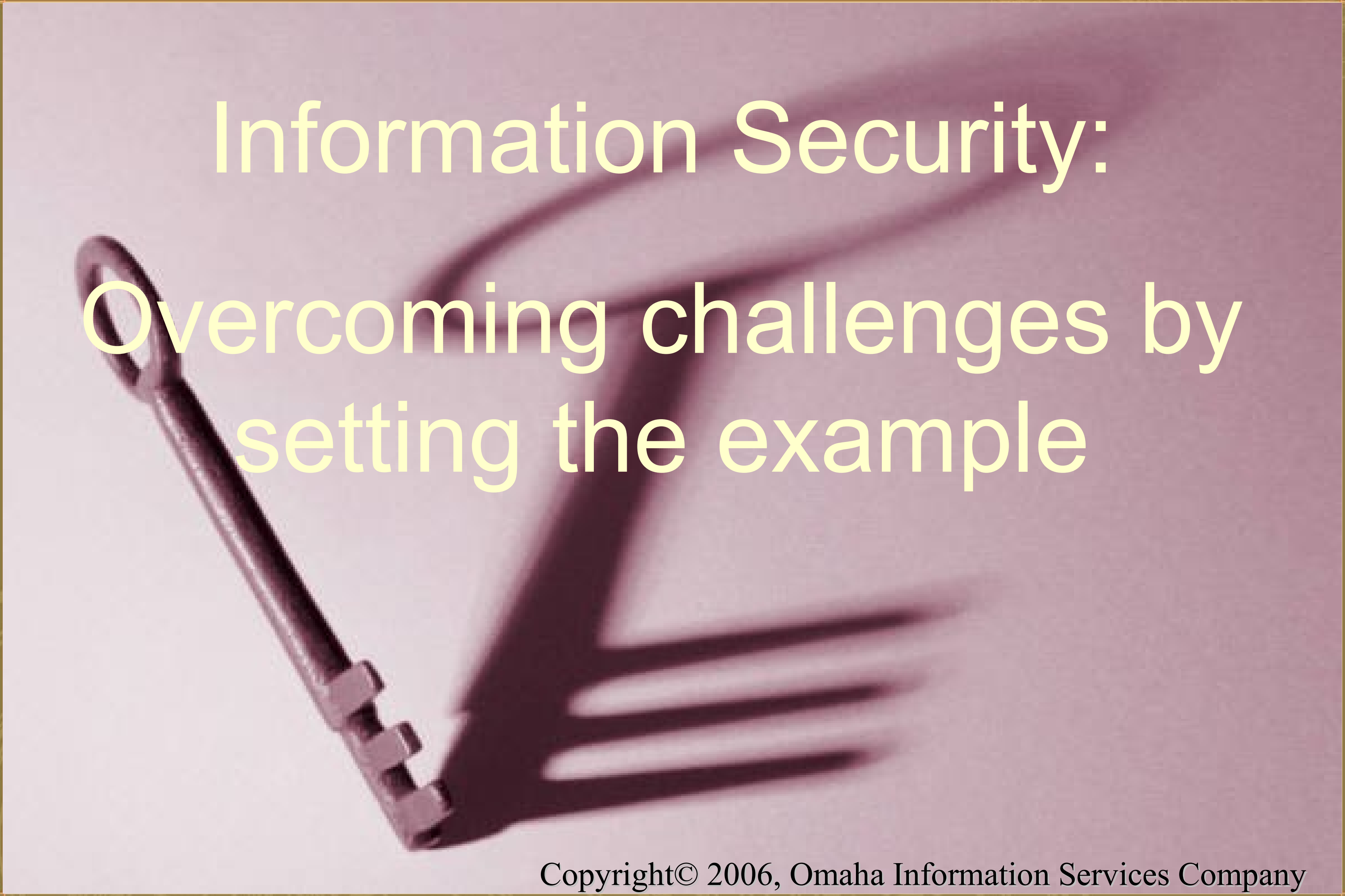
OMAHA INFORMATION SERVICES COMPANY

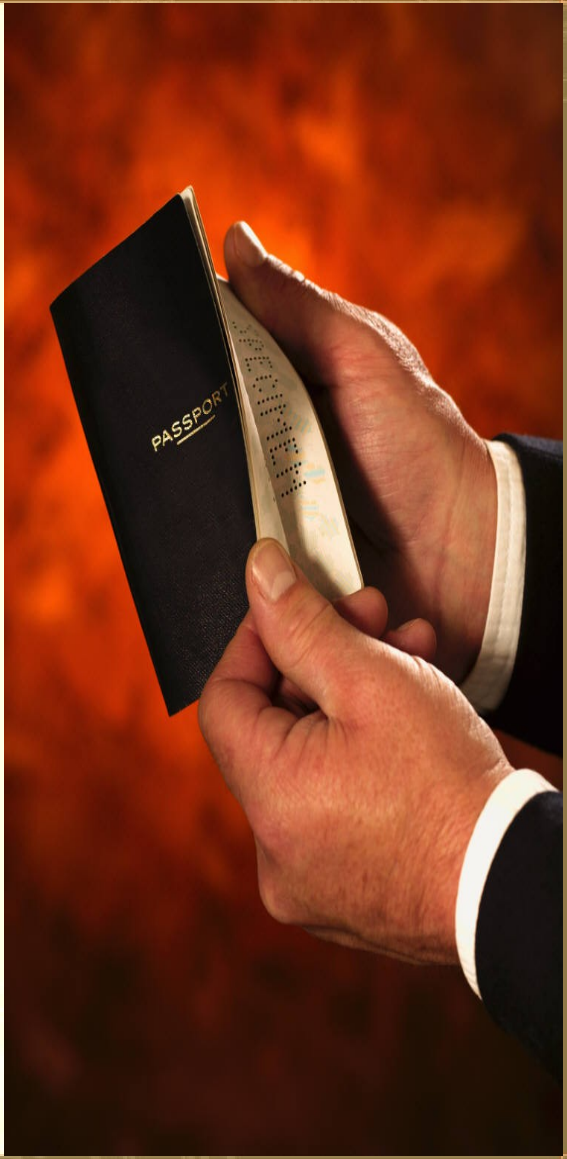
Information Security:

Overcoming challenges by setting the example



