

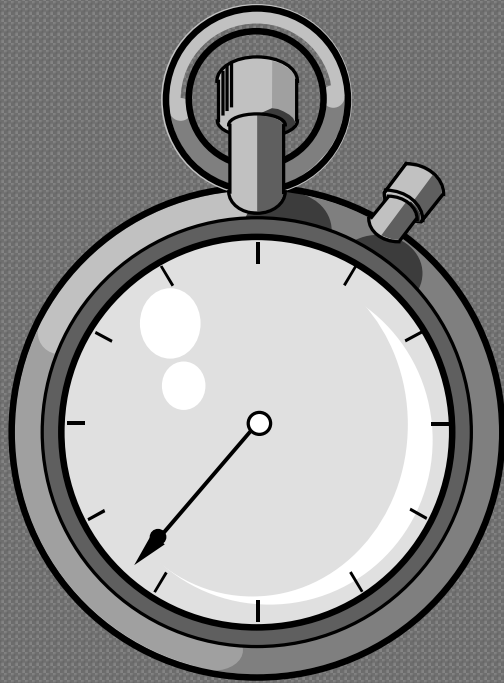
FISSEA 2011

Improved

Customer Service:

A Security Trend

We Really Need



John G. O'Leary, CISSP
O'Leary Management Education

Abstract

To successfully bridge us to the future, there is a trend that needs to gain attention, traction and momentum in our profession. Too often, we security people have served our customers (yes, that's right, those sometimes-pain-in-the-neck users are actually our customers) with something less than courtesy and empathetic understanding. We might have gotten rid of them quickly that time, but we also may have left a bad taste with them for future dealings with any security function. Granted, IT security professionals do not have it easy. We must serve our internal and external customers well while providing appropriate security. But don't even think of slowing down crucial business processes. And isn't the customer always right?

An adversarial relationship with customers makes the bridge to the future rickety and unstable, rife with potholes and deteriorating cables. Good IT security customer service can smooth the roadway and solidify the bridge.

Abstract

In this session, we'll analyze the situation from three perspectives - the service provider (that's the security practitioners) the business customer, and the security training and education professional, emphasizing the need to understand the viewpoints of those we must serve and deal with. We will also analyze complications and particular difficulties inherent in doing anything that provokes as many potential conflicts as IT security. Customers want what they want, they want it now, and they don't want to hear that what they want represents a significant risk to the organization. We have to remember the function of the agency or business, and we want to serve our customers well, but we also understand that the responsibilities of security professionals are to safeguard organizational assets. And sometimes that means protecting users from themselves. In this session we'll provide specific recommendations for actions that will help us educate IT Security to fit established customer service principles and resolve conflicts while continuing to provide appropriate security for our organizations.

Specific Objectives

After this workshop, participants should be more able to:

- Identify critical success factors of customer service
- Understand how IT security services fit customer service principles, and where conflicts may arise
- Incorporate those success factors and principles into effective security training
- Educate security professionals to take ownership of security problems for users and guide them through to resolution that best fits the organization's needs



