



Security in knowledge

## Security Culture:

### Figuring Out How Bad Your Company Really Is

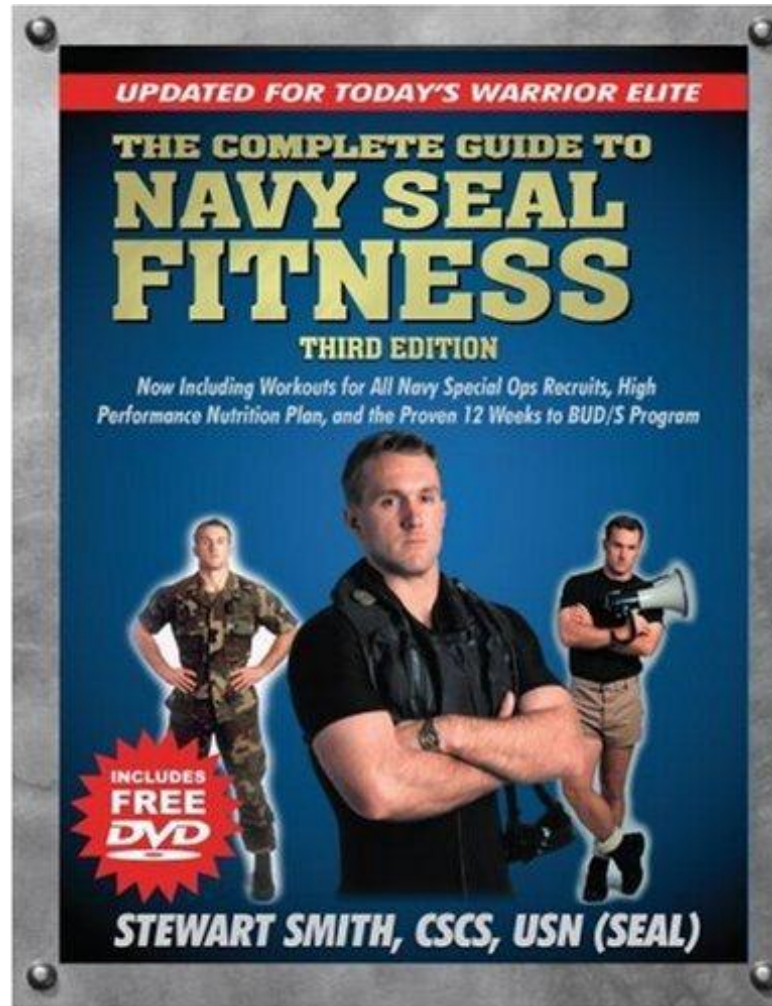
Ira Winkler, CISSP

Codonomicon

Session ID: EXP-W25

Session Classification: Intermediate

# Stew



# My Teachable Moments

- ▶ Person reporting their coworker spoke a lot of Chinese on the phone
- ▶ Tailgating employee stopping a laptop thief
- ▶ Employee being fired for stopping a tailgater
- ▶ Security guard stopping our car when driving around late at night
  - ▶ Very stupid, but at least aware
- ▶ People being paged and shutting server room door
- ▶ Security guard stopping Stew and drilling him

# My Only Almost Failure

- ▶ Stopped me as I tried to tailgate in
- ▶ Had me wait in the entry area
- ▶ Had half the people running around trying to serve me, while checking out my story
- ▶ Would not let me move anywhere

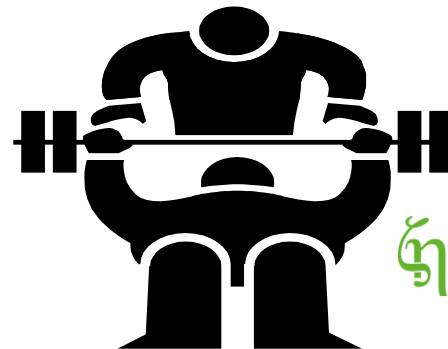
# Yes, You Are The Problem

- ▶ Sadly, I know in 2 minutes whether your security culture sucks
- ▶ Do you know that you will get push back prior to attempting to take an action?
- ▶ Do you start making excuses on why countermeasures will be rejected even before you try?
- ▶ Do your users get support for bypassing security controls?

