

# Mitigating the Insider Threat (and Other Security Issues)

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team  
Argonne National Laboratory

<http://www.ne.anl.gov/capabilities/vat>

# Argonne National Laboratory

~\$738 million annual budget

1500 acres, 3400 employees, 4400 facility users, 1500 students  
R&D and technical assistance for government & industry



Argonne  
NATIONAL  
LABORATORY

*... for a brighter future*



U.S. Department  
of Energy

UChicago ►  
Argonne<sub>LLC</sub>

A U.S. Department of Energy laboratory  
managed by UChicago Argonne, LLC



# Vulnerability Assessment Team (VAT)



A multi-disciplinary team of physicists, engineers, hackers, & social scientists.

The VAT has done detailed vulnerability assessments on hundreds of different security devices, systems, & programs.

The greatest of faults, I should say, is to be conscious of none.  
-- Thomas Carlyle (1795-1881)

## Sponsors

- DHS
- DoD
- DOS
- IAEA
- Euratom
- DOE/NNSA
- private companies
- intelligence agencies
- public interest organizations



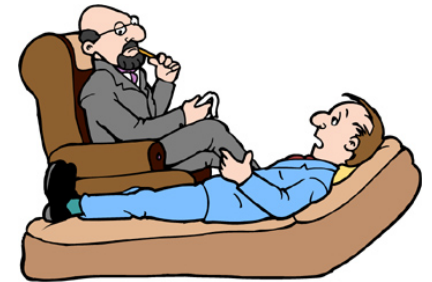
<http://www.youtube.com/watch?v=frBBGJqkz9E>



# **The Human Factor in Security**

# Largely Unstudied Human Factors in Security

- Two-Person Rule
- The psychology of seal inspection
- Security Culture & Security Climate
- Countermeasures for the Insider Threat
- Reducing security guard turnover
- Countermeasures to Perceptual Blindness



**Inspector Jacques Clouseau:** The good cop/bad cop routine is working perfectly.  
**Ponton:** You know, usually two different cops do that.

-- From the movie *The Pink Panther* (2006)



# Security Culture & Climate

- **Security Climate** (informal perceptions) is probably even more important than **Security Culture** (formal policies & procedures)
- In a healthy security culture/climate:
  - Everybody is constantly thinking about security.
  - There are on-the-spot awards for (1) good security practice & (2) proactive/creative thinking and actions.
  - Security ideas, concerns, questions, suggestions, criticisms are welcome from any quarter.
  - Finding vulnerabilities is viewed as good news.



If everybody is thinking alike, then nobody is thinking.  
-- George S. Patton (1885-1945)



