Establish Security Psychology
~ How to Educate and Training for End users ~

CONTENTS

I. INTRODUCTION
   1. Definition of Information Assets
      • People: To operate and monitor the services
      • Information & data: To feed the process and to be produced by the service
      • Technology: To automate and support the service
      • Facilities: In which to perform the service
   2. Aspect of Human protection
      Bird’s eye view of Human protection (Education, Training, Awareness)

II. Practical Security Training for End-users
   1. Purpose of this training
      1-1 Training background (Targeted attack by phone)
      1-2 Participants
   2. Education & Training
      2-1 Concept of Education & Training
      2-2 Result of Training

Conclusion
1. Definition of Information Assets

- People: To operate and monitor the services
- Information & data: To feed the process and to be produced by the service
- Technology: To automate and support the service
- Facilities: In which to perform the service

If any of them cannot be protected, security incident may be occurred.

To protect assets:
- Technical protection: F/W, IDS, SIEM, Anti-virus etc.
- Human protection: Education, Training, Awareness

2. Aspect of Human protection

Bird’s eye view of Human protection (Education, Training, Awareness)
1. Purpose of this training

1-1 Training background (Targeted attack by phone)
- Private information about a woman who was stalked and killed by her former boyfriend a year ago is thought to have been leaked by the local government in Japan.
- Senior official of the firm is suspected of obtaining her address from the local government within hours of receiving the request and giving it to the detective agency.
- It seems that the senior official used the elicitation technique which is technique used to discreetly gather information.

1-2 Participants of 3-hour training
- 37 staff of other local government
  - Citizen service group
  - Systems dept. etc.

2. Education & Training

2-1 Concept of Education & Training
- Due to the local government request, education and training will be determined 3 hours.
- Shortage of time;
  - Group work and discussions in subgroups will be replaced by watching a video.
  - Show typical figures below, teach participants not to make a simple mistake.
    - Fig. 1: No parking
    - Fig. 2: Illusion of Fraser
    - Fig. 3: Muller-Lyer illusion

FBI https://www.fbi.gov/file-repository/elicitationbrochure.pdf/view

Fig. 1: No Parking
Fig. 2: Illusion of Fraser
Fig. 3: Muller-Lyer illusion
2.  Education & Training

2-1 Concept of Education & Training
- Related topics of the Incident
  - Details of information leaks from the local government are not disclosed. Since the training is for local government staff, the contents of the incident were described briefly.
  - The information security issues of the local government, especially the security management was explained.
- Elicitation Techniques (One of the most important social engineering)
  - This Elicitation techniques seemed to be used at this incident and were explained in detail.
- Teamwork training
  - Overview of human error & Countermeasures in other fields:
    - Aviation: CRM (Crew Resource Management)
    - Medical: Team STEPPS (Team Strategies and Tools to Enhance Performance and Patient Safety)
  - Human Error: an organization problem, not an individual problem.
  - Inattentinal Blindness: a psychological lack of attention that is not associated with any vision defects or deficits. Use the invisible gorilla's video to make participants understand the meaning of inattentiveness blindness.

FBI: https://www.fbi.gov/file-repository/elicitation-brochure.pdf

2-2 Result of Training
- Training Satisfaction
  - Very useful............................. 57% (21 people)
  - Somewhat helpful........................ 43% (16 people)
  - Not very useful / Not useful at all: 0%
- Some comments for training
  - How to deal with the importance of organizational strength and organization?
  - It was an opportunity to think about the problem of the current information informing method
  - I reaffirmed the importance of business analysis
  - It was a good opportunity to reaffirm the stalker incident
  - It was a good opportunity to think human error from many points
  - I got the mental attitude to protect personal information
  - The way of thinking, the checking method etc were helpful
  - The point of view of thinking about creating a structure according to workers was helpful
- Would you recommend this training to others?

<table>
<thead>
<tr>
<th></th>
<th>1 : Low</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6 : High</th>
<th>No Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(3%)</td>
<td>35 (95%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>(3%)</td>
<td>34 (92%)</td>
<td>3 (8%)</td>
<td>7 (19%)</td>
<td>16 (43%)</td>
<td>2 (5%)</td>
<td>(cumulative)</td>
</tr>
<tr>
<td>3</td>
<td>(8%)</td>
<td>33 (89%)</td>
<td>30 (81%)</td>
<td>23 (62%)</td>
<td>7 (19%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(19%)</td>
<td></td>
<td></td>
<td>7 (19%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>(43%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>(5%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Establish Security Psychology  
~ How to Educate and Training for End users ~

2. Education & Training

2-2 Result of Training

<table>
<thead>
<tr>
<th></th>
<th>0: Low</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding of the training</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>12</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>Utilization of Business</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>3</td>
<td>6</td>
<td>11</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Same as attendee's motivation</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>3</td>
<td>7</td>
<td>9</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Instructor's skill and materials, etc.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>11</td>
<td>5</td>
<td>8</td>
</tr>
</tbody>
</table>

Note1: NPS (Net Promoter Score)
Not at all likely | Neutral | Extremely
Detractor | Neutral | Promoter

Note2: The Kirkpatrick Model

Level 4: Results
The degree to which targeted outcomes occur as a result of the training and the support and accountability package

Level 3: Behavior
The degree to which participants apply what they learned during training when they are back on the job

Level 2: Learning
The degree to which participants acquire the intended knowledge, skills, attitude, confidence and commitment based on their participation in the training

Level 1: Reaction
The degree to which participants find the training favorable, engaging and relevant to their jobs

Establish Security Psychology  
~ How to Educate and Training for End users ~

Conclusion

- The expected results obtained.
- Group discussion could not be possible due to shortage of time.
- I would like to incorporate Kirkpatrick's evaluation into the training from next time.
Establish Security Psychology
~ How to Educate and Training for End users ~

Thank you!

Acknowledgements
This research of the Information Security Psychology study group has been granted by the Japanese Psychological Association (JPA) from 2011.

Questions ?

Comments!

Rebuttals . . .

Institute of Security Psychology
Emeritus Professor
Katsuya UCHIDA, Ph.D.
e-mail: uchidak@gol.com
Twitter: @woodytokyo
Facebook: woodytokyo
Web: http://www.uchidak.com/Eng/