Format

A. Workshop

Exchange of ideas
Learn from each other
No "canned" solutions

B. Open to questions

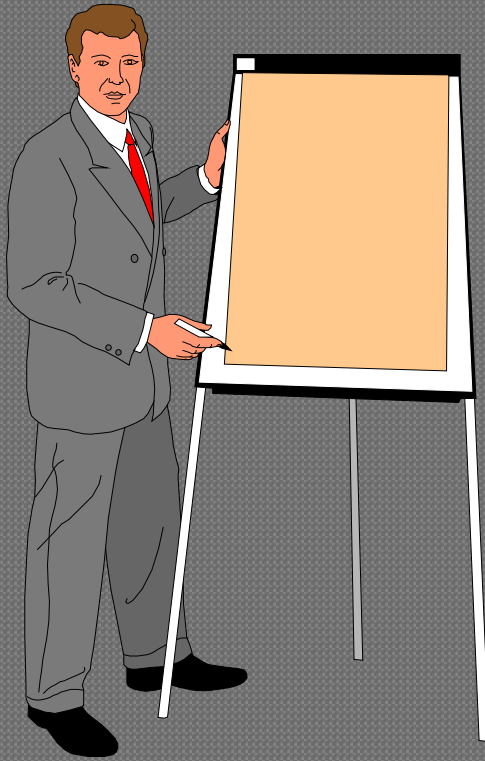
Anytime
Anyone can answer

C. Participation is encouraged

Relevance to your shop
Enhancements to products
Creative solutions



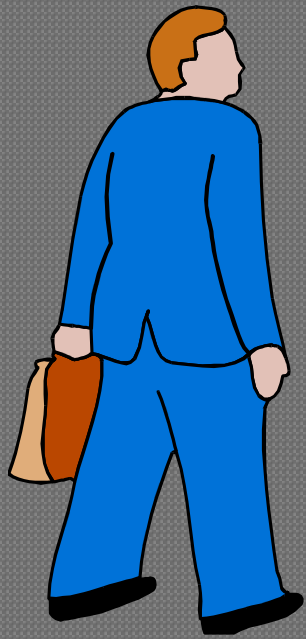
Agenda



**Customer Service
and IT Security**

**Actions for the IT
Security Professional**

Section 1



Customer Service and IT Security



Views of the position

As seen by the ITS Pro

Facilitative
Challenging
Overburdened
Multi-dimensional
Judgment & Tact
Necessary
Path clearing

Dedicated,
Professional



Views of the position



As seen by “others”

Bureaucratic

Dull

Not a real job

Non-technical

Non-management

Paranoid

Roadblocking

Badge, gun &
guard dog





Views of the position

As seen by the ITS Pro

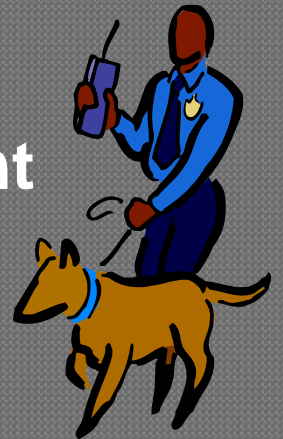
Facilitative
Challenging
Overburdened
Multi-dimensional
Judgment & Tact
Necessary
Path clearing

Dedicated,
Professional

As seen by “others”

Bureaucratic
Dull
Not a real job
Non-technical
Non-management
Paranoid
Roadblocking

Badge, gun &
guard dog



Critical Success Factors for Customer Service

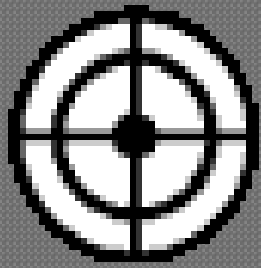
- ❖ From Pat Seybold's book *Customers.com*
 - ❖ Target the right customers
 - ❖ Own the customer's total experience
 - ❖ Streamline business processes that impact the customer
 - ❖ Provide a 360 degree view of the customer relationship



Critical Success Factors for Customer Service

- ❖ From Pat Seybold *Customers.com*
(book)
 - ❖ Let customers help themselves
 - ❖ Help customers do their jobs
 - ❖ Deliver personalized service
 - ❖ Foster community





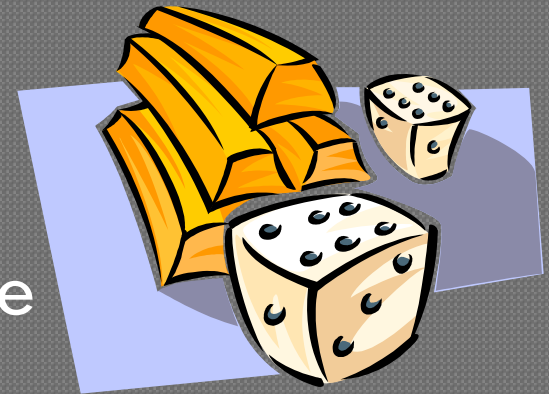
Critical Success Factors for Customer Service

❖ Target the right customers

- ❖ Internal customers

- ❖ Most impact to your enterprise

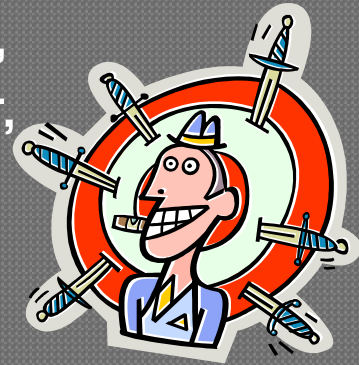
- ❖ Most business payback for your activity



