The 7 Habits of Highly Successful Security Awareness Programs

Samantha Manke and Ira Winkler
Internet Security
Advisors Group
Why Security Awareness?
Captain Kirk

- Who wouldn’t guess a password of “Captain” on an account with the user ID, “Kirk”?
- This happened at NSA
Whose Fault Is it?

- She sounds like an idiot
- She is an Ivy League graduate
- Why was she not previously told that she shouldn’t have that as a password?
- Why was the password allowed in the first place?
This Is Not Unique

- Security professionals make assumptions in the base level of knowledge in end users
- Also extends to knowledge assumptions about other technical professionals
- As per Felix Unger, when you assume you make an ass/u/me
Common Sense

- The problem is that security professionals assume that the users should exercise common sense
- There is no such thing as common sense without a base common knowledge
- Security programs fail, because they assume there is the common knowledge
It’s Not Stupid Users

- It’s incompetent security professionals
- While there are some stupid activities on the part of the users, I always ask what could the security staff have done better?
- Does your staff stop and ask how could the incident have been prevented
- Is there a discussion of both modifying user activity and preventing user activity
Security Awareness is Implementing Security Culture

- Not exactly, but close enough
- Security awareness is to get people to implement secure practices into their daily activities
- Security awareness is to strengthen security culture
- Must instill common knowledge of concerns and base actions
Why Security Awareness?

- The human factor
- Technology can only help so much
  - Security Awareness programs are an integral part of a mature security program
- Cost-Effective Solution
  - Required by standards and regulations
The Problem with Security Awareness Programs

- Varying degrees of quality in awareness programs
- The 3-year cycle
- Poor security cultures
The Study: Opportunity Statement and Methodology
Opportunity Statement

- My work experience allowed me the unique experience to build a program from scratch
- The local ISSA chapter’s Security Awareness user group (a.k.a. “Support Group”) meets bi-monthly and delegates were willing participants
- Security Awareness material is seen as non-proprietary
Approach/Methodology

- Qualitative
  - Face-to-face interviews with Security Awareness Specialists
- Quantitative
  - 2 Surveys
    - 1 for Security employees
    - 1 for Non-Security employees
- Limitations
Analysis: General Trends

- In the end a total of 7 companies participated
  - 2 from the Health Sector
  - 2 from the Manufacturing Sector
  - 1 from the Food Sector
  - 1 from the Financial Sector
  - 1 from the Retail Sector
- Companies were often surprisingly honest about the success of their programs
- No participating company had any metrics to assess their effectiveness
Analysis: General Trends

- Most companies struggle to gain support:
  - From upper management
  - From key departments
  - From their user population

- Compliance:
  - PCI helps with support and budget
  - HIPAA does not
Analysis: General Trends

- Variety of approaches
  - Some Security Awareness Specialists had a security background while others had a marketing or communications background
  - Companies had 1-26 employees contributing to efforts
Analysis: Security Respondents

• 87% of Security Respondents ("SRs") reported their programs are successful
• Roughly half reported having difficulty encouraging their employees to take security seriously
• Only 19% reported a lack of support from management
Analysis: Security Respondents

• 26% reported a lack of enthusiasm for their efforts

• 50% reported having difficulty receiving funding for their initiatives
Analysis: Non-Security Respondents

• 100% of Non-Security employees reported having learned something from their company’s Security Awareness program

• 100% reported being “security-minded individuals”

• 100% reported thinking their company’s Security Awareness programs are successful
Analysis: Non-Security Respondents

- Only 60% reported changing their behavior as a result of Security Awareness
- 92% reported viewing their Security team positively
- 12% reported having conflicts with their Security team
Results

• Security is difficult to administer at most companies
• PCI compliance helps with enforcement and awareness
• Creativity and/or mandatory training are the key(s) to success
• Companies with more top-level support are more successful
The Habits
Habit 1-Create a Strong Foundation

- This is the main source of failure
- Make a 3-month plan
- Topics may change
Assess Approach

- Softball
- Hard push
- Avoid fear-mongering
Deciding Which Components the Program Should Have

- Which mediums of communication will be most effective at your company?
- Which mediums are already saturated?
- What are employees most receptive to?
Recommended Components

• Website
• Posters
• Newsletters/Blog
• Monthly tips
• Lunch and Learns
• Roadshows
• Speakers
• Security Week
Keep the Program Fresh

- Easy to fall behind
- Pay attention to the news
- Create new material for every month
Habit 2 - Organizational Buy-In

- Appeal to the highest level you are able to engage
- Market some materials to the C-level
- Stress benefits of Security Awareness
Habit 3-Participative Learning

- Learning modules
- Interactive components
  - Make user feel involved
- Additional tools--Phishing
Habit 4 - More Creative Endeavors

- Guerilla marketing campaign
- Security Cube
- Demonstrations and movie showings
Habit 5 - Gather Metrics

- No participating company gathered metrics
- Compare rate of reported incidents pre and post
  - Collecting metrics ahead of time so you can potentially measure success after the fact
  - Should you do a pen test/assessment?
Assessing Success

- Assess which components have been successful
- Administer a survey
  - Try to keep it anonymous
  - Offer a drawing that employees can enter for a prize
- Understand limitations
Habit 6-Partner with Key Departments

- Reinforces company message vs. security message
- Consider departments such as:
  - Legal
  - Compliance
  - Human Resources
  - Marketing
  - Privacy
  - Physical Security
Habit 7-Be the Department of How

- Department of “How” vs. Department of “No”
- Teach instead of dictate
- Establish positive security culture
Conclusions
Next Steps

- ISSA’s “Great Security Awareness Experiment” series
- Many opportunities for additional research
  - Non-security employees should be re-surveyed
  - Additional companies from different sectors could be included
  - A deeper dive into participating companies could be conducted to ask about discrepancies
Apply

• Focus on building support before spending too much time on other aspects
• Do a thorough assessment of culture before starting or revamping program
• Consider partnership with other key departments
• Focus security awareness on common knowledge so users can exercise common sense
For More Information

Samantha@isag.com
+1-651-325-5902
http://www.linkedin.com/pub/samantha-manke/21/34/779

ira@isag.com
+1-410-544-3435
www.facebook.com/ira.winkler
@irawinkler
www.linkedin.com/in/irawinkler