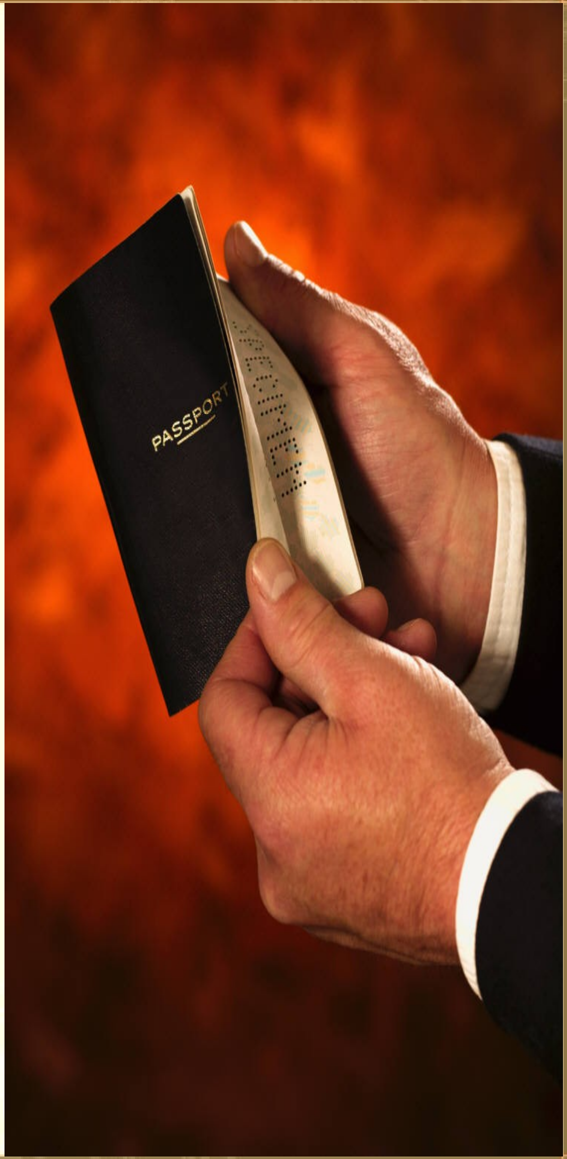
This presentation will cover:

- Who is this dude?
- Fallacies, Myths, and Velvet Traps
- Setting the Example
- About Omaha Information Services Company