Critical Success Factors for Customer Service

❖ Own the customer's total experience

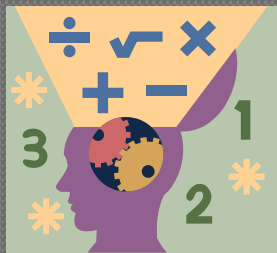
- ❖ The front-line security person is their contact, agent, ombudsman, expert, negotiator, lawyer, designated hitter, State Department, translator, navigator, chauffeur, cop, judge, prosecutor, defense attorney, jury, executioner, champion, superhero, complaint department, etc.
- ❖ That one contact point *is* the security department to the beleaguered user
- ❖ Our training must make sure that user interaction with security is professional and successful



Critical Success Factors for Customer Service

❖ Own the customer's total experience

- ❖ Stay in touch with the customer and with whoever you turned the problem over to for ultimate resolution



- ❖ Put yourself in the middle of the equation
- ❖ Make sure the customer agrees that the solution works and the problem is resolved

Critical Success Factors for Customer Service

❖ Streamline the business processes that impact the customer

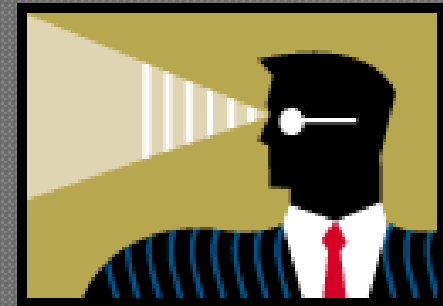
- ❖ Slow = BAD, especially for malware response and handling intrusions
- ❖ Analyze business impact of slow security response (can be enlightening for security people)
- ❖ Teach security how to get the customer involved in revamping the processes



Critical Success Factors for Customer Service

❖ Provide a 360 Degree view of the customer relationship

- ❖ “Here’s what I’m going to do.....”
- ❖ “Here’s where I am in the process.....”
- ❖ “Any other or new information you can give me.....?”
- ❖ Stay in contact



Critical Success Factors for Customer Service

- ❖ **Provide a 360 Degree view
of the customer relationship**



- ❖ This might be hard for an educator to get across to front line security people:
 - ❖ They don't want to maintain contact with complaining users
 - ❖ They have several other things to do, perhaps of higher perceived priority
 - ❖ They might not be the actual solver of the problem
 - ❖ It isn't fun

Critical Success Factors for Customer Service

❖ Let customers help themselves

- ❖ FAQ's
- ❖ Guidelines
- ❖ Self-paced training materials
- ❖ Library of books, articles
- ❖ References to specific websites
- ❖ Implementation examples
- ❖ How-to's
- ❖ But don't force them to dive into the deep end
- ❖ Because it is NOT "intuitively obvious to even the most casual observer"



Complicating Factors

- ◉ From *Your Call is (not that) Important to Us*, Book by Emily Yellin (2009)
 - Customer Service is always among the first targets for cost cutting
 - Live, US-based agent - \$7.50 per call
 - Outsourced offshore - \$2.35 per call
 - Automated response - \$0.32 per call
 - “Reducing cost per contact” and “improving the customer experience” don’t necessarily mesh

Complicating Factors

- It's not enough to just listen to the customers, you've got to actually go do something about what they report and follow up with meaningful contact
- Self-service can save time and money, but can also enhance the perception that the service provider is uncaring or arrogant

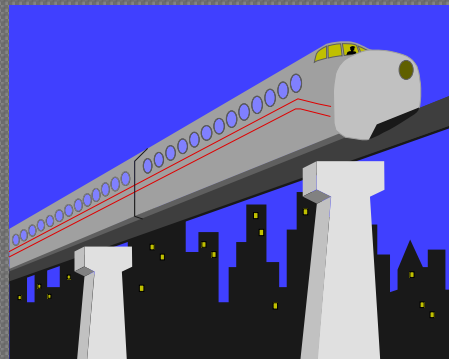
Interrupt-driven Workflow

- ❖ Progressing nicely through one task when:
 - ❖ the phone rings
 - ❖ a co-worker physically shows up at your workspace
 - ❖ your manager calls a meeting
 - ❖ someone's retirement party starts
 - ❖ a fire alarm goes off
 - ❖ the system dies
 - ❖ A small airplane crashes in the parking lot
 - ❖ another snowstorm dumps 2 feet on DC
 - ❖ CNN announces a new computer virus that will probably end life as we know it



