Education & Awareness: Manage the Insider Threat

Honesty and Service®

Carl D. Willis-Ford
Senior Technical Advisor II, SRA International, Inc.
Senior Member, ISSA
FISSEA Working Group

SRA
Enduring Values. Inspired Performance.®

Speaker Background

- 9 years U.S. Navy, nuclear reactor operator, fast attack submarines
- 25+ years experience: Data Management, IT process, Technical Management,
- B.S. Computer Science (1993)
- M.S. Network Security (2006)
- M.S. Technology Management (2008)
- CIO University Certificate (Federal Executive Competencies), GSA/CIOC (2008)

Defining the Insider Threat

- CERT (Carnegie-Mellon University) definitions
  - Malicious 
    - IP theft
    - IT sabotage
    - Fraud
    - Espionage
  - Accidental 
    - Unintentional
- Other researchers add a 3rd category
  - NonMalicious 
    - “Intentional”
    - “self-benefiting without malicious intent”
    - “voluntary rule breaking”
    - “possibly causing damage or security risk”

  Guo, et al. (2011)

The Malicious Insider

- Plenty of research on malicious insiders
  - Many different behavioral and attack models
- CERT
  - Based on analysis of over 800 malicious insider attacks
  - Some Conclusions:
    - No standard profile of a malicious insider
    - No way to use demographics
    - Watch for feedback loops:
      - Unhappy employee leads to poor performance, leads to
      - Disciplinary action leads to unhappier employee, leads to…
- CERT: Motive is usually either personal gain or revenge
- Per 2013 interview, Snowden took his consulting job with the intent to steal data