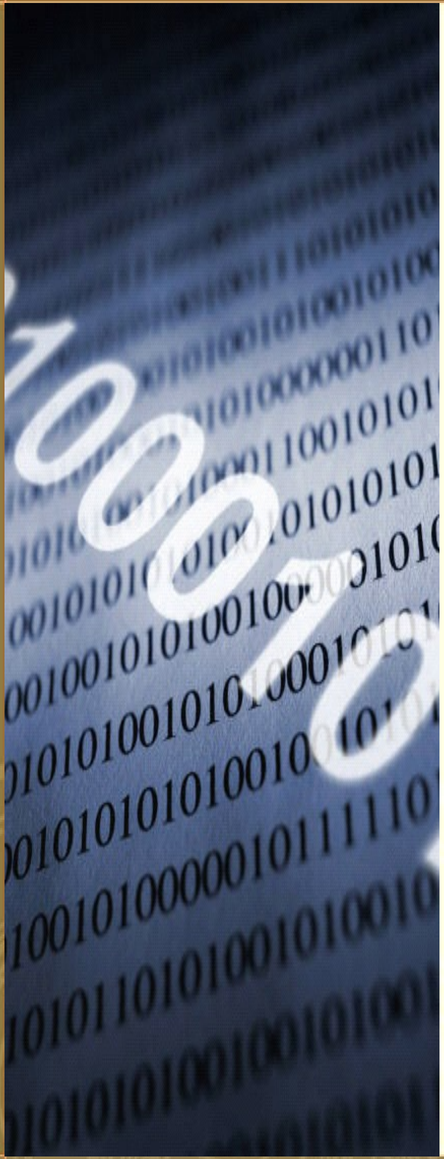
Who is this dude?

- James Phillips, CISSP
- Formerly: UNIX systems programmer and I/S Sr. Security Analyst, Mutual of Omaha Companies
    - Internal Consultant
    - Focused on initiatives
        - Risk Assessments
        - Identity Management
        - Application Security
        - Business Partner Risk Management



"Moderation in all things, including moderation."

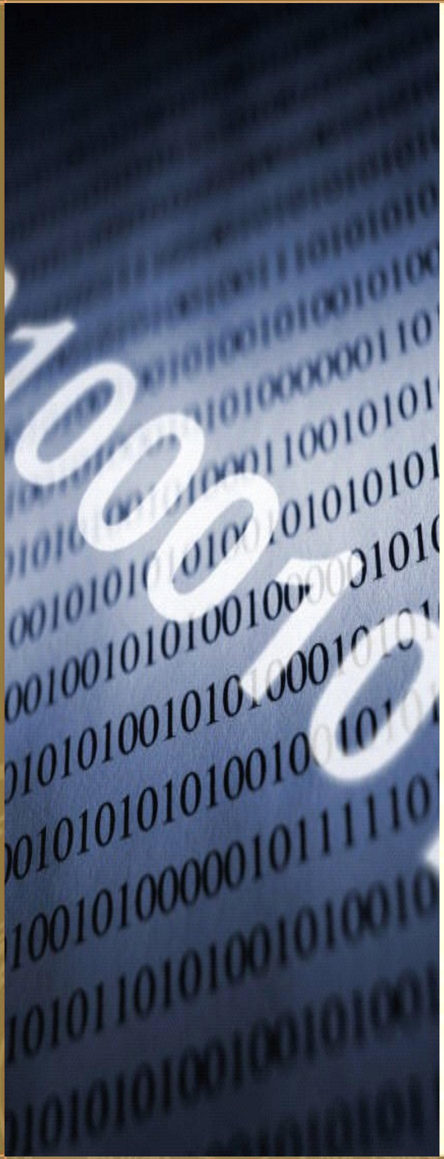
Mark Twain



Fallacies, Myths, & Velvet Traps

- Expert Advice
- The Silver Bullet
- It’s a technology problem
- That’s their problem now
- Not invented here
- Just say No

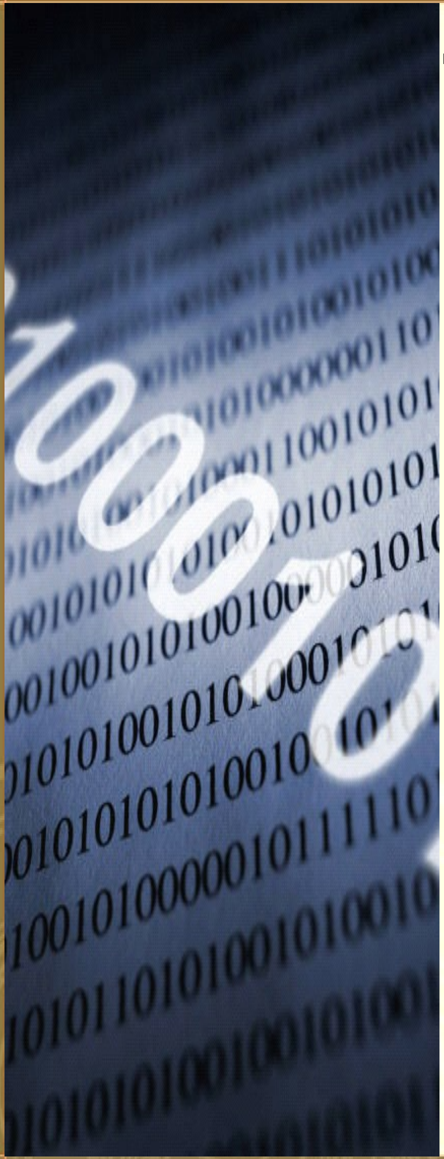
This document is for educational purposes only and is not a substitute for legal advice.



