitigations to firewalls and other network devices	1. Determine scope of incident (number of systems, which data, etc) 2. Determine response plan (when to remediate, how to remediate) 3. Oversee remediation effort 4. Interface with law enforcement 5. Determine root cause 6. Coordinate with all other parties to identify, contain and mitigate the data loss. 7.Research how the attackers were able to comprise system to exfiltrate data, mitigate, and report findings on what information was exfiltrated

Typology of Task Complexity/ Difficulty

Table 3
Complex Task Classifications

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

VivoWorks
Accelerated Workforce Development

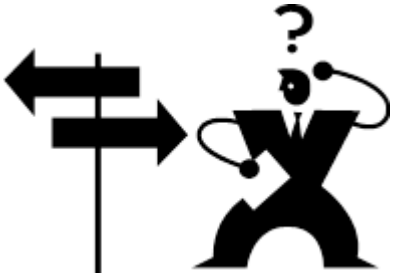
Campbell, 1988, Task Complexity

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?

VivoWorks
Accelerated Workforce Development

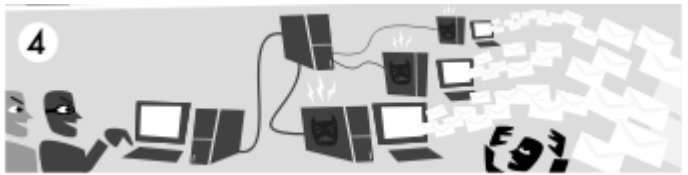
Judgement Task Types

- 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

VivoWorks
Accelerated Workforce Development

Judgement-Based Practice

- Diagnostics
  - Where are we vulnerable?
  - When did they get in?
  - What did they take?
- Network Forensics
- Intrusion Analysis



More Examples?

VivoWorks
Accelerated Workforce Development

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?

VivoWorks
Accelerated Workforce Development

Fuzzy Task Types

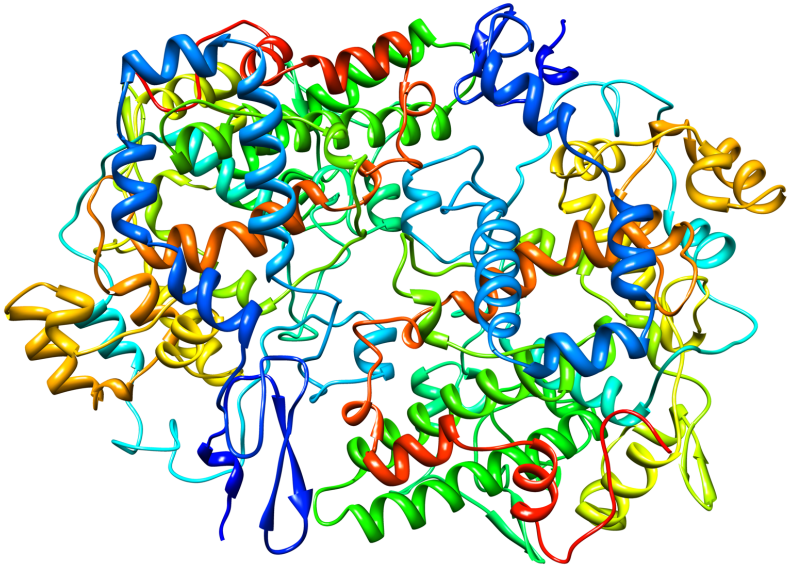
- Outcome multiplicity
- Path multiplicity
- Conflicting interdependence
- Uncertainty
- EX: Business Ventures

VivoWorks
Accelerated Workforce Development

Fuzzy-Based Practice

- Zero-Day
- Inherited Networks

More Examples?

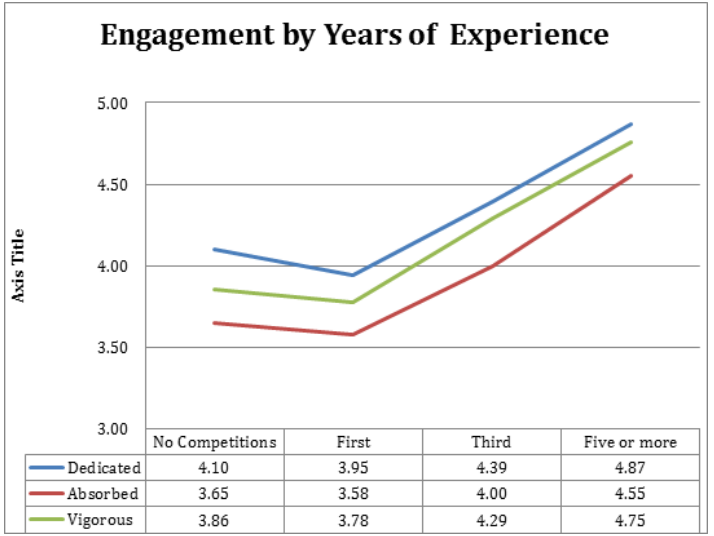


VivoWorks
Accelerated Workforce Development

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

Supporting Engagement

127 > 105 > 70



	No Competitions	First	Third	Five or more
Dedicated	4.10	3.95	4.39	4.87
Absorbed	3.65	3.58	4.00	4.55
Vigorous	3.86	3.78	4.29	4.75

Source: Tobey, D., P. Pusey, D. Burley. March 2014. Engaging Learners in Cybersecurity Careers: Lessons from the launch of the National Cyber League. ACM Inroads: Special Section on Cybersecurity Education

VivoWorks
Accelerated Workforce Development

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

VivoWorks

Accelerated Workforce Development