Integrating The Information Security Awareness in Critical Infrastructure Firms

Mohamed ElHarras
CIIP Strategies and Policies Executive Director

Agenda

- The Connectivity Dissemination.
- Current / Proposed Defense Models.
- The Critical Infrastructure Information (CII).
- The Importance of Awareness.
- Case Study: Mobile Operators.
- Q&A
The Dissolve of Political Borders

- The Internet has made it possible to connect (hence access or attempt to access) any computing device on/off the net.

The Consequences

- The Threat of pervasive and ubiquitous computing while tools of attacks becomes more available as wrap-up for non technical people.
The Current Defense Model

- With that large number of connections, it will not be feasible (or possible) for effective defense to the individual citizen level.

As Per this Model

The cyber security staff is the focal point to handle:
- Detection.
- Reaction.
- Correction.
- Prevention.

The current model requires:
- On-going increase in the number of specialized staff.
- Associated increasing costs.
- Does not cover all possible weak points.
Balancing the Model

- Push the line of defense to non-specialized individuals.
- Rely more on human element to help detecting basic threats / anomalies at early stage.

The Individual is the First Line of Defense.

We need to build his capacity of self-defense.

Selecting the Points of Defense

- Massive impact.
- Quick win.
- Fast deployment.
- Minimum cost.
- On going.
The Critical Infrastructure Sectors

- Affects large sectors of the society or the ability of the government to do its function.
- Usually owned or operated by the private sector.
- Each CI sector affects other sectors in a domino effect model.
- The list of CI Sectors includes:
  - Government services
  - Financial service
  - Telecommunication
  - Energy
  - Transportation
  - Health Services
  - Etc.

Case Study: Mobile Telecommunications

National Telecom Regulatory Authority - EGYPT
The Telecom Critical Information Infrastructure

Pervasive and ubiquitous information on:

- Call details → social patterns and relations ..etc.
- Location details → movement patterns, spontaneous location check ..etc.
- Live call (on air).
- Network architecture layout (BTS, BSC, MSC, ..etc.)
- Network coverage plans.
- Network security measures (on-air, core network, ..etc.)
- Affects majority of the society.

The Telecom in the Arab Countries

Mobile penetration in the Middle East (Source: GSMA Report, 2014)
How to Measure Awareness

- Check list auditing approach.
- The questionnaire approach.
- Interviews: sample staff.
- Observation: staff / processes.
- Focus group: representing business areas.
- Case study (usually after incidents).

Common Corporate Perception of Security

- Top Management: “security is necessary but to the minimum required by law”.
- Employees: computer security is an obstacle to productivity. A common feeling is that “we are paid to produce, not to protect” or “Security is not on my objectives list”.

National Telecom Regulatory Authority - EGYPT
Security Knowledge Matrix

<table>
<thead>
<tr>
<th>Level</th>
<th>Awareness</th>
<th>Training</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective</td>
<td>Recognition</td>
<td>Knowledge</td>
<td>Insight</td>
</tr>
<tr>
<td>Channel</td>
<td>Media</td>
<td>Practical Instruction</td>
<td>Theoretical Instruction</td>
</tr>
<tr>
<td>Example</td>
<td>Video, Newsletter, Poster, giveaways</td>
<td>Lectures, case study, hands-on practice</td>
<td>Seminars, essays</td>
</tr>
<tr>
<td>Test Method</td>
<td>True/False MCQ</td>
<td>Problem solving</td>
<td>Essay</td>
</tr>
<tr>
<td>Attribute</td>
<td>“What”</td>
<td>“How”</td>
<td>“Why”</td>
</tr>
</tbody>
</table>

Source: NIST800

Security Awareness Program Life Cycle

- **Get Commitment**
  - Top management
  - HR
  - Timeframe
  - CS, Sales, etc.

- **Planning**
  - Objectives
  - Audience
  - Depth
  - Channels
  - Cost
  - Team / materials
  - KPIs

- **Measure**
  - Snap shot of current status
  - Change in behavior
  - Consider feedback
  - Improve program

- **Execute**
  - Different channels
  - Embed in Objectives

Change in staff behavior is the best result we can get.
Message Delivery

- Gathering Points.
  - Firm restaurants.
  - Banners by access points (doors / elevator).
  - Stickers by electronic gates.

- Internal Communications:
  - Newsletter.
  - Company briefing meetings.
  - Monthly message from the CEO.

- Interaction with Company Systems:
  - Screen savers.
  - Screen wallpapers.
  - Logon message.
  - Daily tips.
  - Quick quiz.
  - Computer-based training.

Background work

- Human Resources.
  - Incorporate security awareness in job responsibilities when applicable.
  - Proportionately add security awareness to employees appraisal system.
  - Prepare the rewarding system for program heroes.
  - Review materials for message correctness and balance.

- Legal / Regulatory:
  - Add relevant laws / regulations to awareness program.
  - Highlight law penalties in case of violations.
  - Add other related issues (e.g. fraud, corruption ..etc.)
  - Give examples from legal arena.
Common Pitfalls

- Not fitting the environment.
- Inadequate planning.
- Not addressing applicable legal / regulatory requirements.
- No motivation for staff.
- Budget mismanagement or inadequate budget.
- No leadership support.
- Information overload
- Not sharing experience.
- Not evaluating the effectiveness of training.

The Impact of Social Engineering

- Psychological manipulation of people to do action / divulging confidential information.
- Most common in people-facing functions (e.g. customer care agents, technical support, marketing).
- Best technique:
  - The familiar customer → normal to be there so the CC lowers self-defense.
  - The angry customer → angry at someone else rather than the target CC agent.
  - The knowledgeable customer → customer equipped with the necessary information about the company.
- How to fight?
  - Training → listen to customer calls, give examples.
  - Prepare scripts to handle social engineering situations.
  - Stick to the process.
  - Train for non-verbal communications.
Data Leak – Crafted Attacks

- Exploits zero-day / undocumented vulnerabilities.
- Involves highly-skilled preparation and know how.
- Aims at getting the information giving “commercial advantage” to the company.
- Target individual functions, typically the ‘C’ level; the R&D and the Marketing departments.
- How to fight?
  - Awareness program for the company executive.
  - Proportionate technical measures (e.g. encrypt data, secure email, stringent email rules ..etc.)
  - Internal / external stake holders involvement.

Channels of Communications

Source: multiple internet sites
**Model Benefits**

- Massive capacity builder.
- Awareness is a take-home skill.
- Lower cost per individual compared to building large specialized technical force.
- Filters false positives.
- Off load specialized staff to more serious threats.
- Early detection of some threats.

**Key References**

- The International Society of Security Awareness Professionals http://www.iasapgroup.org/
- Rebecca Herold, “Managing an Information Security and Privacy Awareness and Program and Training Program”, CRC 2011
Q & A

- YYYY