# Insider Threat



# 2 Kinds of Insider Threat

Inadvertent vs. Deliberate Compromising of Security



**Schryver's Law:** Sufficiently advanced incompetence is indistinguishable from malice.

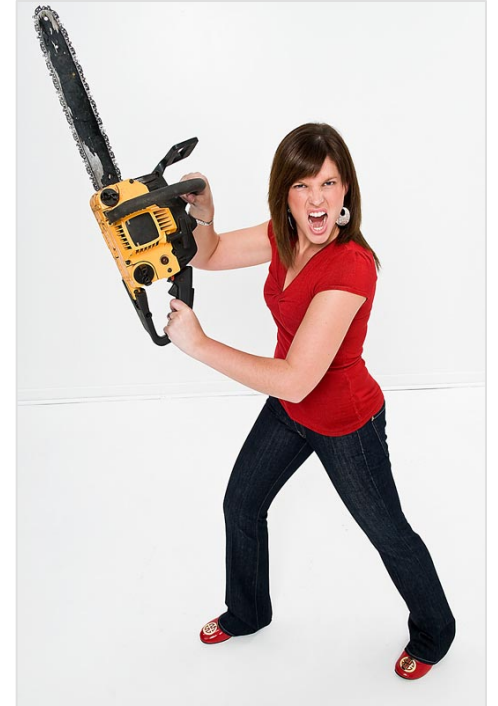


Motivation for Insider Attacks	Countermeasure
greed/financial need	?
<b>revenge</b>	<b>disgruntlement mitigation</b>
terrorism	periodic background checks
ideology, political activism, or radicalism	periodic background checks
coercion/blackmail	periodic background checks
social engineering/seduction	education
<b>narcissism/ego/need to feel important or smart, or to gain recognition</b>	<b>enlist &amp; ego stroke hacker types</b>
<b>desire to prove that a warned about vulnerability or threat is real</b>	<b>take security professionals &amp; their concerns seriously; welcome criticism</b>
desire for excitement	?
mental illness?	periodic background checks?
inadvertent compromise of security via carelessness, error, ignorance, laziness, arrogance	educate, motivate, reward, <del>punish</del>



# Disgruntlement Mitigation

- Employee disgruntlement is a risk factor for workplace violence, sabotage, theft, espionage, and employee turnover.
- While disgruntlement is certainly not the only insider threat motivator, it is an important one.
- Vulnerability Assessors should take a close look at Disgruntlement Mitigation.



For the third goal, I blame the ball. -- Saudi goalkeeper Mohammed Al-Deayea



# Disgruntlement Mitigation Blunders

**Employee perceptions are the only reality!**

- Phony or non-existent grievance, complaint, & conflict resolution processes (Note: if good, they'll be used a lot)
- Phony or non-existent anonymous whistleblower program & anonymous tip hot line
- Non-existent, poor, or retaliatory employee assistance programs

I watch a lot of game shows and I've come to realize that the people with the answers come and go, but the man who asks the questions has a permanent job.

-- Gracie Allen (1895? – 1964)



# Disgruntlement Mitigation Blunders

- No constraints on bully bosses
- No constraints on HR tyranny, evil, & charlatanism
- Institutional arrogance, insincerity, indifference, denial regarding employees
- Emphasis on being “fair” (i.e. consistent) instead of treating everybody *well*
- Not managing expectations (technical personnel often have very high expectations)



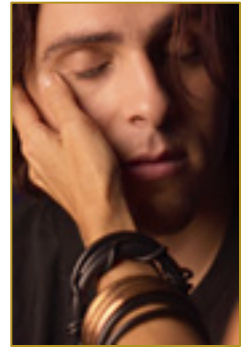
The human-resources trade long ago proved itself, at best, a necessary evil—and at worst, a dark bureaucratic force that blindly enforces nonsensical rules, resists creativity, and impedes constructive change.

-- Keith H. Hammonds



# Disgruntlement Mitigation Blunders

- Ignoring the 80% rule about the importance of listening, empathizing, validating, & permitting venting
- Not recognizing that whatever an employee or contactor says is upsetting him/her probably isn't the real issue



Sincerity is everything. If you can fake that, you've got it made.  
-- George Burns (1885-1996)



# Disgruntlement Mitigation Blunders

- Not being prepared for domestic violence coming into the workplace



- Not watching for the usual precursors to insider attacks due to disgruntlement, especially sudden changes in:

- performance
- use of drugs or alcohol
- signs of aggression or hostility
- being late for work or a no show
- not getting along with co-workers



Always go to other people's funerals. Otherwise, they might not come to yours. -- Yogi Berra



# Poor Insider Threat Practice

- Not testing if employees can be bribed
- Thinking that only employees are insiders
- Thinking that low-level employees are not a threat
- Not watching employees/contractors who think they may soon be gone
- Not treating laid off or fired personnel well
- Not publicly prosecuting insider offenders



In my opinion, we don't devote nearly enough scientific research to finding a cure for jerks.  
-- Bill Watterson (Calvin & Hobbes)

