Talk for the 58th Annual ASIS Meeting
Philadelphia, PA, September 10-13, 2012

Under-Utilized Methods for Mitigating the Insider Threat

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team
Argonne National Laboratory

630-252-6168 rogerj@anl.gov
http://www.ne.anl.gov/capabilities/vat

Argonne National Laboratory

~$738 million annual budget
1500 acres, 3400 employees, 4400 facility users, 1100 students
R&D and technical assistance for government & industry

Vulnerability Assessment Team (VAT)

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

The VAT has done vulnerability assessments on over 1000 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

Check us out on YouTube: keywords = argonne break into

Human Factors in Security

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

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.
  - No scapegoating!
  - Finding vulnerabilities is viewed as good news.

When it comes to security, the silicon is fine. It's the carbon we have to deal with.
-- Mark Rasch

Examples of Largely Unstudied Human Factors in Security

- Two-Person Rule

- Insider Threat Mitigation
- Security Culture & Security Climate

- Identifying Characteristics of Security Theater
- Countermeasures to Perceptual Blindness, Misdirection, & Sleight-of-Hand

- Reducing security guard turnover (~40% to 400% per year)
- Human factors in nuclear safeguards inspections
- Cognitive psychology of seal and cargo inspection

Illuminating Books Relevant to the Human Factor in Security

(all fun reads)

Ken Perenyi, **Caveat Emptor: The Secrete Life of an American Art Forger** (2012)

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

CTravis & 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)*

Insider Threat

Motivation for Insider Attacks	Countermeasures
greed/financial need	periodic background checks, bribery anti-sting operations
revenge	disgruntlement mitigation
terrorism	periodic background checks
ideology, political activism, or radicalism	periodic background checks
coercion/blackmail	periodic background checks
social engineering/seduction	security awareness training
narcissism/ego/need to feel important or smart, or to gain recognition	enlist & stroke egos of hacker types
desire to prove that a warned about vulnerability or threat is real (self-identified Cassandras)	take security professionals & their concerns seriously; welcome criticism
desire for excitement	make jobs interesting?
mental illness?	periodic background checks?
inadvertent compromise of security due to carelessness, error, ignorance, laziness, or arrogance	educate, motivate, reward, ~~punish~~, analyze attitudes to predict problems

2 Kinds of Insider Threat

Inadvertent vs. Deliberate Compromising of Security

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

Insider Threat – Inadvertent

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.

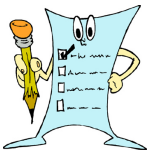
Definition—**Counter-Intelligence Program** (n):
Security Awareness Training so awful that it insults everyone's intelligence.

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. Talk about the carrots, not the sticks.
- Avoid the negative terms: Don't! Never! No!
- What's in it for me?

Security Awareness Training

- Make connections to personal security: home computer travel 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 talking-head executives, references to CFRs, or self-serving fluff about HR, the security organ-ization 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

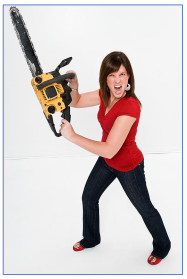
Security Awareness Training

- Teach about social engineering and that adversaries often conduct espionage or intelligence via:

  - industry “surveys”
  - social networking sites
  - 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

Insider Threat – Deliberate

Good Insider Threat Practice



- Publicly prosecute insider offenders
- Avoid the perp walk!
- Pay attention to morale
- Watch employees/contractors/vendors who think they may soon be gone
- Treat retired, laid off, and fired personnel well
- Consider using bribery anti-stings

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

Countermeasure: Bribery Anti-Stings

- Occasionally test if randomly chosen employees, contractors, vendors, consultants, etc. can be bribed.
- Let the person keep the money if he/she rejects and reports the bribe. Then widely praise and publicize him/her as a hero.
- Allow at least 2 days for the bribe to be rejected and reported.
- There must be clear, frequently publicized rules about the need to report a bribe and exactly how to do it.
- There are legal entrapment issues but the goal is not to fire or arrest a lot of people (as in a sting operation), but rather to undercut the effectiveness of future bribe attempts by making people think it might be a test.

Good Insider Threat Practice

- Periodic background checks

Question on a job application form: Do you support the overthrow of the government by force, subversion, or violence? Answer from one applicant: Violence.

- Periodically google & check insiders' public social media
- Use role-based access control & actively updating it
- Identify/Recruit/Ego-Stroke hacker types and Cassandras within the organization
- Watch out for poor drug testing security

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)

Good Insider Threat Practice

- Think about which employees/contractors/positions are most likely to be targeted by adversaries for compromise, or have the most potentially risky insider access.
- Security professionals need to be the "friendly cop on the beat" & pick up scuttlebutt
- Do thorough exit interviews, and interviews with people who turn down job offers
- Avoid special treatment for VIPs
- Avoid 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…"

Good Insider Threat Practice

- Avoid: Witch Hunts, Spying, Secret Police, Invasions of Privacy, Violation of Civil Liberties. (Mind Nietzsche's Admonition: In fighting monsters, be careful not to become one yourself!)

- Do effective disgruntlement mitigation. Don't assume managers or HR will automatically deal with it, or that it's not a security issue.