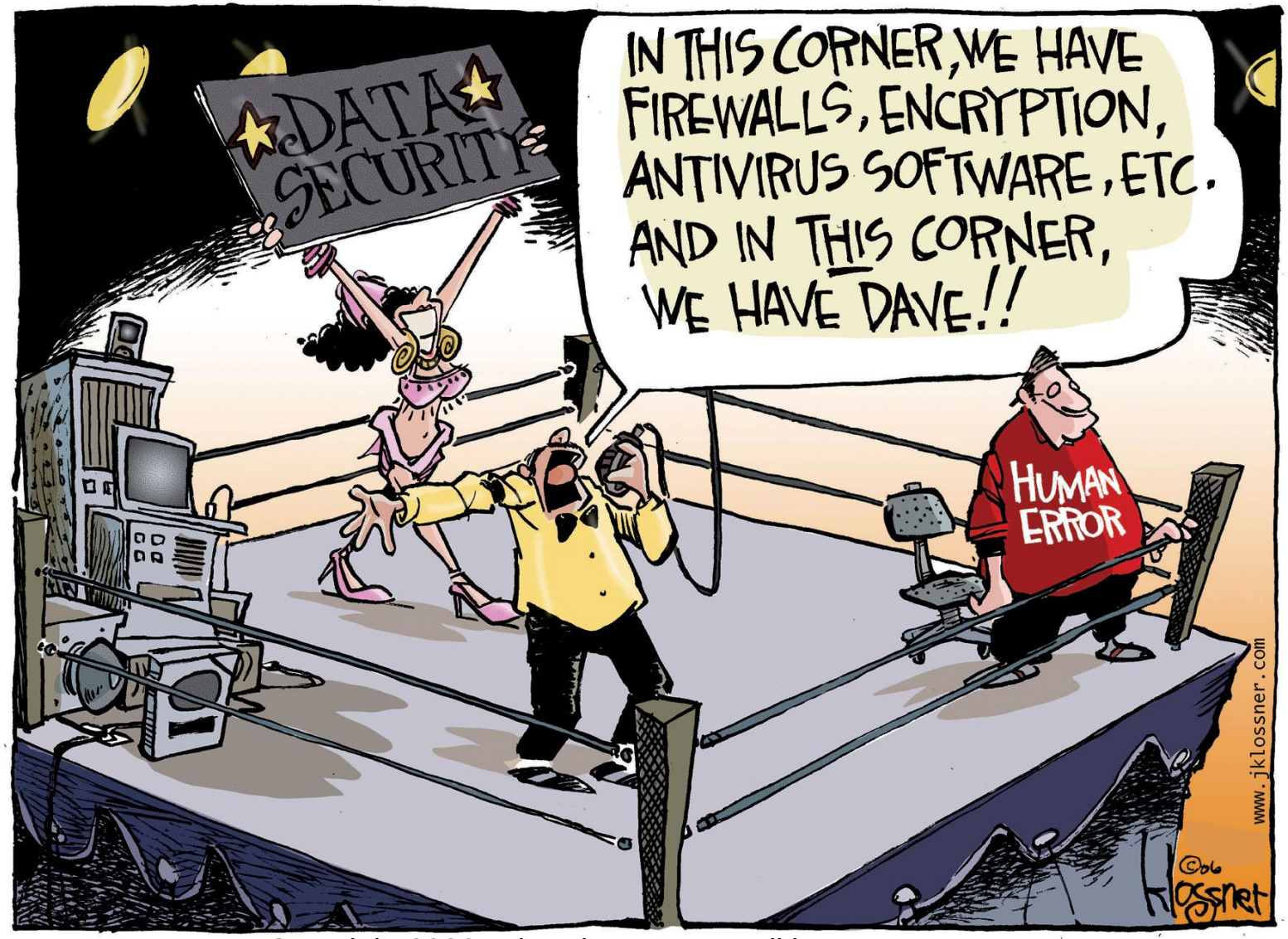
The Malicious Insider, Part 2

- CERT: Insiders exploit business process vulnerabilities as often as they exploit technical vulnerabilities
- "Multiple Case Study Approach to Identify Aggravating Variables of Insider Threats in Information Systems"
  - Good example of the need to understand the methodology
  - Only used 3 case studies
  - Good correlation with theoretical model, but only 3 case studies
  - Showed that Malicious Insider success relies heavily upon other factors, such as weak policy, poorly followed process, and lack of training: "it was through additional aggravating variables originating with IT personnel's and management's actions/inactions that data breach incidents occurred."

Malicious Insider Threat & Training

- Include insider threat awareness in periodic training
- Encourage employees to identify potential insider by their behavior:
  - Threatening the organization or bragging about the damage they could do
  - Downloading large amounts of data after they resign but before they leave
  - Attempted **social engineering** (remind employees that it isn't just outsiders that may try this)
    - Have to know/understand policy in order to know when someone is trying to get them to break it
- Give employees a non-threatening channel to report
- Per reports, Snowden used social engineering ("I need help") to gain access to more data

The Accidental Insider Threat



The Accidental Insider Threat

Less research than Malicious, CERT is a mainstay

CERT Definition (2013):

- An unintentional insider threat is
  - (1) a current or former employee, contractor, or business partner
  - (2) who has or had authorized access to an organization's network, system, or data and who,
  - (3) through action or inaction without malicious intent,
  - (4) causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.
- Major characteristic is 'failure in human performance'

Accidental Insider Examples

- Accidental Disclosure
  - Posting sensitive data on public website
  - Sending sensitive data to wrong email address
- Malicious Code
  - Clicking on suspicious link in email
  - Using ‘found’ USB drive
- Physical data release
  - Losing paper records
- Portable equipment
  - Losing laptop, tablet
  - Losing portable storage device (USB drive, CD)

Categorizing to Better Understand

- Negligent
  - Willing to ignore policy to make things easy
- Well Meaning
  - Completing work takes priority over following policy

Real World Example, January 2013

- Goold Data Systems ‘terrific employee’
- Employee was Account Manager handling Medicaid data for Utah

- Employee had trouble uploading a file requested by State Health Dept.
  - Copied 6,000 medical records to USB drive
  - Lost the USB drive

- CEO admits the employee probably didn’t even know she was breaking policy – **this makes it accidental**

- ‘Well meaning’…

The Accidental Insider Threat, Parallels

- Lacey (2010)
  - Draws parallels between industrial safety programs and information security programs
  - “Experience in the safety profession, for example, has indicated that most safety incidents are blame-free, i.e. no particular individual can be considered to have been directly responsible.”
  - Cites industrial safety research from 1932
    - Almost 90% of workplace accidents caused by human failure
    - For every major accident (death/serious bodily harm)
      - 29 minor incidents
      - 300 near misses

Accidental Insiders and Training

- Cert Insider Threat Team

  "Training and awareness programs should focus on enhancing staff's recognition of the UIT problem and help individuals identify possible cognitive biases and limitations that might put them at a higher risk of committing such errors or judgment lapses."

- Lacey
  - Industrial safety programs study the accidents AND the near misses to determine what is needed for training
  - Rather than just look at who to blame, look at the underlying cause of the accident: process, training, culture…

The NonMalicious Insider

(from a 3M privacy filter ad)

The NonMalicious Insider

- Harder to quantify, since sometimes lumped in with accidental
  - Did the employee know they were violating policy?
- Little empirical research, many theoretical models

- Guo, et al. (2011)
  - “Intentional”
  - “self-benefiting without malicious intent”
  - “voluntary rule breaking”
  - “possibly causing damage or security risk”
- The most common reasons for NMSVs:
  - To make job easier or more convenient (or doable)
  - To help a co-worker

NonMalicious Examples

- Co-workers that helped Snowden
  - Did they know it was against policy to share account/password?
- Irish Garda officer and Anonymous
  - Did he know it was against policy to forward business email to home account?
- In both cases, the answer is most likely ‘yes’.
- However…did they understand the risks associated with their actions? That answer could easily be ‘no’.
  - Personal Risk (of getting caught, of being punished)
  - Risk to the organization