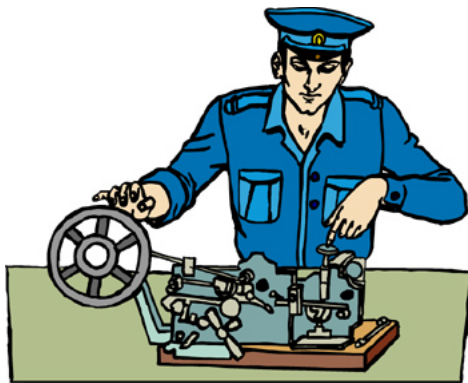




# Poor Insider Threat Practice



- Not thinking about which employees/contractors/positions are most likely to be targeted by adversaries for compromise
- Not having greeters or posters with eyes
- The perp walk
- Polygraphs



It has been pointed out that many states require more formal training to become a licensed barber than to become a licensed polygraph examiner.



# Polygraphs = Snake Oil

National Academy of Sciences \$860,000 study:  
“The Polygraph and Lie Detection” (October 2002)  
<http://www.nap.edu/books/0309084369/html/>



## Some Conclusions:

“Polygraph test accuracy may be degraded by countermeasures...”

“...overconfidence in the polygraph—a belief in its accuracy that goes beyond what is justified by the evidence—...presents a danger to national security...”

“Its accuracy in distinguishing actual or potential security violators from innocent test takers is insufficient to justify reliance on its use in employee security screening...”

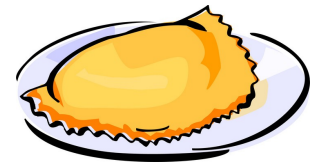


# Security Guard Turnover

- ◆ typical for contract guards: 40 - 400% per year
- ◆ a serious economic/productivity issue
- ◆ a serious insider threat issue

Harry Solomon: I didn't have enough experience to sell hot dogs, so they made me a security guard.

-- *Third Rock from the Sun*



# Countermeasures for Guard Turnover

- ◆ realistic job interviews
- ◆ personality tests
- ◆ new employee training
- ◆ better supervisors
- ◆ other tools of i/o psychology



Q: What did you get on your SAT test?

A: Nail polish.

-- Interviewer and response from Jennifer Lopez



# Poor Security for Urine Drug Tests

It's easy to tamper with urine test kits.

Most urine testing programs (government, companies, athletes) have very poor security protocols.

Emphasis has been on false negatives, but false positives are equally troubling.

Serious implications for safety, courts, public welfare, national security, fairness, careers, livelihood, reputations, sports.

*Journal of Drug Issues* **39**, 1015-1028 (2009)



# Compliance-Based Security

# Compliance-Based Security

## Old Paradigm:

- Compliance gets us good Security.

## New Paradigm:

- Compliance—though it may be necessary and can be of value—often causes distractions, gets in the way of good Security, or can be incompatible with it.



Advice to children crossing the street: Damn the lights!  
Watch the cars. The lights ain't never killed nobody.


-- Moms Mabley (1894-1975)



# Rule of Thumb

**30% Maxim:** In any large organization, at least 30% of the security rules, policies, and procedures are pointless, absurd, ineffective, or actually undermine security (by wasting energy and resources, by creating cynicism about security, and/or by driving behaviors that were not anticipated).

This includes Security Theater, foolish “one-size-fits-all” policies, rules that only the good guys follow, punitive rules, and policies that make abstract sense to bureaucrats and committees who lack knowledge of the real-world issues.



I was taking a bath in a Leningrad hotel when the floor concierge yelled that she had a cable for me. “Put it under the door,” I cried. “I can’t,” she shouted. “It’s on a tray!” -- Anthony Burgess



# Security Training

# Training & Auditing

## Old Paradigm:

- Training for security personnel is mostly about their understanding security rules, policies, and procedures.
- Performance for security personnel is measured by how well they adhere to security rules, policies, and procedures.

## New Paradigm:

- Training for security personnel emphasizes creative “What if?” exercises (mental and field practice).
- Performance for security personnel is measured by how resourcefully they deal with day-to-day real-world security issues, and with “What if?” exercises.



In preparing for battle, I have always found that plans are useless, but planning is indispensable.  
-- Dwight D. Eisenhower (1890-1969)



# Security Awareness Training

**Definition--Security Awareness Training (n):**  
Presentations that convince employees who once vaguely believed that security was a good idea that they were sadly mistaken.