Interrupt-driven Workflow

- ❖ Lose your train of thought
- ❖ Takes time to get back to the same status you had reached prior to the interrupt
- ❖ You probably interrupted another task to get back to this one



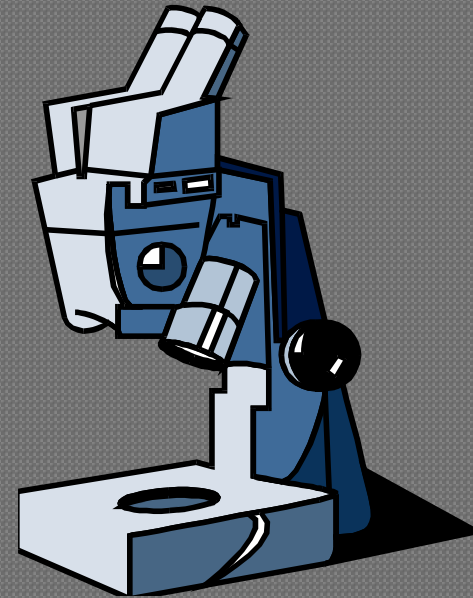
Interrupt-driven Workflow

- ❖ Re-learning
- ❖ Reviewing
- ❖ Re-doing
- ❖ Inefficient
- ❖ Invites errors



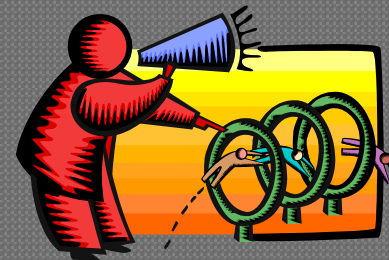
Interrupt-driven Workflow

- ❖ Shifting mind sets
 - ❖ Different contexts
 - ❖ Different rationales
 - ❖ Different valuations on similar items
-
- ❖ Training must comprehend these shifts and differences



Interrupt-driven Workflow

- ❖ Customer Service ramifications
 - ❖ Which customer are you supposed to serve?
 - ❖ Jeopardize fulfilling one commitment to respond to an interrupt
 - ❖ Sometimes make snap decisions and commitments just to get them off the phone
 - ❖ Often try to palm them off on somebody else (“Not my area, talk to Bubba”)



Motivation



- ❖ Hard to maintain
- ❖ Multiple, situational, sometimes seemingly conflicting definitions of “your job”
- ❖ Different perceptions of you when you perform different elements of “your job”
- ❖ Everyone else expects your support when they’re doing “their job”

Motivation



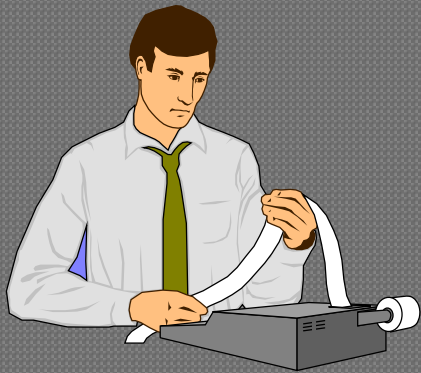
- ❖ Some interesting, challenging tasks
- ❖ Some dull, boring, thankless drudgery
- ❖ Some whining, complaints, and abuse from co-workers
- ❖ Some (rare) thanks from users
- Mixed signals from management

Motivation

❖ Customer Service ramifications

- ❖ Absence of motivation shows
- ❖ People can also hear it in your voice
- ❖ They judge the entire security department based on their interface with you
- ❖ They don't believe what you say
 - ❖ that you're interested
 - ❖ that you'll get back to them
 - ❖ that you'll look further into their problem





Judgment and Balance

- ❖ “You guys just give everybody access to everything, no matter what. No wonder they crash my files. Don’tcha read the papers? WikiLleaks!! This stuff’s valuable”
- ❖ “You guys make a federal case out of it when anyone wants to do anything. Hey, we’re trying to run an agency here and serve our customers.”

