



Education

# **Guarding the Jewels: A Primer on Storage Network Security**

Richard Austin, CISSP

- The material contained in this tutorial is copyrighted by the SNIA.
  - Member companies and individuals may use this material in presentations and literature under the following conditions:
    - ◆ Any slide or slides used must be reproduced without modification
    - ◆ The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.
  - This presentation is a project of the SNIA Education Committee.
  - Neither the Author nor the Presenter is an attorney and nothing in this presentation is intended to be nor should be construed as legal advice or opinion. If you need legal advice or legal opinion please contact an attorney.
  - The information presented herein represents the Author's personal opinion and current understanding of the issues involved. The Author, the Presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.
- NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.**

## ➤ Guarding the Jewels

- ◆ Information has come to be the crown jewels of the modern enterprise but with its value has come increased risk of compromise or unauthorized disclosure. This presentation will review the common risks in the storage network environment, useful ways of mitigating them and the guidance provided by the SNIA Best Common Practices for Storage Security.

# What is “security”?

## ➤ A “To Do” list

- ◆ Check all these boxes and I’ll be secure
- ◆ By the way, which set of boxes should I be checking?

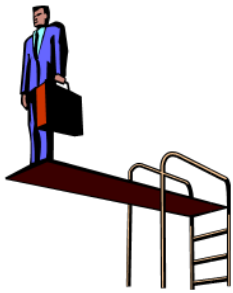


## ➤ A Journey

- ◆ Follow the road and “Security” is somewhere out there
- ◆ How will I know when I get there?

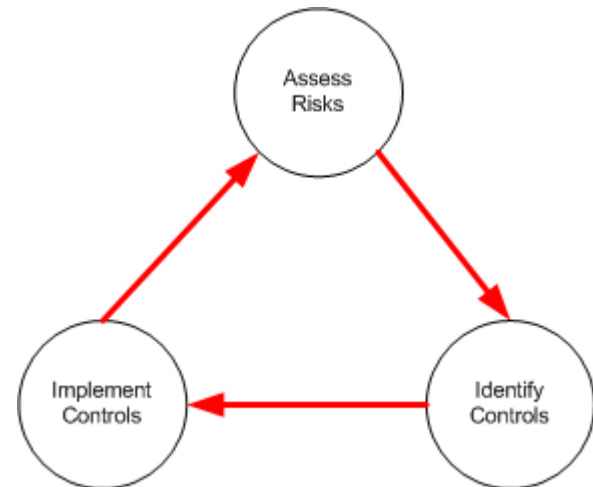


## ➤ Security is really about managing risk



# How do I manage risk?

- There are myriad “risk management” processes
  - ◆ Microsoft SRMG
  - ◆ FAIR
  - ◆ NIST
- Choose one that “fits” you and your organization
- It’s more important to have a process rather than which you use



