Honesty and Service®

# Non-Malicious Security Violations

*Carl D. Willis-Ford*

*Senior Technical Advisor II, SRA International, Inc.*

*Senior Member, ISSA*

*Doctoral Candidate, Capitol College*

*Significant Work. Extraordinary People. SRA.*

# 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)
- Doctor of Science in Information Assurance, 2014 (expected)

# What do we mean by NMSVs?

- **“Intentional”**
- **“self-benefiting without malicious intent”**
- **“voluntary rule breaking”**
- **“possibly causing damage or security risk”**

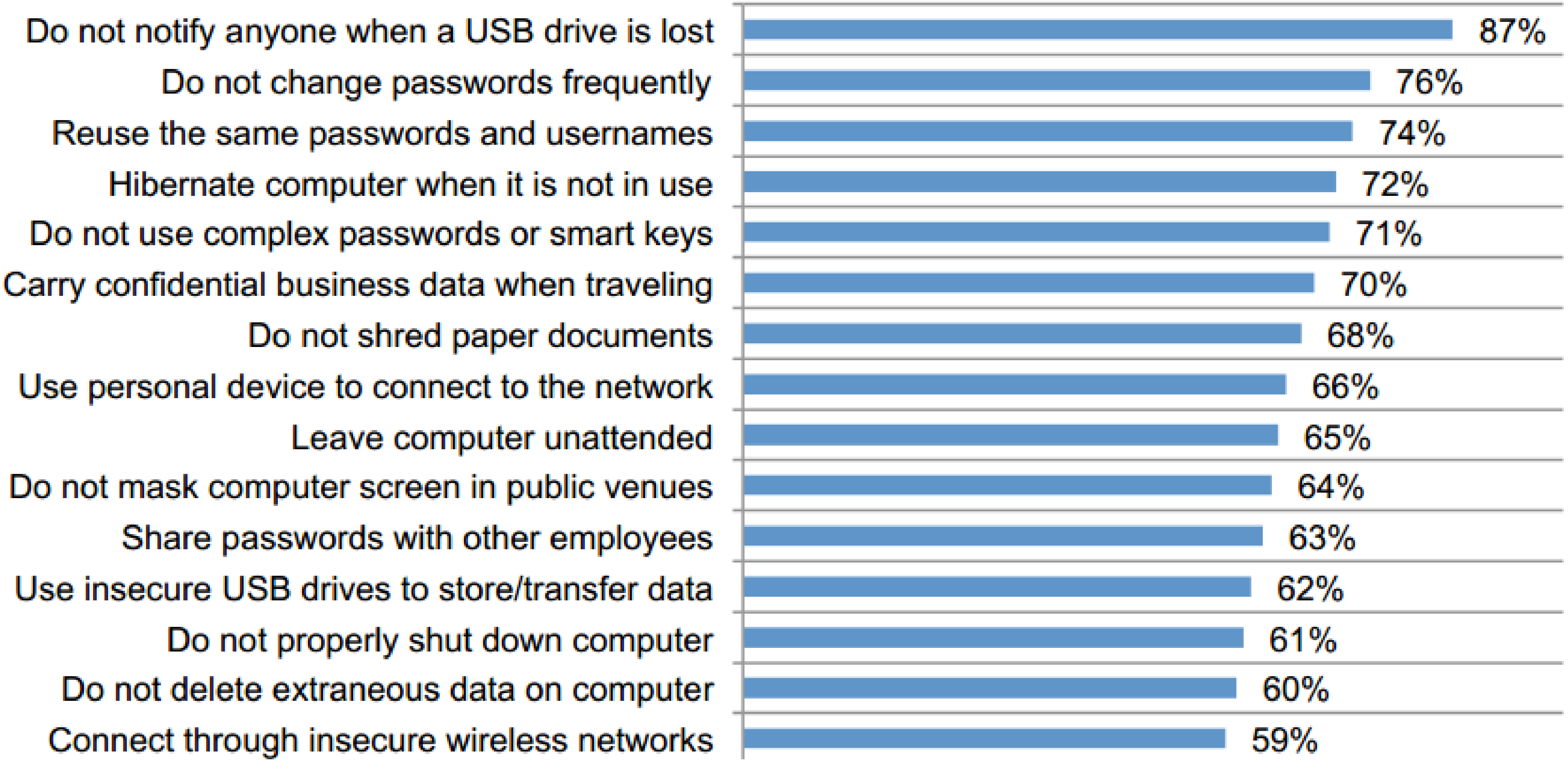
**Guo, et al. (2011)**

## The most common reasons for NMSVs:

- To make job easier or more convenient (or doable)
- To help a co-worker

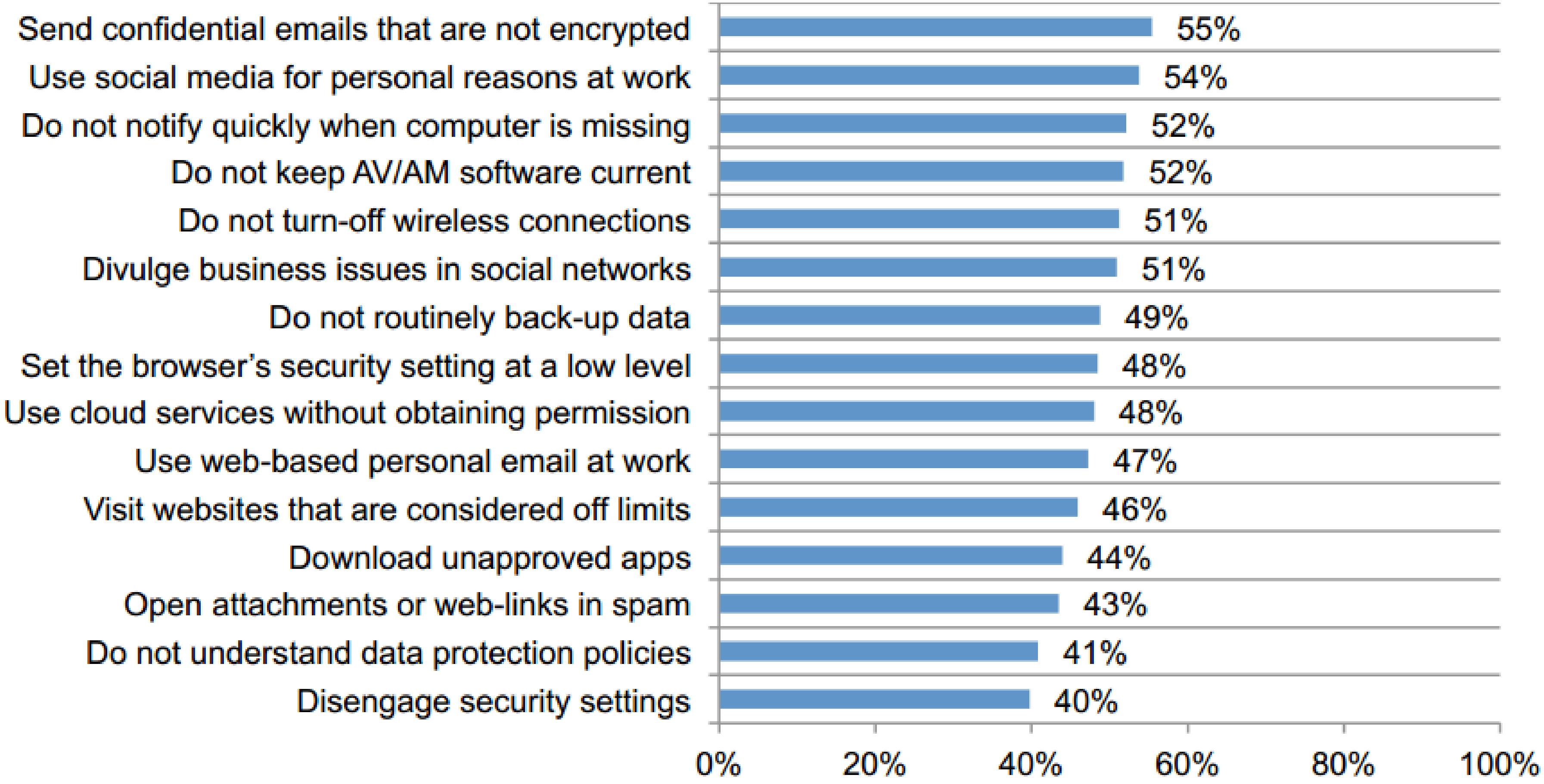
Honesty and Service®

# Common NMSVs, Part 1



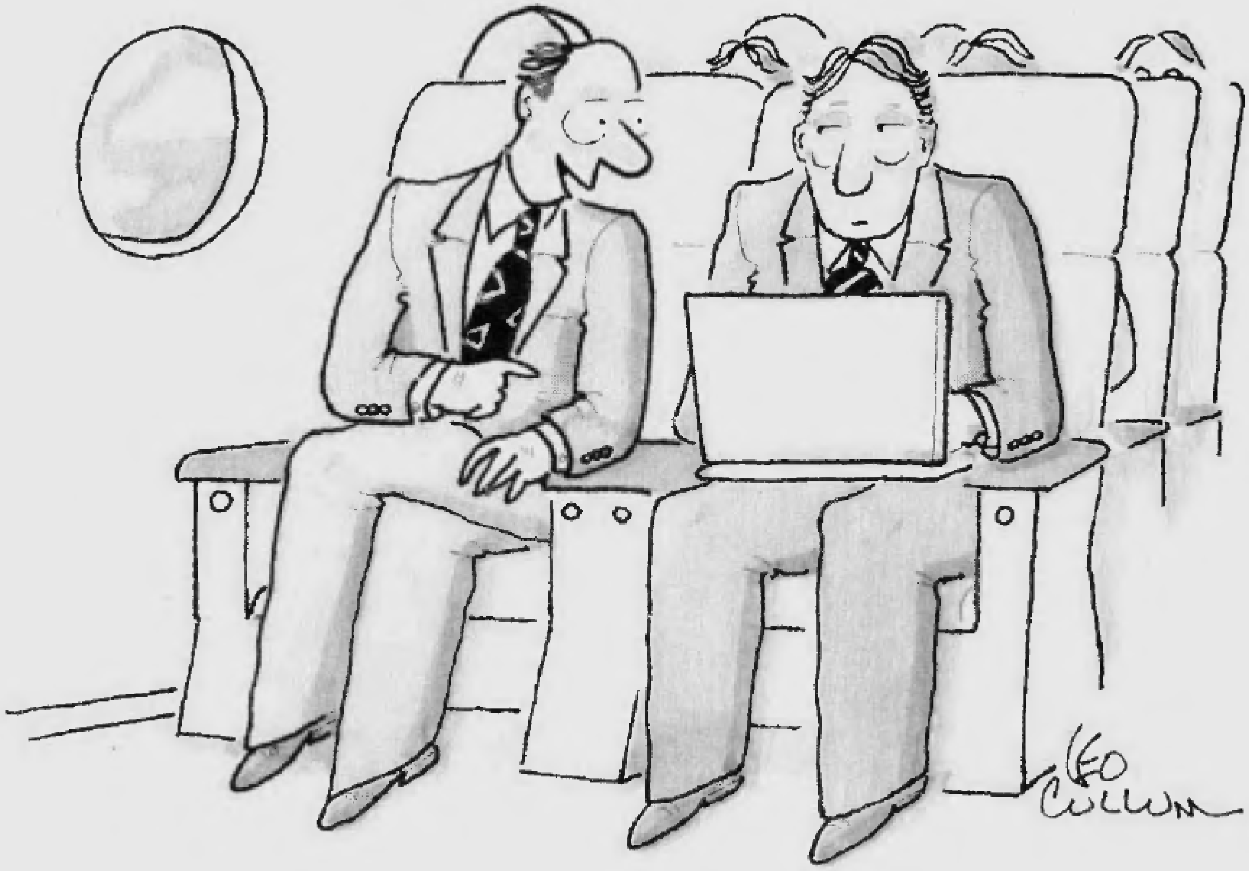
Ponemon Institute (2012)

# Common NMSVs, Part 2



# Example

(from a 3M privacy filter ad)



"You spelled 'confidential' wrong."

