Leveraging Models from other Professions to Build a Holistic Cybersecurity Education Framework

Diana L. Burley, Ph.D. (dburley@gwu.edu)
Lance Hoffman, Ph.D. (lanceh@gwu.edu)
Costis Toregas, Ph.D. (toregas1@gwu.edu)

The George Washington University

2012 FISSEA Conference - March 2012
Outline/Purpose

- To illustrate how we might leverage educational models from other similarly complex professions to develop a holistic cybersecurity education and workforce development structure.

- During this session, we will:
  - Discuss the motivation for this inquiry
  - Highlight an example that unbundles the medical education analogy
  - Identify key questions and elicit feedback
Motivation

+ US must develop a comprehensive and coordinated effort to develop (educate and train) cybersecurity professionals (e.g. Evans & Reeder, 2010; Internet Policy Task Force, 2011; Burley & Bishop, 2011; Mulligan & Schneider, 2011)

+ This effort should be underpinned by a paradigmatic shift that adjusts the current emphasis from “students as customers” to “society as customers” and treats cybersecurity as a public good (Burley & Bishop, 2011; Mulligan & Schneider, 2011)

Educational models from other similarly complex professions along with insight from education research provides a starting point for framing this effort.
Transition in US Medical Education

- 19th Century medicine is compared to current state of cybersecurity profession
  - The emerging field addressed a complex, dynamic and somewhat unpredictable environment
  - Professionals had uneven capabilities
  - There were few standards of professional practice

- 20th Century - Flexner Report (1910) revealed serious gaps in medical education and spurred a focus on structure and process

- 21st Century - Shift from the structure- and process-based curriculum to a competency-based curriculum and outcome evaluation (Carraccio et al., 2002).
Curriculum...

<table>
<thead>
<tr>
<th></th>
<th>(19th Century Med Ed) Structure-based</th>
<th>(21st Century Med Ed) Competency-based</th>
<th>...as a Vehicle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orientation</td>
<td>Disciplinary focused</td>
<td>Emergent, dynamic</td>
<td>Fulcrum</td>
</tr>
<tr>
<td>Goal</td>
<td>Knowledge acquisition</td>
<td>Knowledge application</td>
<td>Acquisition &amp; application</td>
</tr>
<tr>
<td>Driver</td>
<td>Industry requirements/regulations/accreditation</td>
<td>Holistic view of the system (students, content, pedagogy)</td>
<td>Institutional focus</td>
</tr>
<tr>
<td>Priority</td>
<td>Employability</td>
<td>Community building</td>
<td>Institutional agenda</td>
</tr>
<tr>
<td>Customer</td>
<td>Student</td>
<td>System</td>
<td>Society</td>
</tr>
</tbody>
</table>

(19th Century Med Ed) Structure-based

(21st Century Med Ed) Competency-based

(Fotheringham et al., 2012)
Unbalanced Effort

SUGGESTED (but INSUFFICIENT EFFORT):
- Comprehensive
- Coordinated
- Paradigm shift

LOAD:
- Workforce Initiatives (e.g. NICE, OPM)
- Curriculum Mapping

Competency-based: Process

Vehicle

Balanced Curriculum (Product & Process)
Unbundling the Medical Analogy

Initiatives designed to define the cybersecurity professional framework (e.g. NICE) are driving cybersecurity education toward a structure-based curriculum that focuses on knowledge acquisition and employability. This is valuable **BUT IT IS ALSO:**

- Akin to 19th century medical education and **counter to current trends in medical education** toward a competency-based curricular model that emphasizes a knowledge application and societal needs.
- **Counter to calls for a coordinated and comprehensive effort** that treats cybersecurity as a public good

To follow the lead of medical education AND respond to calls for a paradigm shift, cybersecurity educators should increase effort toward a **competency-based curriculum that emphasizes a holistic perspective** – one that minimizes gaps, reduces overlaps, and supports outcome-based assessments.
Questions to Move us Forward

- Does the academy’s conceptualization of what cybersecurity professionals must know and be able to do align with the current and emerging realities of professional practice?

- Is the cybersecurity curriculum organized and delivered in ways that align with what cyber security professionals must know and be able to do now and in the future? And if not, how might it be?

- What professional goals and values might guide the cybersecurity profession in the continuously evolving context?
For additional information contact:
Diana L. Burley, Ph.D. (dburley@gwu.edu)
Lance Hoffman, Ph.D. (lanceh@gwu.edu)
Costis Toregas, Ph.D. (toregas1@gwu.edu)

References:

- Evans, K. and Reeder, F. 2010. Human Capital Crisis in Cybersecurity. Center for Strategic and International Studies