# What is risk?

- ▶ The chance of something bad happening

$$R = f(t, v, a)$$

That looks like math, let's leave now

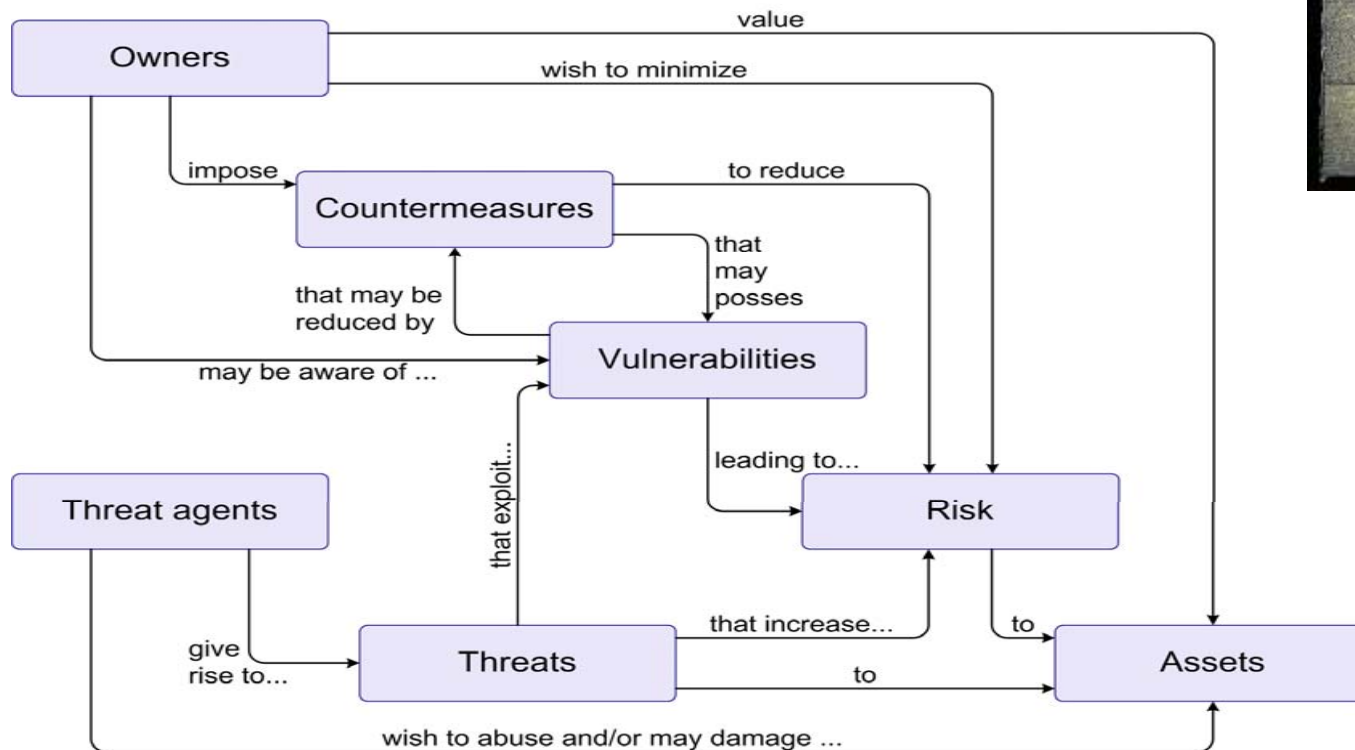


$$R = f(t, v, a)$$

- In order to understand our risks, we must have a good handle on three things:
  - ◆ Threats – the “bad thing”
  - ◆ Vulnerabilities – what allows threats to do bad things to assets
  - ◆ Assets – the things we’re paid to protect

# Coming to Terms

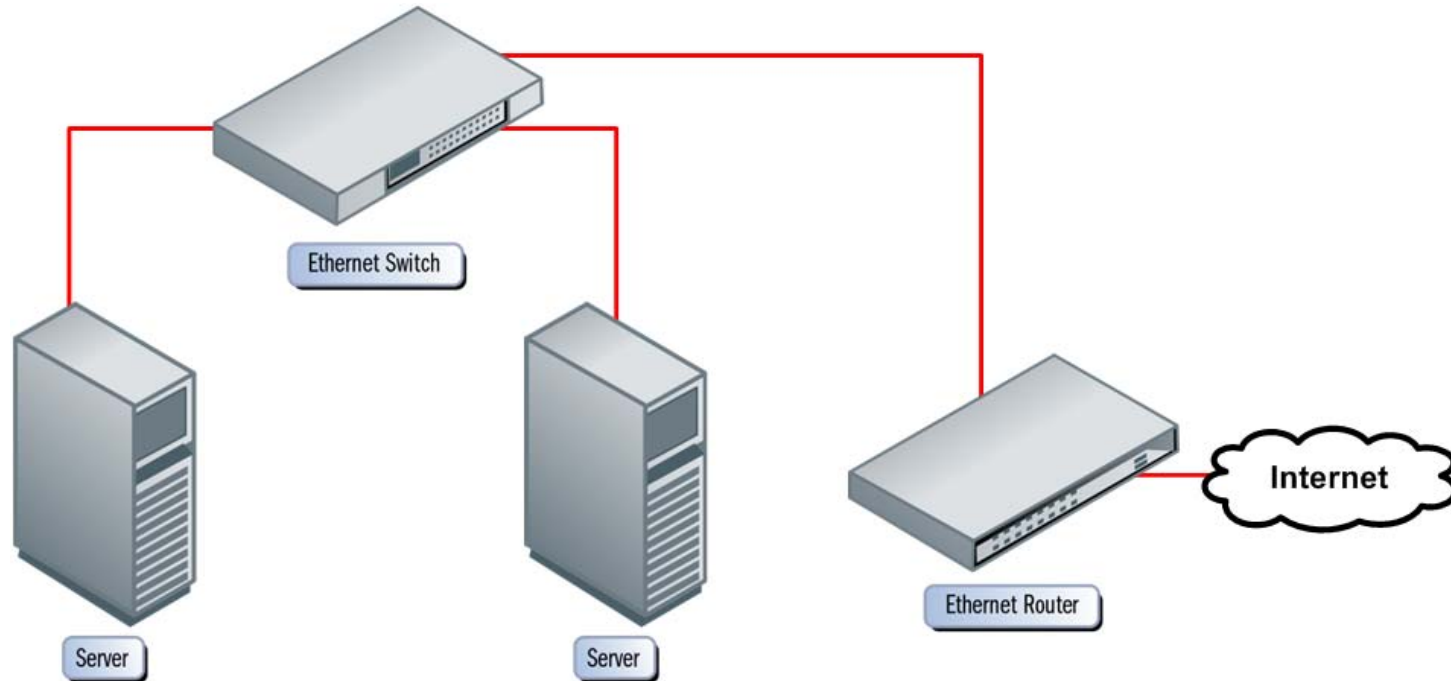
- Security people have a language all their own but here's the Rosetta Stone