# Real-World Example #1

- **January 2012 conference call between FBI and U.K.'s Serious Organized Crime Agency (SOCA)**
  - Subject of call was to discuss strategies in handling hacktivist group Anonymous

- **Recorded call was released by Anonymous in early February**

- **After arrests in March, details revealed:**

**Hacker had compromised home email accounts of Irish police officers, one of whom had forwarded conference call details from his business account to his home (Gmail) account.**

**…he didn't want to drive into the office for the call…**

# Real-World Example #2

- Snowden case

- Investigation into how he was able to access such a wide array of information

- Reports are that he talked at least one co-worker (possibly several) into either giving him their passwords or typing their passwords on his computer to give him one-time access (he copied what they typed).

- Snowden’s actions were malicious (social engineering)
- Co-workers’ actions were NMSVs

# Real World Example #3

Do you know this woman?

…she wants to be your friend

# The Robin Sage Experiment

- **December 2009 to January 2010**
- **Fake Facebook, Twitter, LinkedIn profiles, posing as a Cyber Threat Analyst**
- **Sent requests and established social network connections with over 300 security professionals**
  - Men and women of all ages
  - NSA, DoD, and Global 500 companies
- **Results**
  - Deployed troops discussing locations and movement
  - Consulting opportunities from Lockheed Martin and Google
  - Given business sensitive documents for review
  - Able to determine answers to password change questions based on information provided in online conversations

http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf

# Under the Radar or not?

- **Snowden widely reported as having ‘stolen’ passwords, when, at least initially, they apparently given to him or voluntarily typed into his machine to give him access**