Conflicting Priorities: *Security vs. Freedom*



- ❖ Everybody knows we need some kind of control
 - ❖ welllll *most* people
- ❖ Everybody wants his or her own “stuff” to be protected
- ❖ Customer Service for security is perceived to include protecting their stuff



Security vs. Freedom

- ❖ “Stuff” to be protected includes:
 - ❖ programs, files, PC’s, LAN, personnel data, state secrets, WikiLeaks data, contract bids, taxpayer info, reorg plans, research, medical records, interns, political contributions, e-mail about competitors, plans for taking over the world, State-, City- or FEMA-level recovery plans, Sarbox compliance test results, metadata on your word processor files, . . .



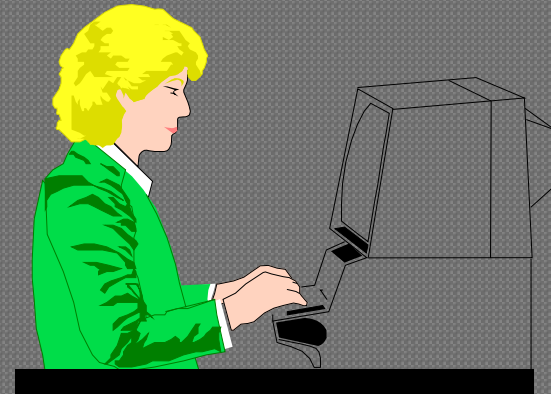
Security vs. Freedom

- ❖ Customer Service ramifications
 - ❖ Not all “stuff” is equally valuable to the firm or agency
 - ❖ Who decides levels of importance?
 - ❖ Some protection mechanisms are cumbersome and complicated
 - ❖ “Owner” of a resource might not want Bubba to have access, but Bubba might need it to do his job
 - ❖ And who “owns” a data warehouse - a massive integrated file storing various kinds of data used by multiple departments



Control vs. Unlimited Access

- ❖ Everybody wants (maybe expects) more powerful tools to augment productivity
- ❖ Everybody wants quick access to the information they need:
 - ❖ to do their jobs faster and more accurately
 - ❖ to respond to real needs today and tomorrow
- ❖ Everybody wants to be trusted



Limiting Danger vs. Productivity

- ❖ Nobody wants to be controlled
 - ❖ It's demeaning
 - ❖ It slows us down
 - ❖ We're not children
 - ❖ We know what we're doing
 - ❖ It stifles our creativity
 - ❖ It conflicts with other pressures we get to make better "widgets" faster



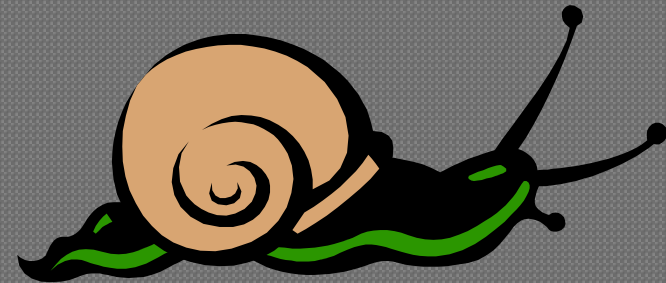
Limiting Danger vs. Productivity

- ❖ People resent the implication

- ❖ We're not so stupid that we'll break our own networks

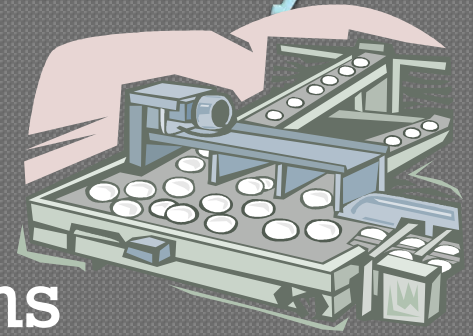
- ❖ We're not crooks . . . or spies

- ❖ We went through rigorous clearance screening before we were hired



- ❖ **Caution!!** Our training for security people must not insult or demean them

Limiting Danger vs. Productivity



❖ Customer Service ramifications

- ❖ Just what kind of widgets does this place make?
- ❖ What's more important - widget making or IT security procedures?
- ❖ “You expect me to still answer 14 queries an hour, but now I have to use a fingerprint reader and remember a PIN and answer random challenges and use this card with a digital certificate on it??”