**Definition—Counter-Intelligence Program (n):**  
Security Awareness Training so awful that it insults everyone's intelligence.



**Game Show Host:** Watling Street, which now forms part of the A5, was built by which ancient civilization?

**Contestant:** Apes?



# Security Awareness Training

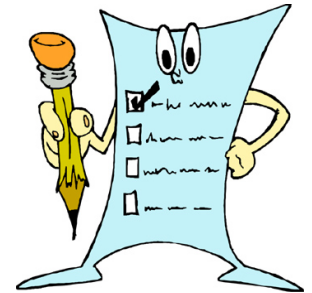


- We train dogs. We educate, remind, encourage, & motivate people.
- Tailor to the audience
- Promote, sell, & motivate good security by employees, contractors, and vendors. Don't threaten or intimidate!
- Use examples. Show people how to do things, don't tell them what not to do.
- Avoid the negative terms: Don't! Never! No!
- What's in it for me?



# Security Awareness Training

- Make connections to personal security: home computer security, burglary, identity theft, etc.
- Refer to news stories about security breaches in other organizations and the consequences.
- Have metrics for effectiveness of the training (and the security)
- No dumb trivia questions on the quiz!
- Use people-oriented instructors, not bureaucrats, technocrats, burnouts, zombies, or deadwood.



Shouldn't the Air and Space Museum be empty?  
-- Dennis Miller



# Security Awareness Training

- Be entertaining, vivid, & positive, NOT threatening, boring, patronizing, or full of organizational charts, camera-challenged executives, references to CFRs, or self-serving fluff about HR, the security organization or the training department.
- Less is more. Stick with the most important risks.
- Security Awareness posters should offer useful security tips & solutions, not platitudes, mindlessness, insults, & threats.



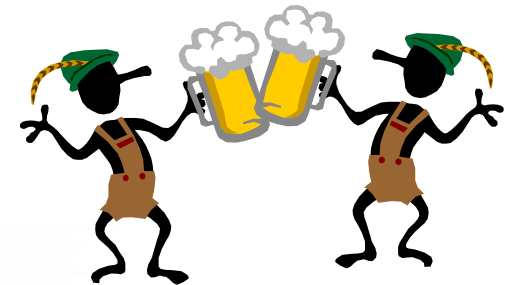
That cartoon character, Asterix. I wonder how rude his real name is.

-- Jimmy Carr



# Security Awareness Training

- Teach about social engineering and that adversaries often conduct espionage or intelligence via:
  - industry “surveys”
  - bogus headhunters & job interviews
  - phony trade journal interviews
  - hanging out at nearby restaurants/bars
  - public affairs & the graphics department
  - recruiting crafts people & custodians
  - impersonation
  - targeting based on ethnicity, religion, or foreign nationality



# Perceptual Blindness



[http://wn.com/Transport\\_for\\_London\\_\\_Whodunnit](http://wn.com/Transport_for_London__Whodunnit)



# 50 Years of Cognitive Psychology Research

- People are remarkably poor observers.
- They don't realize how bad they are.
- “Perceptual Blindness” = “Inattentional Blindness”:  
the phenomena of not being able to perceive things that are in plain sight, especially if you're focused on a particular visual task.
- “Change Blindness” (a kind of Perceptual Blindness):  
observers often fail to notice changes—including blatant ones—even when the changes are expected.



As a rule, we perceive what we expect to perceive.  
The unexpected is usually not perceived at all.  
-- Peter Drucker (1909-2005)

# Consequences for Security

There are serious implications for security guards & safeguards inspectors, especially those who:

- ✓ check security badges
- ✓ watch video monitors
- ✓ make daily rounds
- ✓ inspect seals
- ✓ guard gates
- ✓ operate safeguards equipment
- ✓ etc.



