Cybersecurity Training Framework

Presented by Dr. Sherry Lakes

Federal Information Systems Security Educators Association (FISSEA) Annual Conference
14-15 March, 2018
Background

Biggest Known Data Breaches of 2013 and 2014

- Adobe: 152
- Community Health Service: 4.5
- Ebay: 145
- LexisNexis: 1
- Neiman Marcus: 1.1
- Target: 70
- JP Morgan Chase: 76
- Ubuntu: 2
- Home Depot: 56

Gmail: 5
Cybersecurity Initiatives

- Education
  - FISSEA
  - NICE

- Policy
  - Executive Orders
  - Publications

- Technology
  - Firewalls
  - Secure Token Services
Cybersecurity Professionals (Projected Need)

Information Security Analyst
Percent change in employment, projected

- Information Security Analyst: 37%
- Computer Operations: 18%
- Total All Occupations: 11%

Note: All Occupations include all occupations in the U.S. economy.

http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6
Cybersecurity Professionals (Increased Demand)

- Increased the demand for cybersecurity professionals
- Shortage of cybersecurity professionals has caused cybersecurity–related job openings in U.S. companies to go unmet
- Potentially negative impact of the shortage of cybersecurity professionals
Cybersecurity Professionals (Resolution)

- Instructor
  - What they know

- Student
  - Who wants to know
  - What they want to know
Chapman’s Model of Students’ College Choice

**Career Objectives** are not part of Chapman’s model
Cybersecurity Professionals (Student)

- Who wants to know
  - Novice
  - Experienced
  - Leadership

- What they want to know
  - General
  - Focused Area
  - Certification
Cybersecurity Professionals (Student)

<table>
<thead>
<tr>
<th>Objective</th>
<th>Course</th>
<th>Student</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Certification</td>
<td>Decision-Maker</td>
</tr>
<tr>
<td></td>
<td>Focus Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>General</td>
<td></td>
</tr>
</tbody>
</table>
Traditional Approach

- Preconditions
- Assumption/Compliance
- Objectives
- Rigid
- Commonality
- Delivery
Alternative Approach

- Enduring Framework
  - Impact Levels
  - Threats, Risk, Mitigation
  - Consistent
  - Reciprocal
Cybersecurity Professionals (Instructor)

- Capability
  - Novice
  - Experienced
  - Style
Why a Framework

- A framework is always used
  - Informal or formal
  - Inside a SME’s head
  - Ad-Hoc
Proposed Use of a Formal Framework

- Assess Effectiveness prior to delivery
- Documented
- Repeatability
- Consistency
- Formally agreed upon
- Understood by Stakeholders
Example Formal Framework

ADDIE Model:
- Analysis
- Design
- Development
- Implementation
- Evaluation
Example Formal Framework

- Kirkpatrick's Four-Level Training Evaluation Model:
  - Reaction
  - Learning
  - Behavior
  - Results
Cybersecurity Training Framework

- Course Objective
  - General Focus Area Certification
- Instructor
  - Experience Approach Personality
- Student
  - Novice Practitioner Decision-Maker
- Delivery
  - Synchronous Asynchronous Lecture
- Duration
  - Abridged
  - Comprehensive (Short)
  - Comprehensive (Long)
- Effectiveness
Framework Structure

- Category of Concern
  - similar groupings of elements to simplify analysis, and provide longevity to the model

- Each Category of Concern is defined by a set of Attributes
  - characteristics of the elements categories

- Each Attribute is rated on a scale, based on an Axiom related to the Attribute
  - Minimal Effectiveness Rating is derived from aggregate of attribute ratings

"Millennials tend to use social media more than baby-boomers"
# Rating Table

<table>
<thead>
<tr>
<th>Rating (Importance)</th>
<th>Objective</th>
<th>Category/Attribute</th>
<th>Instructor</th>
<th>Delivery</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Focus</td>
<td>Practitioner</td>
<td>Experience</td>
<td>Asynchronous</td>
<td>Abridged</td>
</tr>
<tr>
<td>Medium</td>
<td>Certification</td>
<td>Novice</td>
<td>Approach</td>
<td>Lecture</td>
<td>Comp (Short)</td>
</tr>
<tr>
<td>Low</td>
<td>General</td>
<td>Decision-Maker</td>
<td>Personality</td>
<td>Synchronous</td>
<td>Comp (Long)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rating (Importance)</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>H</td>
</tr>
<tr>
<td>Medium</td>
<td>M</td>
</tr>
<tr>
<td>Low</td>
<td>M</td>
</tr>
</tbody>
</table>
## Use Case

<table>
<thead>
<tr>
<th>Rating (Importance)</th>
<th>Objective</th>
<th>Category/Attribute</th>
<th>Instructor</th>
<th>Delivery</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Focus</td>
<td>Practitioner</td>
<td>Experience</td>
<td>Asynchronous</td>
<td>Abridged</td>
</tr>
<tr>
<td>Medium</td>
<td>Certification</td>
<td>Novice</td>
<td>Approach</td>
<td>Lecture</td>
<td>Comp (Short)</td>
</tr>
<tr>
<td>Low</td>
<td>General</td>
<td>Decision-Maker</td>
<td>Personality</td>
<td>Synchronous</td>
<td>Comp (Long)</td>
</tr>
</tbody>
</table>

20
Implementation Guidance

Course Objective
- General Focus Area Certification
- Experience Approach Personality

Student
- Novice Practitioner Decision-Maker

Delivery
- Synchronous Asynchronous Lecture
- Abridged Comprehensive (Short) Comprehensive (Long)

Duration
- L
- M
- M

Effectiveness
- M

Highest
Way Forward

- Increased Demand for Cyber Professionals
- More Effective Training
  - Repeatable
  - Consistent

- Collect actual use cases
- Determine baseline importance weights
- Automate Framework Calculations
- Augment Framework with more granularity
THANK YOU!!!