Security Functions



- ❖ Identification
- ❖ Authentication
- ❖ Authorization
- ❖ Administration
- ❖ Logging
- ❖ Review and follow-up

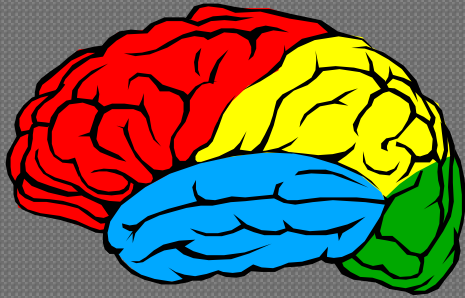
Security Functions

- ❖ Control Design
- ❖ Implementation
- ❖ Evaluation
- ❖ Training
- ❖ Troubleshooting
- ❖ Incident response
- ❖
- ❖ Other duties as assigned



Customer Service Ramifications

Job demands are higher
Service expectations are higher

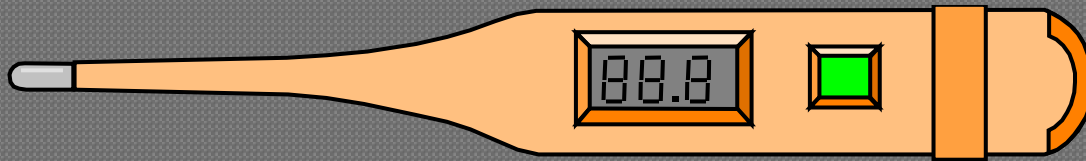


Customer satisfaction
Customer delight

Continuing customer desire
(might not be realistic for security)
Customer Lust??

Customer Service Ramifications

*“Shut up and re-boot” (Dogbert)
is not tech support*



*“No, you can’t do that” might not be
appropriate security customer service*

*“Sure, you can have access to anything
you want” probably doesn’t make the
grade either*

Cost Effectiveness

Reasonable Security

Value of resource(s) being protected

Data

Hardware

Reputation (Brand)

Software

Network

Cost of protection



Amount someone would spend to get at it

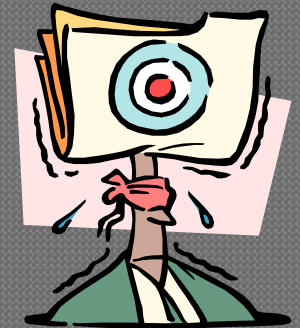


Amount they'd gain or we'd lose if they did

Cost Effective IT

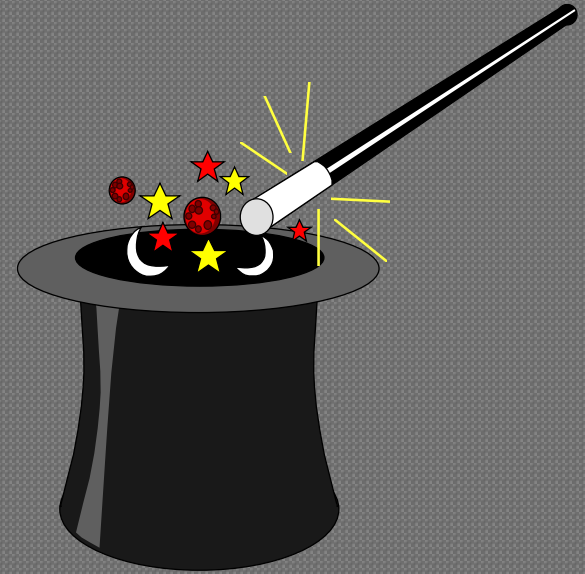
Security Customer Service

- ❖ Good ITS customer service saves money
 - ❖ People get back to work more quickly
 - ❖ Problems are contained and stay small
 - ❖ Fewer wild rumors and panic
 - ❖ Less hiding of problems
 - ❖ Better awareness of security issues and concerns
 - ❖ Not as many “oops’es”
 - ❖ *Stress all these in training security professionals*