If you don't see it often, you often don't see it.  
-- Jeremy Wolfe



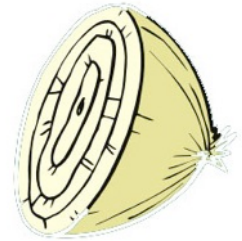
# Countermeasures for Perceptual Blindness

- ◆ plan for it in the security plan
- ◆ educate security guards about it & demonstrate it
- ◆ do mental preparation: lots of rehearsing of “What if?”
- ◆ arrange for strange events during exercises
- ◆ get training from magicians about distraction, misdirection, & sleight-of-hand; **Note: training in observational skills might actually make things worse!**
- ◆ use technology to cover for human perceptual weaknesses
- ◆ Choose one or more security guards to be the generalist(s) to examine the overall scene without specific assigned detailed observational responsibilities. They should look for the unexpected and the rare.



# Other Warnings & Issues

# Warning: Multiple Layers of Security ("Security in Depth")



- ❖ Increases cost & complexity
- ❖ Multiple layers of bad security do not equal good security.
- ❖ Often mindlessly applied: the layers are not automatically backups for each other, or may even interfere with each other
- ❖ Leads to complacency
- ❖ Tends to be a cop-out to avoid improving any 1 layer or thinking critically about security
- ❖ **How many sieves do you have to stack before the water won't leak through?**



# Facts About Access Control Devices

For most Access Control systems (including biometrics), it's easy to:



- clone the signature of an authorized person
- do a man-in-the-middle (MM) attack
- access the database or password
- “counterfeit” the device
- install a backdoor



Harry Potter this. Harry Potter that. I'd never even heard of Harry Potter until that book came out!

-- Caller, Radio 5 Live (UK)

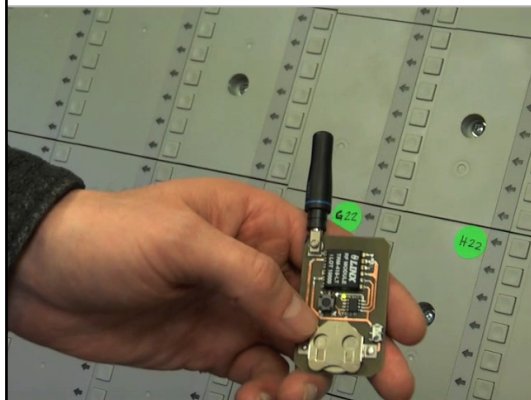


# Backdoor, MM, or Counterfeit Attacks

**The importance of a cradle-to-grave, secure chain of custody:**

Most security devices and systems can be compromised in 15 seconds (at the factory or vendor, on the loading dock, in transit, in the receiving department, or after being installed).

Most “security” devices have little built-in security or ability to detect intrusion/tampering.



Sometimes security implementations look fool proof.  
And by that I mean proof that fools exist.