# Door Monitor or Personal Trainer?



- ▶ A door monitor checks a box
- ▶ A door monitor tries to ensure only the right people get in
- ▶ A door monitor watches people do dumb things, but avoids getting involved
- ▶ A door monitor gets fired when someone ends up hurting themselves
- ▶ A personal trainer helps people do things right
- ▶ A personal trainer keeps the place clean
- ▶ A personal trainer intervenes when he sees people about to hurt themselves



# There is Hope

- ▶ At a CISO event, Security Culture was specifically the top concern for the CISO program committee
- ▶ It shows that technologies are seen as limited
- ▶ There is interest in how to influence the user population
- ▶ I just hope it is more than talk

# Why the Interest in Culture?

- ▶ Culture is an environment of user behavior
- ▶ You can have a Strong or Weak culture
  - ▶ You have a culture; it might as well be a good one
- ▶ It is about users doing things right in the first place
- ▶ When users do things right, there are fewer incidents
- ▶ Fewer incidents result in fewer costs
- ▶ Strong security culture generally implies a more operationally efficient environment as well
- ▶ Smart CISOs don't want to suffer Death by 1,000 Cuts



# Incident Prevention Saves Money

- ▶ Bank services provider
- ▶ Every incident causes the service provider to move resources to investigate incident
- ▶ Just about every attack resulted from a user security failure
  - ▶ Downloaded malware
  - ▶ Open up malicious attachments
  - ▶ No anti-virus software, or outdated definitions
  - ▶ Unpatched operating systems or software
- ▶ Lost time and resources dealing with the incidents

# NSA's Security Culture

- ▶ Everybody wears their badge
- ▶ People generally don't talk about their job, even with people inside NSA
- ▶ There is significant control of electronic and printed media
- ▶ People generally don't take work home with them
- ▶ Mobile devices are locked up outside the work environment
- ▶ People don't quit



# Typical Organization

- ▶ Badges are a nuisance
- ▶ Everyone loves to talk and complain about their work
- ▶ Restaurants are a great place to catch up on work related issues
- ▶ People write down passwords
- ▶ Nobody stops strangers
- ▶ Computers are left open while unattended
- ▶ Suffer Death by 1,000 Cuts

# Should or Must?

- ▶ Is security a Should or a Must to your organization?
- ▶ When something is a Should, it only gets done if everything else is accomplished
- ▶ If something is a Must, it does happen
- ▶ Everyone thinks that they should be secure
- ▶ Few organizations believe they Must be secure

# Department of How



Security in knowledge

# How Security is Perceived



# Typical Security Function

- ▶ Stop people from doing dumb things
- ▶ Put out the fires
- ▶ Reactively deal with organizational mandates
- ▶ Consulted as an afterthought
- ▶ Sometimes there to check a box
  - ▶ Sadly which is frequently the case at “small” financial institutions
- ▶ Makes recommendations that they are forced to justify

# Strong Security Culture

- ▶ Proactively involved in decision making process
- ▶ Consulted proactively on new efforts to ensure security is integrated into the efforts
- ▶ Consultation for ongoing efforts
- ▶ Security has the authority to stop activities as appropriate
- ▶ Employees act securely by default
- ▶ Security is ubiquitous to actions
- ▶ They are “aware”
- ▶ People do not actively attempt to bypass security countermeasures



# Department of How

- ▶ By default, you don't say, No
- ▶ You listen to what the company wants to do, and you figure out how to enable it
- ▶ Security is the enabler as a whole

# It's Not Awareness Programs as a Concept That Suck



# I Really Am Sick of the Awareness “Debate”

- ▶ There is no debate
- ▶ A person writes a poorly thought out article, and it gets published on a slow news day
- ▶ I agree that most programs suck
- ▶ All security countermeasures can be implemented poorly
- ▶ Anti-virus software can be implemented poorly, and nobody says we should give up on it
- ▶ It is an absurd argument that is only good in that it is at least not boring
- ▶ Even the conference theme is “Security in Knowledge”

# Most Awareness Programs Aren't

- ▶ Awareness vs Training
- ▶ Training involves providing a given body of knowledge and ensuring that there is some level of short term comprehension
- ▶ A once a year, 10 minute video is not an awareness program
- ▶ It checks a box, but doesn't create awareness
- ▶ Easy to cheat on the "awareness tests"

# Who's Running Your Program?

- ▶ Most technical people running the program don't want to be in the position
- ▶ Few people have experience or training in social sciences
- ▶ Techies don't understand communications
- ▶ Marcoms don't understand the technology
- ▶ Security people think anyone can run awareness programs, as they don't think it requires a special skill set
- ▶ They don't understand the concept of changing and reinforcing behaviors
- ▶ It's as insulting as a person saying that since they use MS Word that they can maintain a firewall

# Common Knowledge & Common Sense

- ▶ There is no common sense without common knowledge
- ▶ Security programs fail because they assume common knowledge
- ▶ Most stupid user stories originate from stupid security professionals
- ▶ Awareness programs need to create common knowledge so users can exercise common sense
- ▶ Common knowledge creates behavior change, aka an exercise of common sense

# Awareness Creates Behavior Change

- ▶ Awareness programs need to be implemented properly
- ▶ It goes beyond checking a box
- ▶ It requires identifying the information that needs to be highlighted
- ▶ It requires presentation in formats that are likely to be accepted by the user population
  - ▶ Video
  - ▶ Newsletter
  - ▶ Blog
  - ▶ Posters
- ▶ It requires reinforcement
- ▶ Metrics to prove improvement