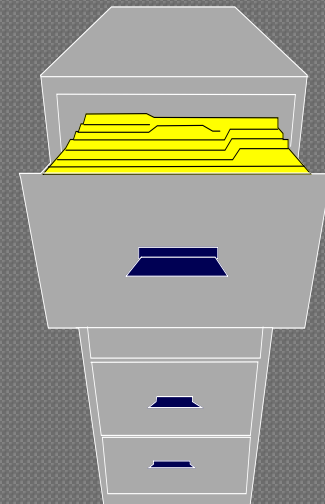
Section 2

Actions for the Security Professional



Think Like a Customer

- ❖ Focus on widget-making
- ❖ Business viewpoint
 - ❖ Security supports the business
 - ❖ Business impacts of
 - ❖ inadequate security
 - ❖ overly rigorous security



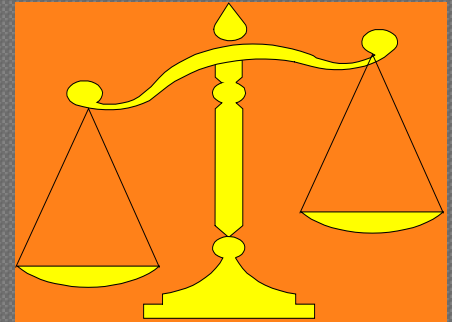
Treat Customers with Respect

- ❖ They're trying to do their jobs
- ❖ Complex environment
- ❖ Impact analysis of change requests
- ❖ Information Security is complicated, and not first in their minds
- ❖ Their (users') expertise is valuable



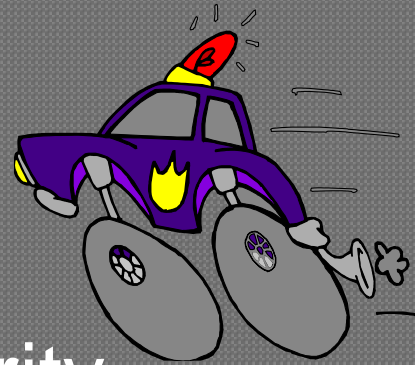
Speak Their Language

- ❖ Security jargon is not standard English
- ❖ Agency-specific terms
- ❖ Profession- or field-specific
- ❖ You build/enhance credibility
- ❖ Summarize in basic business English



Get it Right

- ❖ Speed is important, but accuracy is crucial
- ❖ Reflects, positively or negatively, on all of security
- ❖ Try to coax all relevant details from them before acting



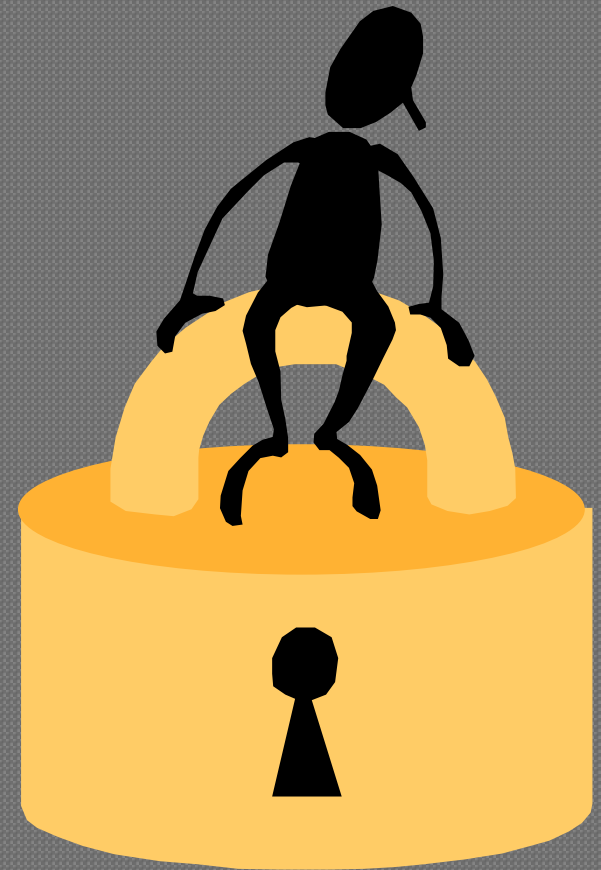
Take Ownership of Problems



- ❖ You might not be the one who'll solve it, but you are the voice they heard first
- ❖ Get as many relevant details as you can think of from the customer
- ❖ Keep the customer apprised of status
- ❖ Check progress on solution
 - ❖ keep after the “solver”
 - ❖ ask co-workers if they've handled similar issues
- ❖ *Emphasize this in training; remember, the security guy wants to finish and move on*