A mule will labor ten years willingly and patiently for the privilege of kicking you once.
-- William Faulkner (1897-1962)

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 whistle blower program & anonymous tip hot line
- Non-existent, poor, or retaliatory employee assistance programs

Harry Potter this. Harry Potter that. I'd never even heard of Harry Potter until that book came out!
-- Caller, Radio 5 Live (UK)

Disgruntlement Mitigation Blunders

- No identification/constraints on bully bosses
- No constraints on HR tyranny, evil, & charlatanism
- Institutional arrogance, insincerity, indifference, denial regarding employees
- Emphasis on being "fair" 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

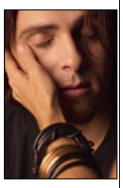
- Not being prepared for domestic violence coming into the workplace

- Not watching for the usual precursors to insider attacks due to disgruntlement, especially <u>sudden</u> <u>changes</u> in:
  - hygiene
  - performance
  - rule compliance
  - 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

Disgruntlement Mitigation Blunders

- Not recognizing that whatever an employee or contactor says is upsetting him/her probably isn't the real issue.
- Ignoring the 80% rule about the importance of listening, empathizing, validating, & permitting venting. (You don't have to agree with the disgruntled individual.)
- Not trying to fix the problem; not offering a consolation prize if you can't.



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

Countermeasures from Psychology

Under-Utilized Countermeasures From Psychology

- Have people sign a loyalty, ethics, or honesty statement at the top of a form before they answer questions or provide information, not at the bottom.

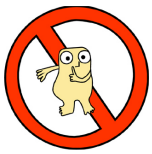
- Use building/facility greeters & posters with eyes.

I consider myself to be a pretty good judge of people. That's why I don't like any of them.
-- Roseanne Barr

Under-Utilized Countermeasures From Psychology

- Bright lighting in sensitive areas.

- Visually open, acoustically closed interior architecture

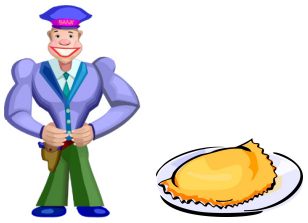


- Proactive techniques from i/o psychology for dealing with guard turnover

Security Officer 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

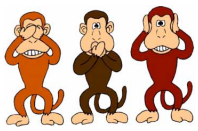
- realistic job interviews
- personality tests
- new employee training
- better supervisors
- other tools of i/o psychology

Q: What did you get on your SAT test?
A: Nail polish.
-- Interviewer and response from Jennifer Lopez

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)



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; avoid groupthink
- be your own devil's advocate and/or appoint one
- constantly ask yourself: "What am I being a knucklehead about? How is my security going to fail?"

- be uncomfortable/scared
- embrace appropriate humor

Security Theater

&

Compliance-Based Security

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

Rule of Thumb

30% Maxim: In any large organization, <u>at least</u> 30% of the security rules, policies, and procedures will be dumb or counter productive.

This includes Security Theater, foolish "one-size-fits-all" policies, rules that only the good guys follow, punitive practices, and policies that make abstract sense to bureaucrats, committees, and higher-ups who lack knowledge of 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

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.

Some New Security Paradigms

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)

The Insider Threat

Old Paradigm:

- The insider threat is our employees, mostly the technical and high-level ones.

New Paradigm:

- Our insider threat comes from employees, but also contractors, vendors, customers, terminated employees, retirees, consultants, service providers, crafts people, graphic arts professionals, interns, and spouses/significant others.

- Low-level personnel can be a major threat, too.

My husband and I have five kids. It's a lot, I know, but we're going to keep trying until we get one we like.
-- Fiona O'Loughlin

Security Training

Old Paradigm:

- Security Awareness Training for general employees is for the purpose of threatening and intimidating them into compliance.

New Paradigm:

- Security Awareness Training seeks to motivate and educate general employees about security, and seek their help.

If you always do what you always did, you will always get what you always got.
-- Moms Mabley (1894-1975)

Security Officer Training

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)

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 not withstanding) 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.

Pain & Gain

Old Paradigm:

- Security is painful and must inconvenience and hassle employees, contractors, & visitors.
- Hassling is a metric for security effectiveness.

New Paradigm:

- Security cannot interfere with productivity any more than necessary.
- Once Security becomes the enemy of productivity and employees, all is lost and the bad guys have partially won.
- Employee acceptance is one metric for effective Security.

Now that the world is getting over the initial shock, and the war against terrorism has begun, what now for bridal retailers?
-- Actual 2002 editorial in the trade magazine *Bridal Buyer*

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."

Problem: Lack of Research-Based Security Practice

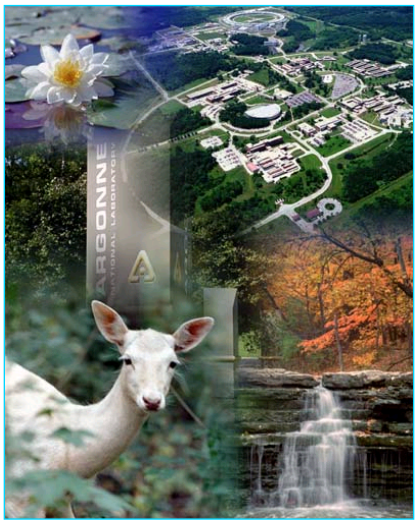
The Journal of Physical Security

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

http://jps.anl.gov

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.youtube.com/watch?v=frBBGJqkz9E

Additional information is available from:

rogerj@anl.gov
and
http://www.ne.anl.gov/capabilities/vat

Argonne NATIONAL LABORATORY

VAT

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)