Expert Advice

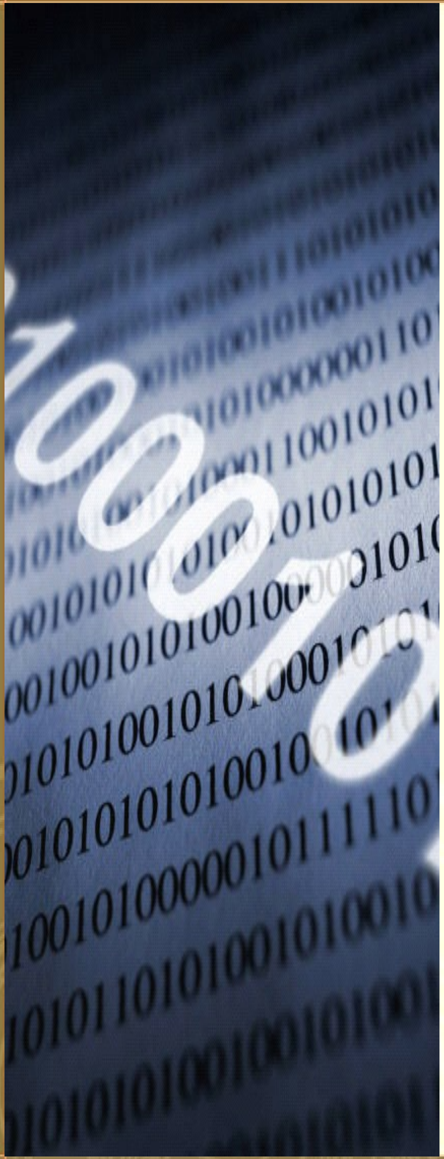
"An expert is somebody who is more than 50 miles from home, has no responsibility for implementing the advice he gives, and shows slides." - Edwin Meese III

- Context
- Experience
- Expert advice is just that, advice
- Think critically
- Seek relevance to *your* situation



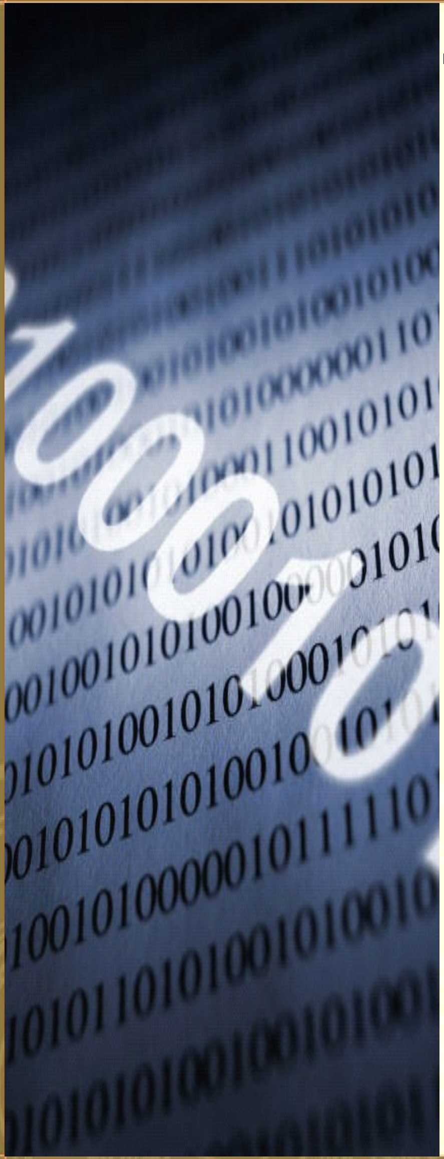
The Silver Bullet

- Poor choice for projectile weapons
  - Harder and lighter than lead
    - Less energy transfer
    - Accelerates wear
  - Expensive to use and manufacture
- “Compliance” Software frequently mistaken for silver bullets