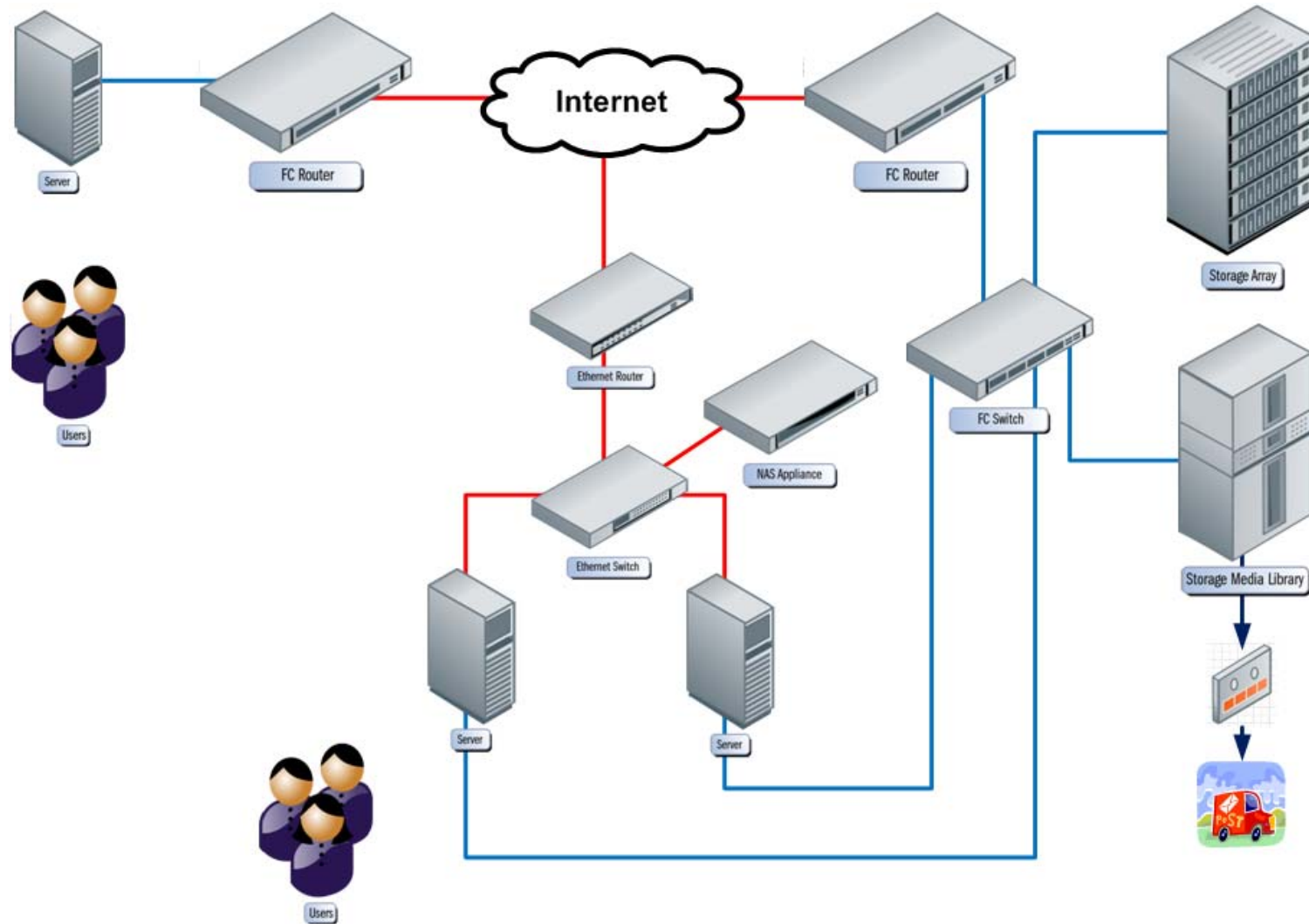
ISO/IEC15408-1: Information technology – Security techniques – Evaluation criteria for IS security – Part 1: Introduction and general model, p. 13