- **Verizon Data Breach report includes NMSVs as ‘accidents’**

- **Computer Security Institute’s annual survey, as of 2009, recognizes malicious vs. non-malicious security violations**
  - 2010/2011 survey
    - 14.5%:  over 80% of financial losses due to NMSVs.
- **Anecdotally:  NMSVs frequently ‘open the door’ to other attacks, which get more publicized.**

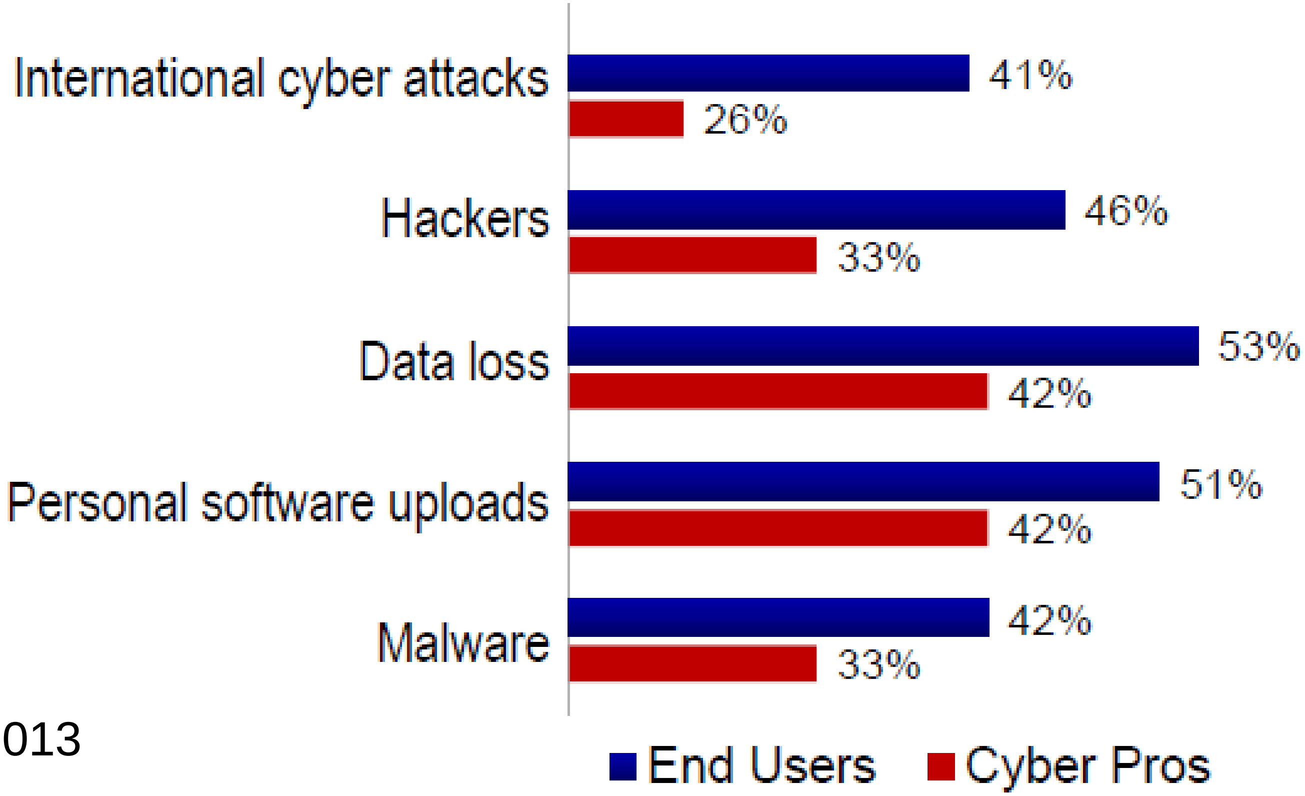
# MeriTalk Research, October 2013

Interviewed IA professionals and end users at unspecified government agencies

- Half of all breaches caused by lack of user compliance
- Only 40% of security pros say that focus is on end-user experience with security
- 20% of end users recalled an instance where they were unable to complete a work assignment on time due to security measures
- 31% of end users say they use some kind of security work-around at least once/week

# MeriTalk Research, October 2013

**Percentage who believe their agency is completely prepared for the following challenges:**



MeriTalk, 2013

# Strategies

## From research sources:

- **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
    - Single Sign-On
- **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

# 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)
  - 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"

  Overcome the 'convenience' factor

# Resources

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46
- 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.
- 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
- MeriTalk: The Cyber Security Experience, October 15, 2013
- Stewart, G., & Lacey, D. (2012). Death by a thousand facts. *Information Management & Computer Security*, *20*(1), 29–38
- CERT Insider Threat Team. (2013) Unintentional insider threats: A foundational study.

# Contact Information

**Carl Willis-Ford**

**carl_willis-ford@sra.com**

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