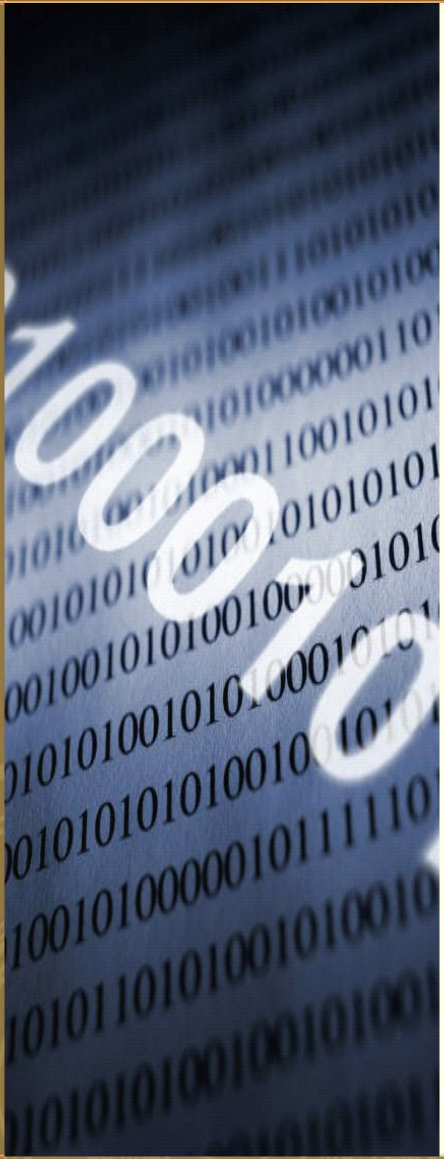
It’s a technology problem

- See also: *Silver Bullet*
- Thinking commonly applied to process or personnel problems by technology people
- Most Information Security problems are hybrid problems
  - Technology can help, but not *solve* the problems
  - e.g. Compliance, Application security, Identity Management
- Technology solutions can automate and accelerate bad habits



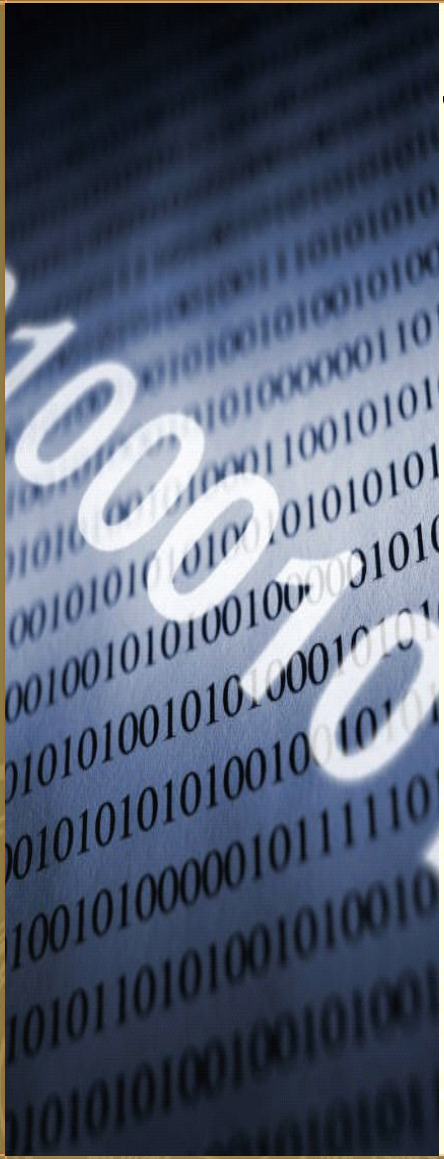
That’s their problem now

- Frequently applied to Outsourcing
- Frequently used to avoid oversight
    - If I outsource this, I can get it done faster and cheaper and to spec
    - Costs are not accurately calculated
- *Is* risk denial
- *Is not* risk transfer
- It’s your data, and your problem