NonMalicious Training Strategies

- Educate users on risks to organization
  - MeriTalk survey
  - Adams & Sasse (2009)
  - Herath & Rao (2009)
  - "…*relative advantage for job performance*, ***perceived security risk***, *workgroup norm*, and *perceived identity match* are the key predictors…" of intent to perform NMSVs. (Guo, Yuan, Archer, & Connelly(2011)
- Again, look to Industrial Safety Programs
  - Traditional view of risk communication in awareness training is "flawed"
  - "to achieve effective and efficient communications **it is critical to understand the relevant beliefs of the audience**. It is not enough to know "what" behaviours exist that are causing information security risk.
  - Communicators must understand "why" the behaviour is occurring which requires an **understanding of an audience's constraints and supporting beliefs**.
    - Stewart & Lacey, 2012

Educate Security Engineers

- Consider Human Factors when designing Security Programs
  - Human Factors courses are not part of many advanced information security degree programs
  - 62% of NSA COE Institutions neither require nor offer courses
  - 36% offered but did not require courses
  - 2% require Human Factors courses
- Prioritizing the end user experience
  - MeriTalk survey: think about the end user trying to follow policy in their daily work rhythm. Help them figure out how to get things done while being compliant:
    - Ban personal thumb drives but don't allow purchase through organization
    - Too many disparate passwords to remember

Wrap-Up

- Will improved training and awareness programs completely eliminate all categories of Insider Threat?
- NO

- How about just the Accidental and NonMalicious?
- NO

- How about…
- NO

No, seriously…wrap it up

- What improved training and awareness programs WILL do:
  - Improve our ability to detect and prevent insider threats
  - Improves a layer of defense
- But we have to get better at it (RSA Conference blog):
  - Present the user with a quiz before content delivery
  - Incentivize training by offering rewards upon completion
  - Train to the risk
  - Start a campaign to improve security awareness
  - Security Awareness should be a continuous improvement process

- Too many organizations have reduced awareness programs to annual fire drills. We'll get out of it what we put into it.

Resources

- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203–236.
- MeriTalk: The Cyber Security Experience, October 15, 2013
- CERT Insider Threat Team http://www.cert.org/insider-threat/
- Moore, A. P., Collins, M. L., Mundie, D. A., Ruefle, R. M., & McIntire, D. M. (2014). Pattern-Based Design of Insider Threat Programs. Retrieved from http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_427430.pdf
- Silowash, G. J., Cappelli, D. M., Moore, A. P., Trzeciak, R. F., Shimeall, T., & Flynn, L. (2012). Common sense guide to mitigating insider threats. Retrieved from http://repository.cmu.edu/sei/677/
- Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits (pp. 236–250). IEEE. http://doi.org/10.1109/SPW.2014.39
- Stewart, G., & Lacey, D. (2012). Death by a thousand facts. *Information Management & Computer Security*, *20*(1), 29–38

Resources, Part 2

- Bureau, F. I. P. (2013). Unintentional Insider Threats: A Foundational Study. Retrieved from http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf
- Buckley, O., Nurse, J. R., Legg, P. A., Goldsmith, M., & Creese, S. (2014). Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat. In *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on* (pp. 8–15). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6978924
- Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4–13. http://doi.org/10.1108/09685221011035223
- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165

More Resources

- Beach, S. K. (2014). Usable Cybersecurity: Human Factors in Cybersecurity Education Curricula. *National Cybersecurity Institute Journal*, *1*(1), 5–21.
- D. M. Cappelli, A. P. Moore, and R. F. Trzeciak, The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes, 1st ed. Addison-Wesley Professional, 2012
- Vaas, Lisa, 1 "terrific employee" + 1 thumb drive + 6,000 lost medical records = fired! (web article). https://nakedsecurity.sophos.com/2013/01/21/1-terrific-employee-1-thumb-drive-6000-lost-medical-records-fired/
- RSA Conference Blog, March 3, 2015. Security Awareness Training: We're Doing it Wrong! http://www.rsaconference.com/blogs/security-awareness-training-were-doing-it-wrong

Even More Resources

- Kamoun, F., & Nicho, M. (2014). Multiple Case Study Approach to Identify Aggravating Variables of Insider Threats in Information Systems. *Communications of the Association for Information Systems*, *35*(1), 18. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3827&context=cais
- D. S. Wall. (2011) Organizational security and the insider threat: Malicious, negligent and well-meaning insiders (white paper). [Online]. Available: https://www4.symantec.com/Vrt/offer?a id=108920
- How to Read a Research Article http://www.sagepub.com/bjohnsonstudy/howtoarticle.htm

Contact Information

Carl Willis-Ford

carl_willis-ford@sra.com

LinkedIn: Carl Willis-Ford
(http://www.linkedin.com/in/srxdba/)