$$R = f(t, v, a)$$

- Asset – SAN infrastructure (IOW, all of our data)
  - ◆ High business impact if damaged or made unavailable
- Vulnerability – Storage administrators use telnet to connect to SAN devices for management
  - ◆ Logon credentials sent in clear text across the network
- Threat – an attacker could sniff storage administrators' logon credentials off the network
  - ◆ Low risk of an outsider getting access to the internal network

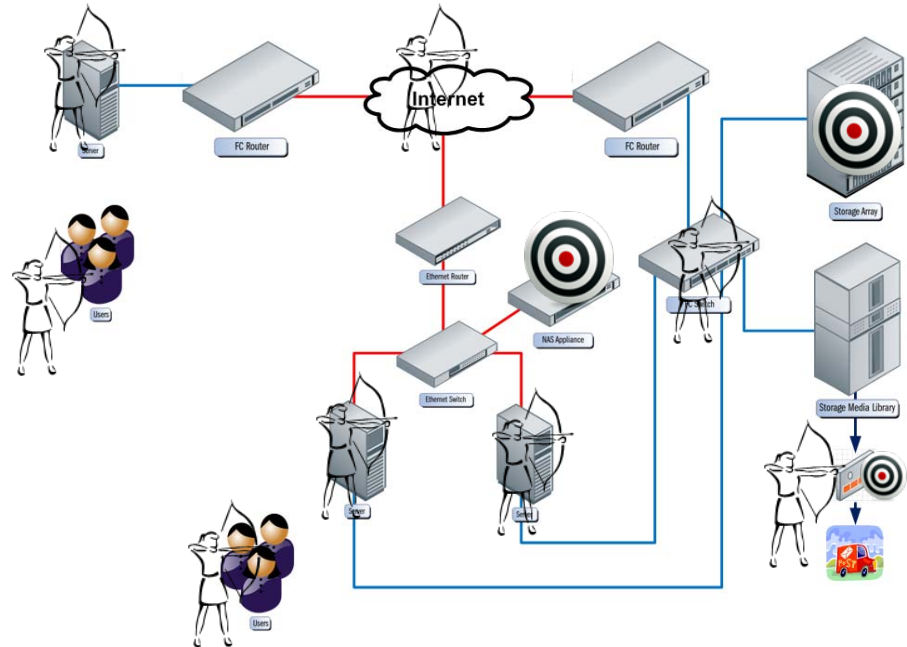


- Data stored on the servers
  - ◆ Want the data? Compromise the server.