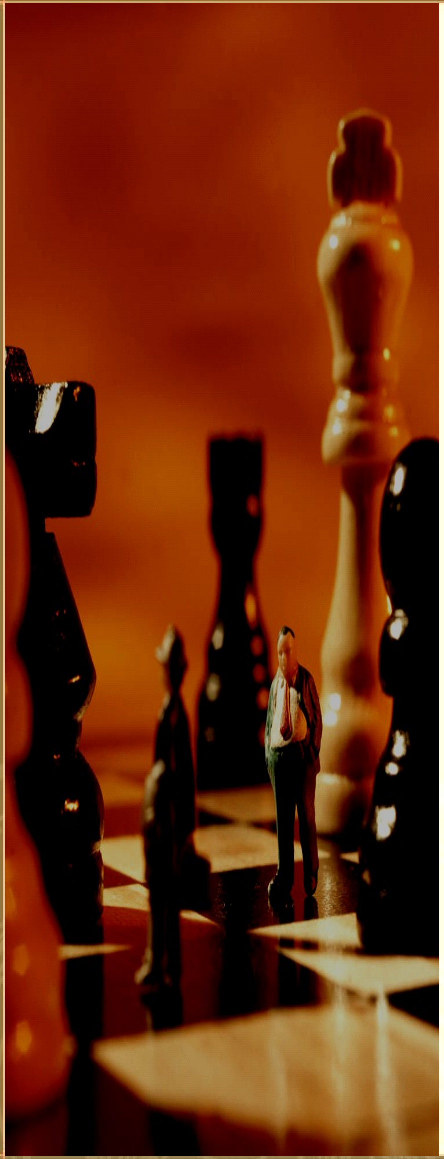
Not invented here

- Distrust of outside advice or solutions
- "No one could possibly understand our unique requirements/limitations"
  - Probably not that unique
  - Continual re-invention of wheel results in a plethora of uniquely shaped wheels
    - Some of which may be round
    - Most of which are expensive and difficult to maintain



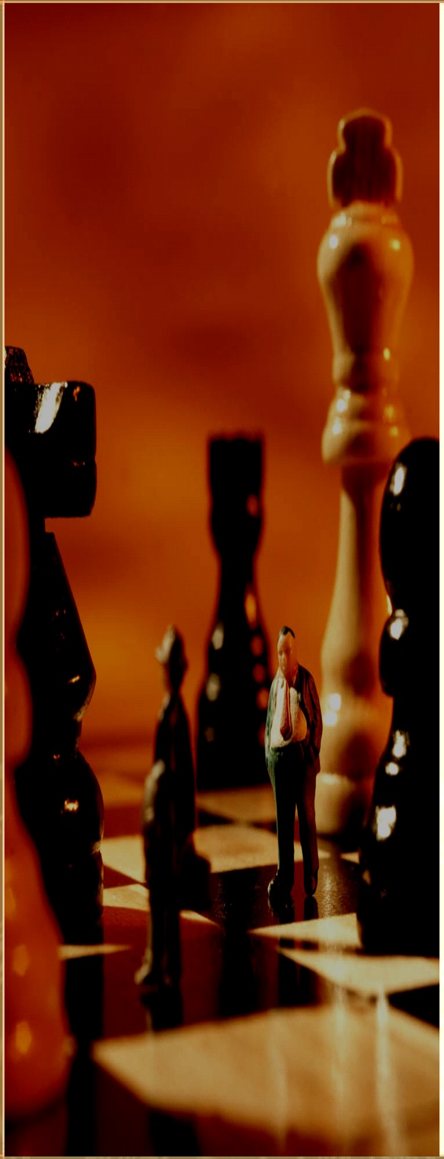
Just say No

- No (unfortunately) is not an answer business people will accept
    - Encourages escalation
    - Doesn’t solve the problem
- Determine the problem
    - Ask “What are you trying to accomplish”?
    - Understand their requirements
- Explain your requirements
- Present an alternative



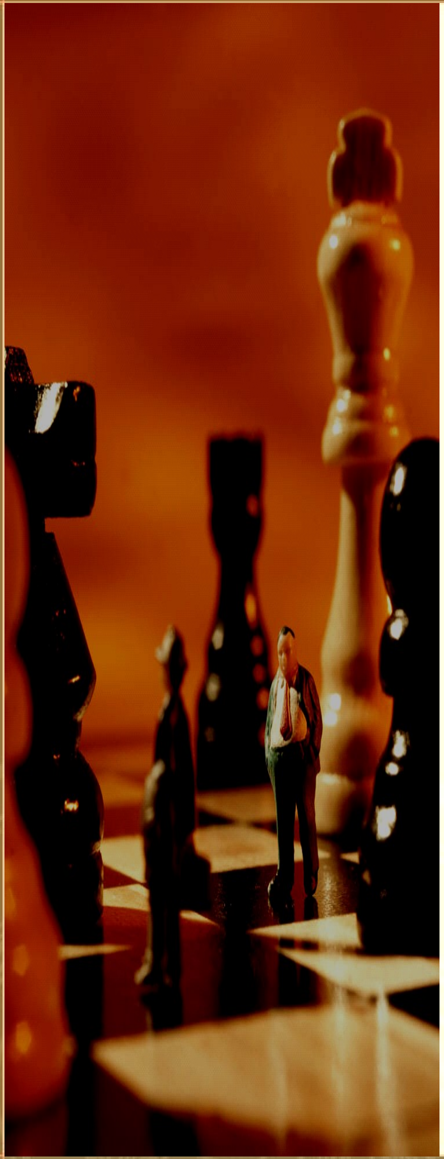
Setting the Example

- Adapt to changing roles
- Know your tools
- Know your audience
- Transfer knowledge
- Eat your own dog food
- Be fair