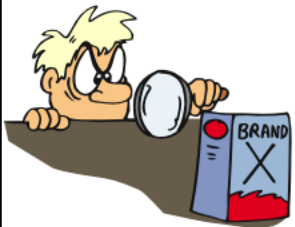
-- Dan Philpott



# Access Control (AC)

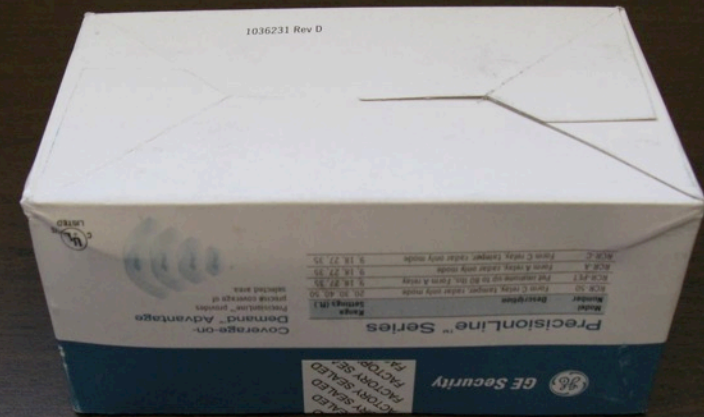
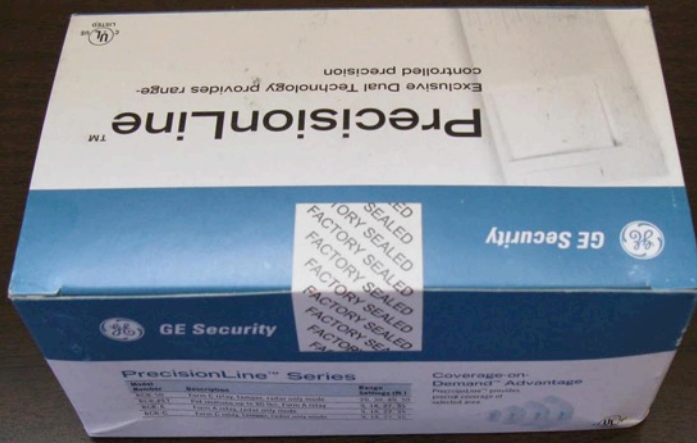
Question: Is that really your AC device, or is it a counterfeit or a tampered version?  
(...perhaps one that lets anybody in, with occasional random false rejects to look realistic.)

- Check at random, unpredictable times with random, unpredictable people that the unauthorized are rejected.



I was the kid next door's imaginary friend.  
-- Emo Philips

# Security of Security Products



# Confusing Inventory & Security

## Inventory

- Counting and locating stuff
- No nefarious adversary
- May detect innocent errors by insiders, but not surreptitious attacks by insiders or outsiders.



## Security

- Meant to counter nefarious adversaries (insiders and outsiders)
- Watch out for mission creep: inventory systems that come to be viewed as security systems!



# Examples of confusing Inventory & Security

- rf transponders (RFIDs)



- contact memory buttons



- prox cards



- GPS



- Nuclear MC&A

Usually easy to:

- \* lift
- \* counterfeit
- \* tamper with the reader
- \* spoof the reader from a distance

Very easy to spoof,  
not just jam!

# Problem: Lack of Research-Based Security Practice



A free, online,  
peer-reviewed R&D journal

<http://jps.anl.gov>

The Journal of Physical Security

There are three kinds of men. The one that learns by reading. The few who learn by observation. The rest of them have to pee on the electric fence for themselves.

-- Will Rogers (1879 - 1935)



# For More Information...



<http://www.ne.anl.gov/capabilities/vat>

200+ related papers, reports, and presentations are available from

Roger Johnston  
Vulnerability Assessment Team  
Argonne National Laboratory  
<http://www.anl.gov>

(includes Security Maxims)



If you look for truth, you may find comfort in the end; if you look for comfort you will get neither truth nor comfort...only soft soap and wishful thinking to begin, and in the end, despair. -- C.S. Lewis (1898-1963)



Supplemental material not part of the presentation...



# illuminating Books Relevant to the Human Factor in Security

(all fun reads)

G Marcus, ***Kluge: The Haphazard Construction of the Human Mind*** (2008)

C Travis & E Aronson, ***Mistakes Were Made (But Not by Me)*** (2007)

BL Katcher & A Snyder, ***30 Reasons Employees Hate Their Managers***  
(2007)

RL Ackoff & S Rovin, ***Beating the System: Using Creativity to Outsmart Bureaucracies*** (2005)

K Mitnick & WL Simon, ***The Art of Intrusion*** (2005).

RJ Sternberg (Editor), ***Why Smart People Can Be So Stupid*** (2002)





# What's Wrong with This Picture?

"While serious, the incident in question was the result of human error, not a failure of security systems. We have a robust system in place to report and investigate potential violations. In my opinion, this is a circumstance where those systems worked well."