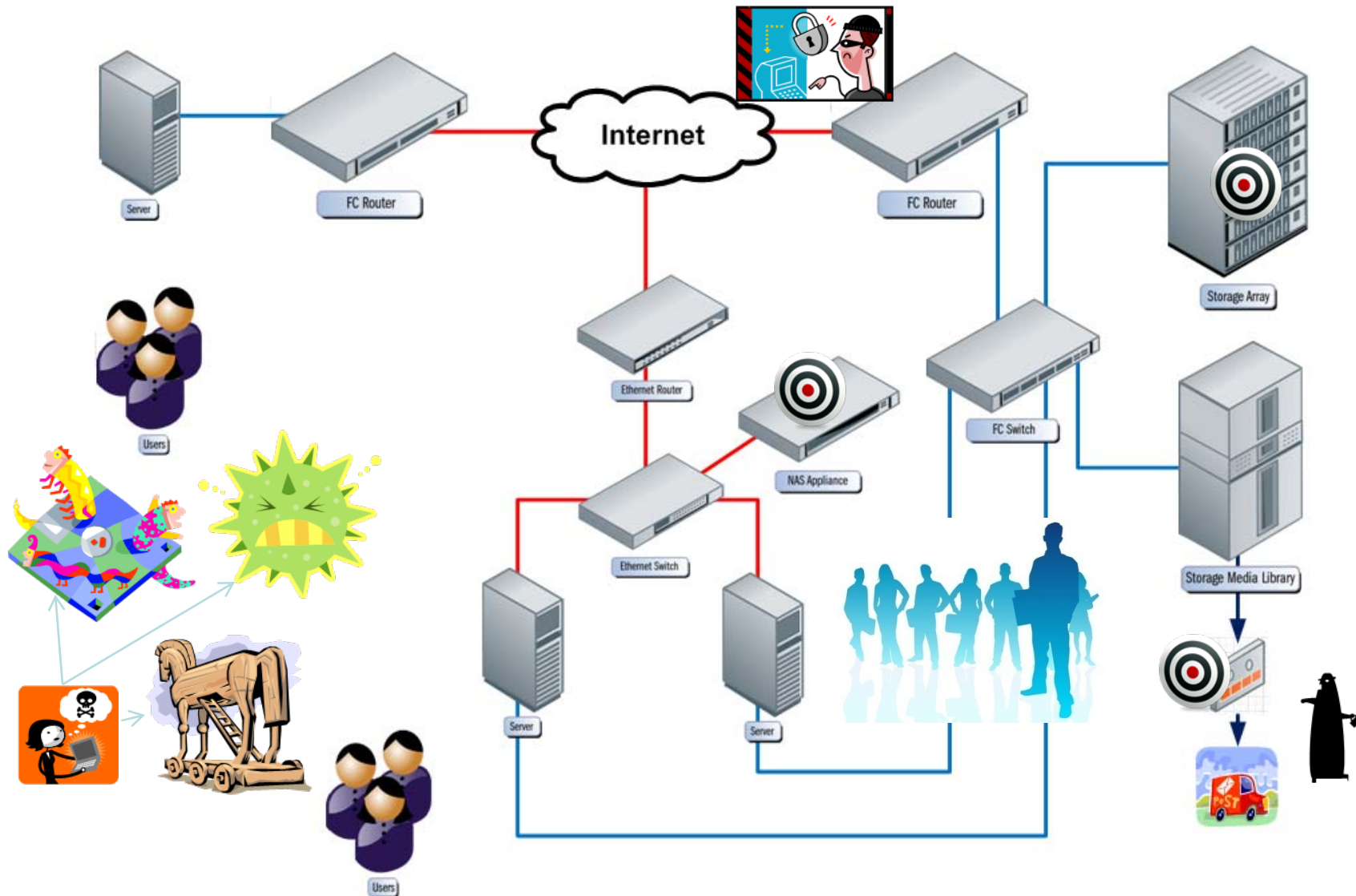


# This is bad

- Reduced the number of targets
- Greatly increased the value of targets
- Added more ways to “get a shot” at the targets



# Some Common Threats



# The SNIA Best Common Practices (BCPs)

[http://www.snia.org/forums/ssif/programs/best\\_practices/](http://www.snia.org/forums/ssif/programs/best_practices/)

# The Best Common Practices

- NOT a checklist
- Good general practices that help reduce common risks
- Choose the ones that are relevant in your environment
  - ◆ If your risk assessment identifies a particular area, then look to see what the BCP's recommend as ways to manage risks in that area



# Storage Security Challenges

- Control of Privileged Users (Administrators)
- Protection of Storage Management
- Credential & Trust Management
- Data In-flight Protection
- Data At-rest Protection
- Data Availability Protection (redundancy, resiliency, integrity, performance)
- Data Backup & Recovery (disaster recovery, business continuity)
- Long-term Information Security (access, crypto, authenticity)
- Defense & Intelligence (labeled storage, MLS)
- Information Lifecycle Management (ILM)

*“A ‘challenge’ is a ‘problem’ wearing a three-piece suit.”  
-- anonymous*

- Core (Applicable to Storage Systems/Ecosystems):
  - ◆ General Storage Security
  - ◆ Storage Systems Security
  - ◆ Storage Management Security
- Technology Specific:
  - ◆ Network Attached Storage (NAS)
  - ◆ Block-based IP Storage
  - ◆ Fibre Channel Storage
  - ◆ Encryption for Storage
  - ◆ Key Management for Storage
  - ◆ Long-Term Information Security

- **Risk:** If an attacker can get management access to your SAN, it's not your SAN anymore!
- **Mitigations:**
  - ◆ Compliance with authentication and authorization requirements
  - ◆ Appropriate segregation of management traffic
  - ◆ Use of secure channels for all remote management
  - ◆ Audit logging with full traceability of all privileged user actions
  - ◆ Configuration management practices
  - ◆ Protections against indirect attacks from IT infrastructure
  - ◆ Appropriate controls and monitoring of vendor maintenance
  - ◆ Consistent controls on in-band and out-of-band management
  - ◆ Protections against malware