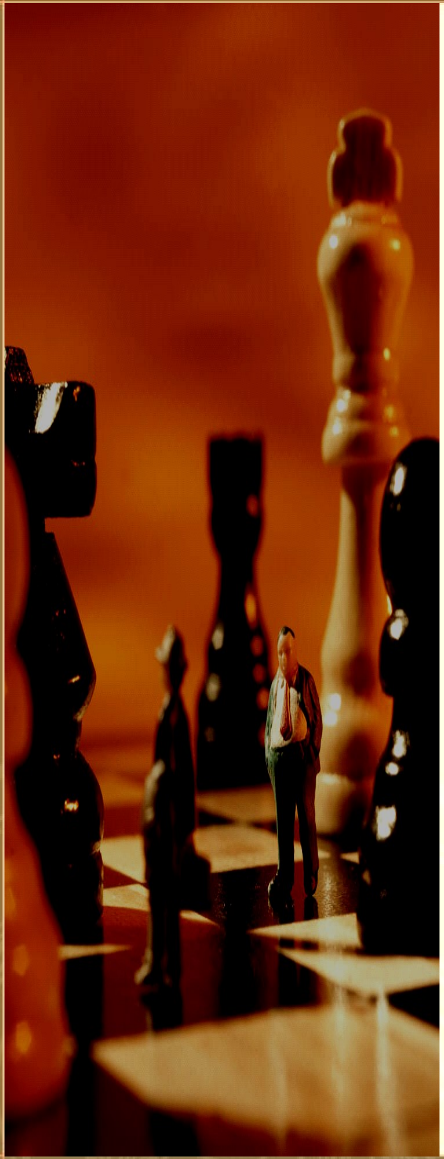
Adapt to changing roles

- Information Security Past
  - Policies
  - User provisioning
  - Technical Housekeeping
  - “Busting” people
- Information Security Present
  - Internal consulting
  - User education/awareness
  - Business knowledge
  - Teaching People



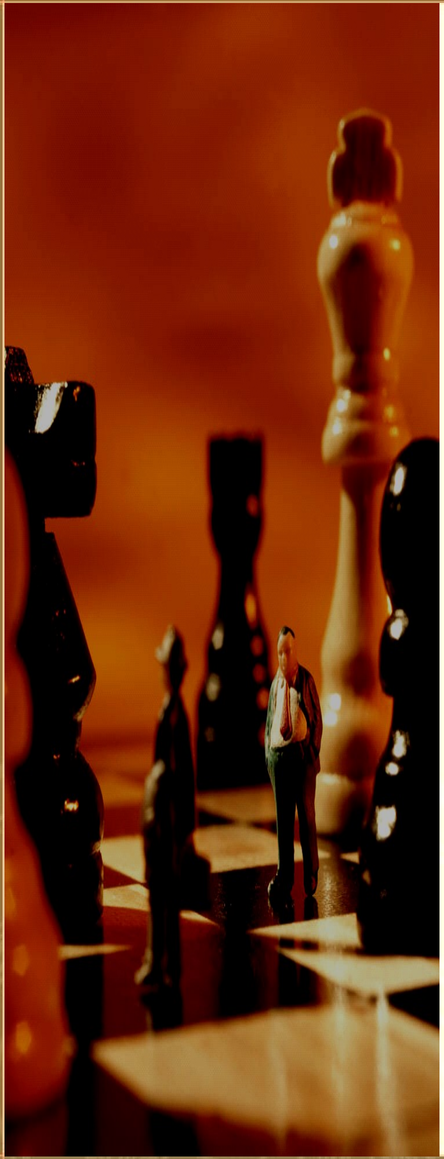
Know your tools

- “You broke the _____!”
- Know when the tool is right
- Know how to tell when tool is wrong
  - review results prior to reporting
  - Used to distract from the real issues
- Security Testing tools are powerful
- Communicate their use!



