Hacking the Corporate Mind

Using Social Engineering Tactics to Improve Organizational Security Acceptance

James Philput

Why Should You Listen To Me?

- Aside from the fact that you paid to be here…
- 15 years worth of IT experience
- 10 years as an infosec geek
  - Primarily network defense
- Currently Sr. Information Assurance Analyst for IAP – Information Assurance Professionals
- Technical reviewer for SANS
- Past author and instructor for SANS
- Past work in the telecommunications, education and medical fields as well as work with state and federal government organizations

Engagement: Improve Organizational Acceptance of Infosec

- **Step 1 – Define the problem**
- Step 2 – Define the rules of engagement
- Step 3 – Attack!
- Step 4 – Lessons Learned

Defining The Problem

- Infosec is struggling
  - With the users
  - With the budget
  - With the bad guys
- Organizations are leaking
  - Financial Data
  - Trade Secrets
  - Embarrassing Memos
- The bad guys are winning

How Can We Fix This?

- Infosec and the Users need to cooperate

Know Your Enemy, Know Yourself

- The largest obstacle to acceptance is:

YOU

Infosec is an Obstacle

- Numerous articles on how to improve IT
  - Technical Press
  - Industry Blogs
  - Mailing Lists
- Commenters Routinely Post Quotes Like These
  - "Security needs to get out of the way"
  - "Just let me work"
  - "The geeks are mean"
  - "IT is unapproachable"

The Users

“Note to Self: They are people not users”
– Lenny Zeltser

- Not fully understanding IT is not a crime
  - Though it can be really annoying
- They’re not geeks
- They’re not dumb
- They are frequently experts in their own fields
- Stop pronouncing “user” with a leading “L”

Business Need Trumps Security

This is the hardest thing for defense geeks to accept

- Changing these perspectives is daunting but doable
  - The dollar cost of a breach goes up when you factor in reputation
    - Damage to corporate image is expensive
    - Damage to executive reputations is also pricey
  - Ask for it in writing
  - Ask how a breach will play in the media
    - Be very careful with this one
- In some cases a risk MUST be accepted in order to do business

Infosec Needs Champions

- Modern infrastructure challenges
    - Consumerization
    - Cloud Computing
    - Fluid Network Boundaries
    - Changing Threat Landscape
- How do we make the users care?
    – Without the use of power tools

Who Are You?

“It’s not who you are. It’s who you know”

- Various

What Do You Want?

- A chance to make things better
- The ability to make the network safer
- The ability to prevent information from being stolen
- To protect the work, lives and livelihoods of the people using our networks

Engagement: Improve Organizational Acceptance of Infosec

- Step 1 – Define the problem
- **Step 2 – Define the rules of engagement**
- Step 3 – Attack!
- Step 4 – Lessons Learned

What is an Infosec Geek to do?

- We can’t hide from the users
- We can’t penalize the group for the actions of a few
- We can’t be the traffic cops of the organization
- We can use our own skills to gain acceptance
    - Problem Solving
    - Social Engineering

Talk you Introverted Bastards!

- Communication is the key
  - Learn how to make small talk
  - Attend office functions
- Many users accept limitations that they understand
- Simply talking to your users can build bridges
- For many users Introverted=Mean

Engagement: Improve Organizational Acceptance of Infosec

- Step 1 – Define the problem
- Step 2 – Define the rules of engagement
- **Step 3 – Attack!**
- Step 4 – Lessons Learned

Put On Your Social Engineering Hat

- Start paying attention to your users' habits
- Find the best way to infiltrate each target group
- Learn how to speak to them the way they speak to each other
- Get the information you need
- Plant the information you want distributed

Find out how to blend in

- Sometimes a necktie gets you more ears than a well reasoned argument
- Fashion matters to some users
  - Talk to your significant other, or annoying fashionable sibling for pointers
- Suits listen to other suits
  - It's like gang colors
  - If you were running a physical pen test on an organization, would you dress the way you do on a normal day at the office?
  - Clothing has a surprising way of getting people's attention

Examine the Target

- Look at how they work
- Find out where they talk
  - And what they talk about
- Get an idea of what is important to them
  - A little personal interest goes a long way
- Use their names in conversation

Strike

- Recon is complete, now what?
- Use what you've learned
- Protective camouflage
- Communicate as they do

Insert The Data

- You’re no longer
  - The Security Dude(ette)
  - The IT person
- You’ve become $yournamehere
  - Human in the eyes of the users
- Start talking to them
  - About how infosec impacts them
  - What a breach can do to the company
  - What they can do to help fix potential problems
  - How you can make their lives easier and more secure

Case Study: Prox Card Login

- Clinicians want faster access to records
- Non-technical management wants card based system
- Prox card based for various reasons
  - Existing badges can be used
  - No extra item to carry
  - Users already familiar with the technology
  - Prox cards are the cheapest option
- Vendor claims HIPAA compliance
  - Without the need for a PIN at each login

Case Study: Prox Card Login (2)

- The project is sent to the security team
- The cost argument fails
- The policy argument fails
- Infosec speaks to the proposing department
  - Finds that the current login setup is taking away from patient care
  - New system allows more direct time with patient
  - System is secure because clinicians always have their badges

Case Study: Prox Card Login (3)

- Security explains the risks
  - Commodity hardware allows easy badge cloning
  - Cloned badges expose clinicians to liability
    - HIPAA violations
    - Accusations of billing fraud
    - Fraudulent narcotics prescriptions
- Security offers options
  - Chip and PIN based system
  - Prox card with PIN entry at every login
- The prox card system is implemented more securely

Listen to the Users

- Don’t forget to listen
- Learn how they work
- Find out what they need
- Listen to how security “gets in the way”
- Empathize and Explain
- Build your security with the users in mind
  - Help them do their jobs more securely

Change Your Plans

- Adapt your security plans
- Take the complaints and Learn from them
- Make Security make sense to the user
  - Inconsistent policies = violated policies
- Loosen restrictions that don't need to be in your organization

Engagement: Improve Organizational Acceptance of Infosec

- Step 1 – Define the problem
- Step 2 – Define the rules of engagement
- Step 3 – Attack!
- **Step 4 – Lessons Learned**

Communication

- Focus on the audience
- Know their strengths
- Know their limitations
- Shorten your emails

"If you can't explain it simply, you don't understand it well enough"

-Albert Einstein

C-Level Wants Different Information

- Spend x to save y
- Short points, easily digestible
- Clear goals and costs
- Regulatory requirements

Non-Technical Management

- How will this impact them
- How will this impact their employees
- What is the impact to the business
- Is this a regulatory requirement

Technical Management

- What is the problem
- How do we solve it
- How else do we solve it
- What is the likelihood of exploitation

Conclusion

- Communication solves problems
- Understand your users and adapt to allow them to work
- Explain limitations
- It won’t work with everyone, but it will help

Questions?

James Philput
james@philput.com
@jphilput