- **Risk:** iSCSI is a storage protocol BUT it runs over a TCP/IP network!
- **Mitigations:**
  - ◆ Network based protections to establish risk domains
  - ◆ Use of entity-based, mutual authentication (CHAP) for all iSCSI initiators and targets
  - ◆ Appropriate segregation of iSCSI traffic for security and performance
  - ◆ Use of IPsec to ensure in-flight confidentiality of sensitive data
  - ◆ Protections against indirect attacks from IT infrastructure

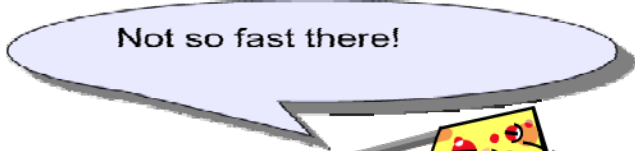
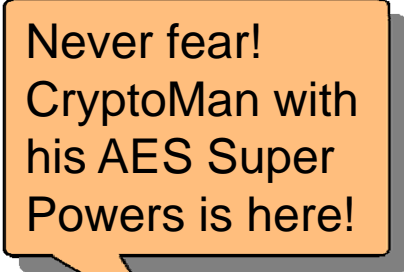
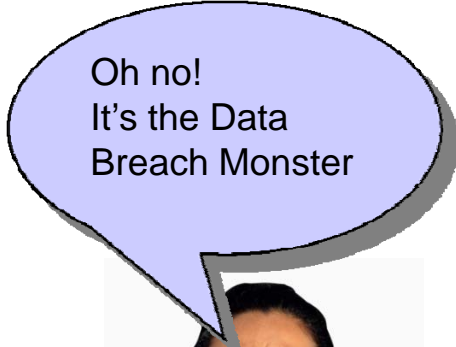
- **Risk:** Unauthorized disclosure when data/equipment/media reaches end of life.
- **Mitigations:**
  - ◆ Mechanisms that actually clear the data residing on the media
    - › Recommendations in NIST SP800-88
  - ◆ Performed in compliance with a data sanitization policy
  - ◆ Sanitization does not violate laws, regulations, or court orders
    - › Is there a discovery request or a preservation order for this data?
  - ◆ Sufficient controls to ensure the mechanisms are not attack vectors
  - ◆ Use of “crypto shredding” factors in the strength of the ciphers
  - ◆ Applied to all copies of data residing in backups, at BC/DR sites, in system caches, application caches (e.g., search engines), device mirrors, etc.



# Encryption



# A Modern Fable



# Poor Key Management

- ▶ A laptop with 700 gazillion customer records was stolen
- ▶ Yes with AES-256
- ▶ On a PIN-protected USB dongle in the same bag as the laptop
- ▶ Was the data encrypted?
- ▶ Where was the key?
- ▶ So the data is really only protected by a 4-digit PIN on the dongle



- **Well-implemented** cryptographic tools and processes are **quite valuable** in controlling certain risks to your information assets
- **Cryptography, however, is not** a magic talisman
  - ◆ “If you think cryptography is the solution to the problem [of information systems security], you understand neither cryptography nor the problem.” *Assessing and Managing Security Risk in IT Systems* by Laurie Kelley and John McCumber, pp. 115-116.
  - ◆ Use it wisely
  - ◆ Use it well



**Check out SNIA Tutorial:  
ABC's of Encryption**

- Encryption for Storage
  - ◆ Protect Externalized Data
  - ◆ Pedigree of Encryption
  - ◆ Risk Assessment in Use of Encryption
  - ◆ Encryption Issues
  
- Key Management for Storage
  - ◆ Key Management Principles
  - ◆ Key Management Functions
  - ◆ Key Management Issues

- **Risk:** Data Leaving Your Control
- **Mitigations:**
  - ◆ Data stored on removable media like backup tapes, must be encrypted while at-rest
  - ◆ Data stored in third-party (untrusted) data centers must be encrypted both in-flight and at-rest
  - ◆ Data transferred between “trusted” data centers must be encrypted in-flight

- Please send any questions or comments on this presentation to SNIA: [tracksecurity@snia.org](mailto:tracksecurity@snia.org)

**Many thanks to the following individuals  
for their contributions to this tutorial.**

**- SNIA Education Committee**

**Richard Austin, CISSP**

**Eric Hibbard, CISA, CISSP**