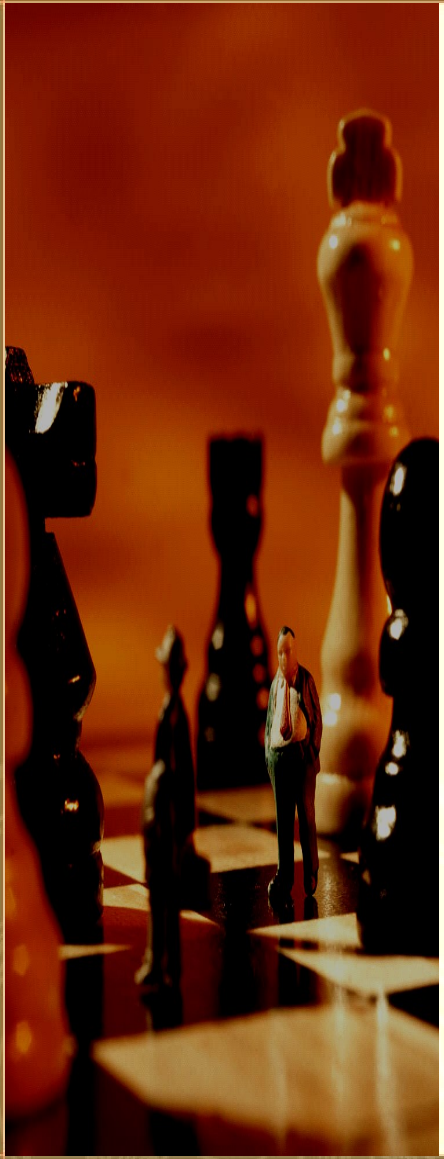
Know your audience

- Speak to their level of understanding
  - Perhaps you need to educate them?
- Use their language
- Lead them to your message
- Use the opportunity to educate
  - Teaching, not preaching



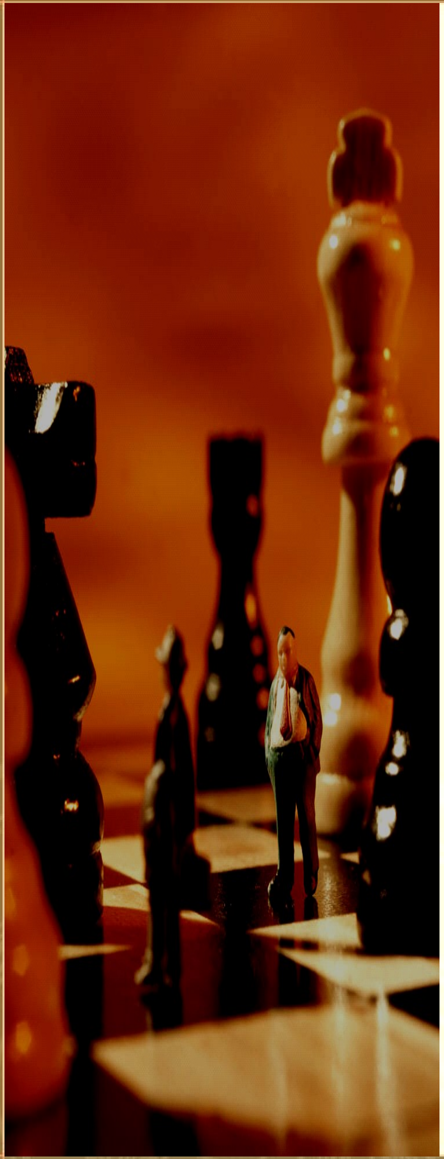
Transfer Knowledge

- Security teams notoriously secretive
- Share the knowledge
  - Our craft is not a trade-secret
  - Offload some work
- Explain the requirements (and their origins)
  - Anticipate the “why” question
    - Company policy
    - Legal
    - Regulatory
- Create internal advocates



Eat your own dog food

- Do not exempt yourself from policies
- Demonstrate their workability
  - Deprive your critics of ammunition
  - Test them on your laziest team member
- Be an “early adopter”
  - Improve the product/process
- Be introspective
- Sell yourself and your mission



Be Fair

"..nothing is more destructive of respect for the government and the law of the land than passing laws which cannot be enforced." – Albert Einstein

- Enforce policies uniformly
- Remember the business objective
- Try a little empathy
  - Did we communicate it properly?
  - Was there buy-in?
  - Is it likely to meet it's goals?
- Change it if necessary

Summary

- Think critically
- The easy way out probably isn’t
- Keep it simple
- Know the business
- Educate users
- Practice what you preach/Lead by example
- Be fair
- Contribute positively

Who is OISC?

OISC is a subsidiary of Mutual of Omaha with experience developed over decades of work in the field of operational risk management and a commitment to integrity and customer service.

Thank you