Anatomy and Forensics of a Failed Course

Al Payne, CISSP
Theta Solutions, LLC.
703-409-4039
Alpayne@verizon.net

Jim Litchko, CAS
Litchko & Associates, Inc.
301-661-3984
jim@litchko.com
Wisdom & Learning

“There are three kinds of people:
– The ones that learn by reading.
– The few who learn by observation.
– The rest of them that have to touch the electric fence for themselves.”

- Will Rogers (paraphrased)

"Good judgment comes from experience and a lot of that comes from bad judgment."

- Will Rogers
Topics of Discussion

• Client Said – We Thought
• Screen Shots VS Hands On
• Structured Lecture VS Interactive

Each section there will be a five minute “What would you have done?” session.
Forensic Lab Case #1

What Client Said vs. What We Thought
Setting The Stage

• Client:
  – Knowledgeable and sophisticated
  – Asked for proposal
  – Train IT security officers to use accepted organization’s security testing tools
  – Headquarters setting with multiple classes

• Similar to other courses we had developed

• We bid and win the contract

• Joy, glee and visions of reasonable $
The Awakening

• Client in the interim has learned and used the tools
• Having gone through the experience client now knows EXACTLY what should be done
• And the FUN begins
What Client ‘Knows’ They Need
What The Clients NOW Wants

• Standard lecture, NOT interactive
• No hands on
• Have remote classroom access
• Change the course content and approach
• Test results analysis as part of the course
• Be one of the instructors for the course
# What Would You Do?

<table>
<thead>
<tr>
<th>What is the problem?</th>
<th>What causes the problem?</th>
<th>What are possible solutions?</th>
<th>What do I recommend?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client said, we thought</td>
<td>Our prior experiences</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard lecture only</td>
<td>Client need for control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen shots, no hands on participation</td>
<td>Attendees needs &amp; expectations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Forensic Lab Case #2

Screen Shots vs. Hands-On
# Course Purpose & Retention

<table>
<thead>
<tr>
<th>Covers</th>
<th>Awareness</th>
<th>Training</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What</td>
<td>How</td>
<td>Why</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Aim</th>
<th>Recognize and remember</th>
<th>Develops skills</th>
<th>Knowledge and understanding</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Regulatory</th>
<th>Required</th>
<th>Required</th>
<th>Prudent</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Read / Test 25%</th>
<th>Use in Exercise 40%</th>
<th>Interactive 85%+</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-line</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Classroom</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Interactive and problem solving</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

This table outlines the purpose and retention goals of a course, covering awareness, training, and education. The table also details the required methods of learning, including read/test, use in exercise, and interactive components. The aim is to recognize and remember, develop skills, and understand knowledge and understanding. Regulatory requirements are indicated as required.
Control VS. Attendees Needs

• Client wanted ‘structure’ to control process, max dollars and not be embarrassed
• Attendees wanted hands on, interactive and collaborative solutions for their systems
Hands On and Collaboration

• Buy into security solution
• Implement it with enthusiasm
• Now have a working partner, more resources and open lines of communications
# What Would You Do?

<table>
<thead>
<tr>
<th>What is the problem?</th>
<th>What causes the problem?</th>
<th>What are possible solutions?</th>
<th>What do I recommend?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client said, we thought</td>
<td>Our prior experiences</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard lecture only</td>
<td>Client need for control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen shots, no hands on participation</td>
<td>Attendees needs &amp; expectations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Forensic Lab Case #3

Structured Lecture vs. Interactive
Let Me At ‘EM Coach

- IT Pros, security types and operators
- We don’t need no stinking manual / course
- Just let us get on the system
- We know more than you paper pushers
- I’m only doing this so I can get certified – NOT learn the policies
Screen Shots ONLY

• Client thought
  – Force them to do it our way
  – Structured
  – All get the same results
  – Allow us to cover a lot of material in the time and dollars allotted
# What Would You Do?

<table>
<thead>
<tr>
<th>What is the problem?</th>
<th>What causes the problem?</th>
<th>What are possible solutions?</th>
<th>What do I recommend?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client said, we thought</td>
<td>Our prior experiences</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard lecture only</td>
<td>Client need for control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen shots, no hands on participation</td>
<td>Attendees needs &amp; expectations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Summary

• Sometimes no matter what goes wrong it still works out right if the content is correct
• WTP, WCTP, WAPS and WDIR sheets
• Interactive and collaborative works for us too
Questions?

Thanks for your time and attention
Al Payne, CISSP  
Jim Litchko, CAS

Combined 60 years experience in managing IT systems and IT security.

Practitioners, integrators, consultants, executives, program managers, budgeters, educators, motivators and facilitators.

Worked in government, military, commercial and academic positions. From NSA to Johns Hopkins University.

Have assessed over 150 IT systems from the White House to an Internet gambling casino.

Authors of four books and speak on security topics at over 30 events a year.

Former Navy and Marine Corp officers.