-- Statement from a high-level government official  
after a serious security incident



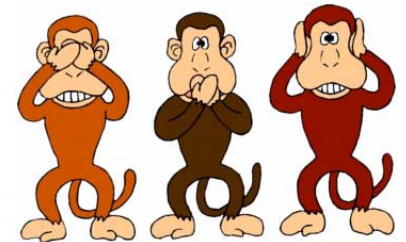
# Cognitive Dissonance

# Blunder: No Countermeasures for Cognitive Dissonance

## Cognitive Dissonance dangers:

- ◆ self-justification  
(self-serving rationalization & excuse making)
- ◆ paralysis/stagnation  
(not addressing problems)
- ◆ confirmation bias / motivated reasoning  
(interpret data only in ways that make us feel good)

I don't want any yes-men around me. I want everyone to tell me the truth—even if it costs him his job.  
-- Samuel Goldwyn (1879-1974)



# Countermeasures for Cognitive Dissonance

- ◆ appreciate how hard security really is
- ◆ avoid binary thinking
- ◆ watch out for over-confidence
- ◆ welcome input, questions, criticism, dissent, & controversy; don't shoot the messenger
- ◆ be your own devil's advocate and/or appoint one
- ◆ avoid groupthink
- ◆ be uncomfortable/scared
- ◆ embrace appropriate humor

~~01~~



# Why High-Tech Devices & Systems Are Usually Vulnerable To Simple Attacks

- Many more legs to attack.
- Users don't understand the device.
- The "Titanic Effect": high-tech arrogance.
- Still must be physically coupled to the real world.
- Still depend on the loyalty & effectiveness of user's personnel.
- The increased standoff distance decreases the user's attention to detail.
- The high-tech features often fail to address the critical vulnerability issues.
- Developers & users have the wrong expertise and focus on the wrong issues.



I cannot imagine any condition which would cause this ship to founder, nor conceive of any vital disaster happening to this vessel.

-- E.J. Smith, Captain of the Titanic



# Security Guards

*But who is to guard the guards themselves?*  
-- Juvenal (55 – 127 AD)



Plato (427 – 347 BC) proposed this answer:  
*They will guard themselves against themselves. We must tell the guardians a noble lie. The noble lie will inform them that they are better than those they serve and it is therefore their responsibility to guard and protect those lesser than themselves. We will instill in them a distaste for power or privilege; they will rule because they believe it right, not because they desire it.*



# Who Does Security

Harry Solomon (reading the paper): Here's a job that I can do: "Police are Seeking Third Gunman." Tomorrow, I'm gonna march over to the police station and show them that I'm the man they're looking for. -- *Third Rock from the Sun*

## Old Paradigm:

- Trained security personnel provide security.
- Security managers and security consultants are the main experts on Security.
- Regular employees, contractors, & visitors are the enemies of good security.

## New Paradigm:

- (The Insider Threat notwithstanding) regular employees, contractors, visitors, local authorities, and neighbors provide security, with help from trained security personnel.
- Frontline security personnel and regular employees are the main experts on local Security.



# Process, Technology, & People

## Old Paradigm:

- Process and Technology (in that order) are our main tools for providing security.

## New Paradigm:

- People and Process (in that order) are our main tools (though Technology can help).



Warning label on a CD player:  
“Do not use the UltraDisc 2000 as a projectile in a catapult.”





# Definition

**Security Theater:** sham or ceremonial security;  
Measures that ostensibly protect people or assets but  
that actually do little or nothing to counter adversaries.

## Actual Courtroom Testimony:

Witness (a Physician): He was probably going to lose the leg, but at least maybe we could get lucky and save the toes.