Remember Your Own Job

- ❖ Security doesn't always make people happy
- ❖ Sometimes the best customer service is refusing a request
- ❖ Be ready to explain why they can't all have ROOT or Registry access



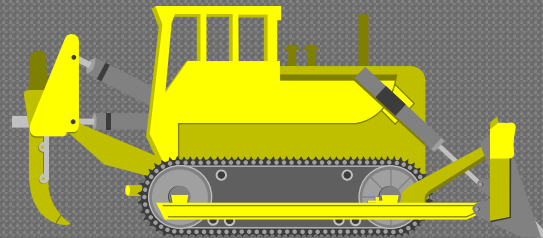
Remember the Function of the Business

- ❖ Security supports the business
 - ❖ Security is critical
 - ❖ Threats are real
 - ❖ Insiders present the most dangerous threat
- ❖ But some people need access to even the most sensitive resources to do their jobs
- ❖ *Training must emphasize that if there is concern about the impact of a security request, seek managerial guidance*

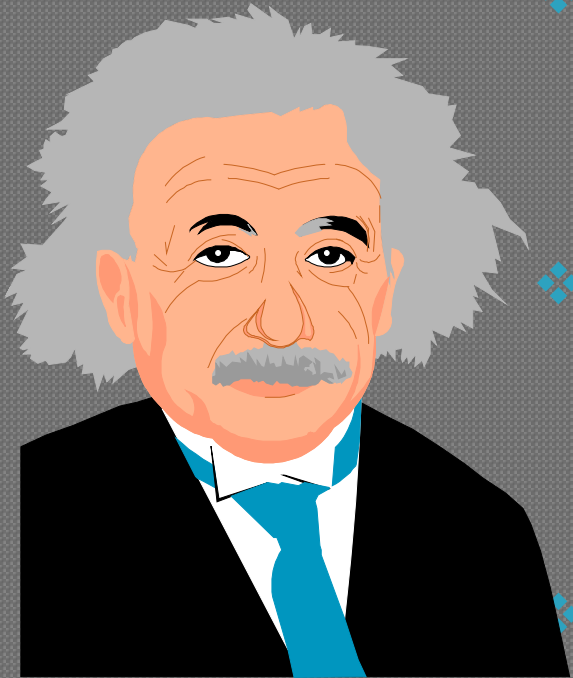


Follow Documented Security Procedures

- ❖ They were developed and put in place:
 - ❖ to fill real needs
 - ❖ to promote consistent application of policies and standards throughout the organization
 - ❖ to provide appropriate service to customers of security administration
 - ❖ to make your tasks easier to perform and to justify
 - ❖ to clarify situations



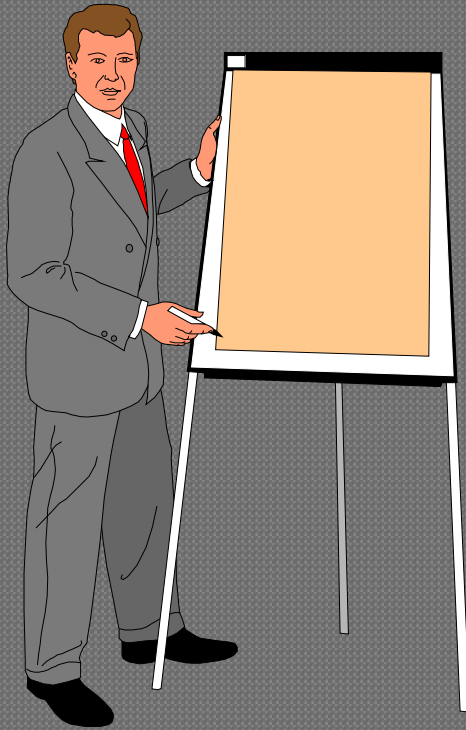
Adapt to the Changing Environment



- ❖ Einstein at Princeton
 - ❖ Teaching Physics
 - ❖ Gave an Exam
- ❖ School official said
“Professor, these questions are the same as last year”
Einstein: “Yes, but this year, the answers are different.”

Summary

We have covered:



**Customer Service and
Information Systems
Security**

**Actions for the Security
Professional**

The end is
here!