# There Are Habits of Good Awareness Programs

- ▶ Samantha Manke's research effort
  - ▶ [samantha@securementem.com](mailto:samantha@securementem.com)
- ▶ There are some good programs out there to learn from
- ▶ There are social scientists doing research in related areas
- ▶ Appeal to employee personal interests
- ▶ What they do at home, they will bring back to the office



# How and No

- ▶ The message should be about How to do the job securely
- ▶ Security practices need to be ubiquitous to operations and functions
- ▶ When there is Common Knowledge, behaviors can be monitored
- ▶ Penalties however are a part of the equation
- ▶ Penalties are not for mistakes or accidents
- ▶ Blatant and purposeful violations are treated seriously
- ▶ Security without teeth is useless

# It's More Than Awareness



Security in knowledge

# Embedded Security Infrastructure

- ▶ Is security part of the planning of technology projects?
- ▶ Are there protections built into the network infrastructure?
- ▶ Is the network resilient?
- ▶ Remember a secure network is also an optimized network that is easier and less expensive to maintain
- ▶ Patching is implemented readily and quickly

# Development Processes

- ▶ Is there proactive testing internally developed and acquired software?
- ▶ Are processes like fuzz testing part of the testing cycles?
- ▶ Things like fuzz testing not only lead to better security, but also lead to more reliable and resilient software

# Making Sure Your Program Doesn't Suck



Security in knowledge

# Start at the Top

- ▶ You need to get top level buy in
  - ▶ Remember the case where the person wanted an employee fired for stopping him from tailgating
- ▶ Appeal to their own personal biases
- ▶ Create an awareness program specifically targeting the interests of executives
  - ▶ Personal safety
  - ▶ Protecting their family
  - ▶ Protecting their laptops
  - ▶ Highlighting
- ▶ Start at the top, but you need the rest of this information before you knock on the door

# Figure Out Where You Are

- ▶ Do you have a chance at all?
- ▶ Are you resigned to being a box check?
- ▶ Do you have any authority?
- ▶ Are you consulted on critical projects?
- ▶ Is there a champion who can tell you where you will have the most effect?
- ▶ Are there regulatory or compliance standards that create a mandate?
- ▶ Was there a recent incident?

# Critical Incidents

- ▶ An incident can be a big motivator for change
  - ▶ Sometimes
  - ▶ TJ Maxx? No. Heartland? Yes
- ▶ Citibank
- ▶ Heartland
- ▶ Recon/Optical
- ▶ Google
- ▶ Microsoft



# You're a Risk Management Pro

- ▶ Learn to speak business
- ▶ If you are a Security professional, you are a failure by definition
- ▶ You need to understand what drives your business
- ▶ What words have the most impact?
- ▶ Where can you drive the most improvement?
- ▶ Learn how to save money and talk risk

# How Do You Think About Yourself?

- ▶ Do you personally think of security as a burden?
- ▶ If you are not saving your company money, you really are not doing your company any good
- ▶ Do you think of security having the ability to save money and provide a business benefit
- ▶ You need to believe that you provide a value service to your organization
  - ▶ If you don't think so, then why should your organization?

# Create Metrics

- ▶ Collect statistics to demonstrate every security countermeasure provides a return on investment
- ▶ There is always a metric that should demonstrate a change in behavior
- ▶ Tie a cost to a negative behavior
- ▶ Figure out the return of security investments
- ▶ Tout your ROI at every opportunity
  - ▶ Dan Meacham and his magic iPad
- ▶ Consider Death by 1,000 Cuts

# Make Your Mark

- ▶ Figure out what type of project will have the most effect
- ▶ What can you start to influence, where you are welcome and you can have an impact?
- ▶ Find a visible project
- ▶ Find an easy project
- ▶ Collect Metrics to prove yourself going forward
- ▶ Take credit if a miracle happens anywhere involved with your effort

# Create a Real Awareness Program

- ▶ Strive to change user behaviors
- ▶ Behavior creates actions
- ▶ Consistent actions create culture
- ▶ Ensure reinforcement
- ▶ Strive for environment of ubiquitous security
- ▶ Think automobile safety

# Start at the Top

- ▶ Without high level support, you have no authority
- ▶ Have a plan that addresses executive concerns
- ▶ Demonstrate how you are critical to the success of the organization
- ▶ Once you have authority, you need to implement from the bottom up
- ▶ Only executive management can mandate that security is a Must

# Conclusions



Security in knowledge

# Conclusions

- ▶ You need to accept where you are, or take action
- ▶ Action is not as easy as I make it sound
- ▶ You need a new skill set, which you should have had the whole time
  - ▶ Speaking business
- ▶ This might sound like personal development, but if you don't value yourself, nobody else will
- ▶ Make security a Must



# For More Information

[ira@securementem.com](mailto:ira@securementem.com)

+1-410-544-3435

[www.facebook.com/ira.winkler](http://www.facebook.com/ira.winkler)

@irawinkler

[www.linkedin.com/in/irawinkler](http://www.linkedin.com/in/irawinkler)