# Security Theater

1. Best way to spot it is with an effective thorough VA.

2. Next best is to look for the characteristic attributes:

- Sense of urgency
- A very difficult security problem
- Involves fad and/or pet technology
- Questions, concerns, & dissent are not welcome or tolerated
- The magic security device, measure, or program has lots of “feel good” aspects to it**
- Strong emotion, over confidence, arrogance, ego, and/or pride related to the security
- Conflicts of interest
- No well-defined adversary
- No well-defined use protocol
- No effective VAs; no devil’s advocate
- The technical people involved are mostly engineers
- Intense desire to “save the world” leads to wishful thinking
- People who know little about security or the technology are in charge



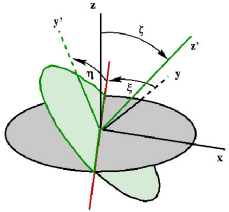
# Examples of Compliance Harming Security

- All the paperwork, bureaucracy, data recording, & preparation for audits causes distractions and wastes resources.
- Creates wrong mindset: Security = Busy Work; Mindless rule-following; the Brass are responsible for security strategies & tactics, not me...
- An over-emphasis on fences (4.5 – 15 sec delay) and entry points leads to bad security.
- Granting access to numerous auditors, overseers, micro-managers, and checkers of the checkers increases the insider threat.
- **Security clearances require self-reporting of professional counseling, thus discouraging it.**
- The rules require overly predictable guard patrols & shift changes.
- Little room for flexibility, individual initiative, hunches, resourcefulness, observational skills, people skills.



# **Vulnerability Assessment**

# Adversarial Vulnerability Assessments



- Perform a mental coordinate transformation and pretend to be the bad guys. (This is much harder than you might think.)

It is sometimes expedient to forget who we are. -- Publilius Syrus (~42 BC)



- Be much more creative than the adversaries. They need only stumble upon 1 vulnerability, the good guys have to worry about all of them.

It's really kinda cool to just be really creative and create something really cool. -- Britney Spears



# Adversarial Vulnerability Assessments



- Don't let the good guys & the existing security infrastructure and tactics define the problem.

Evil will always triumph because good is dumb.  
-- Rick Moranis, as Dark Helmet in *Spaceballs* (1987)



- Gleefully look for trouble, rather than seeking to reassure yourself that everything is fine.

On a laser printer cartridge: “Warning. Do not eat toner.”



**We need to be more like expert fault finders.  
They find problems because they want to find  
problems, and because they are skeptical:**

- bad guys
- therapists
- movie critics
- computer hackers
- scientific peer reviewers
- mothers-in-law

I told my psychiatrist that everyone hates me. He said I was being ridiculous-- everyone hasn't met me yet.

-- Rodney Dangerfield (1921-1997)



“Two mothers-in-law.”

-- Lord John Russell (1832-1900), on being asked what he would consider proper punishment for bigamy.



# Vulnerability Assessment (VA) Blunders

These assumptions are wrong:

- There are a small number of vulnerabilities.
- Most or all can be found & eliminated.
- Vulnerabilities are bad news.
- A VA should ideally find zero vulnerabilities.



He that wrestles with us strengthens our skill.  
Our antagonist is our helper.

-- Edmund Burke (1729-1797)





# Vulnerability Assessment (VA) Blunders

- Confusing Vulnerability Assessments with Threat Assessments, Risk Management, Security Testing, & Security Auditing.
- Sham Rigor & the Fallacy of Precision
- Relying solely on tools that aren't very good at finding vulnerabilities (security surveys, security audits, CARVER, Delphi Method, DBT, Fault Tree Analysis, etc.)
- Letting attack methods define the vulnerabilities, not the other way around
- Not using creative people with a hacker mentality who want to find problems and suggest solutions.



# Vulnerability Assessment (VA) Blunders

- Modular VAs or other artificial constraints on the VA
- Using only security experts
- Not thinking like the bad guys
- Thinking the good guys get to define the problem
- shooting the messengers

My definition of an expert in any field is a person who knows enough about what's really going on to be scared.

-- P.J. Plauger



## Blunder: Not Understanding What a VA is For

The purpose of a vulnerability assessment is to improve security, not to:

- Pass a test
- Generate metrics
- Justify the status quo
- Praise or accuse anybody
- Check against some standard
- Claim there are no vulnerabilities
- Rationalize the research & development
- Endorse a security product or program, or Certify it as “good” or “ready for use”
- Apply a mindless, bureaucratic stamp of approval

