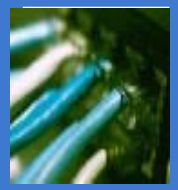



A Design and Security Roadmap Presentation

Ten Ways to Reduce Risk

Ron Shuck, CISSP, CISM, CISA
Director Information Security Services
ron.shuck@sktcompanies.com

ISSA™ Information Systems Security Association — Central Plains Chapter

Agenda

- Security Basics.
- Why Security Matters.
- What is Risk.
- Ten Ways to Reduce Risk.

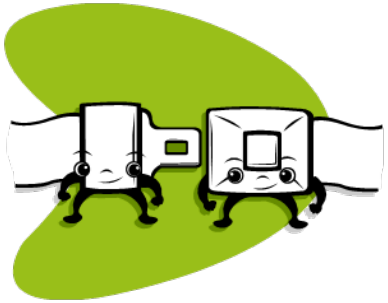
What is Security?

- **Hardware**



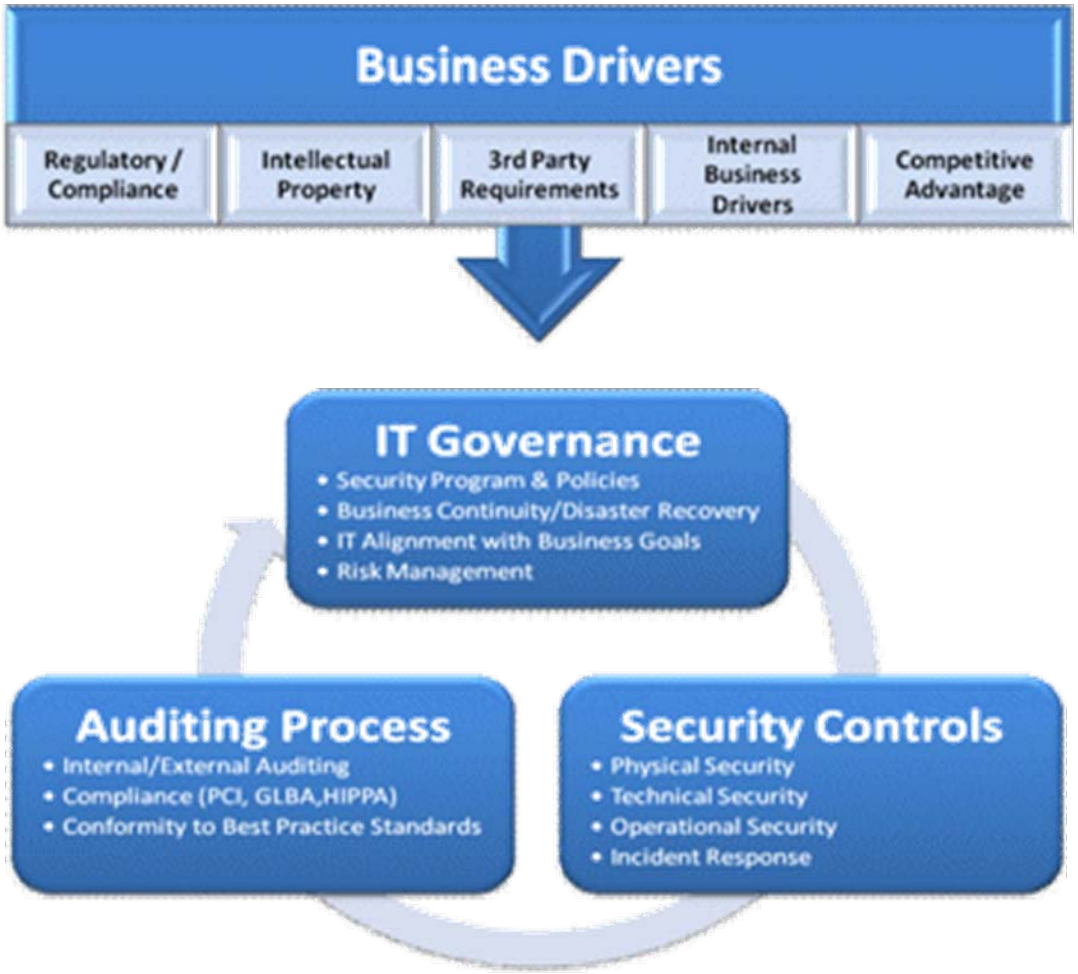
- **Security Policy**

- **Security Infrastructure**

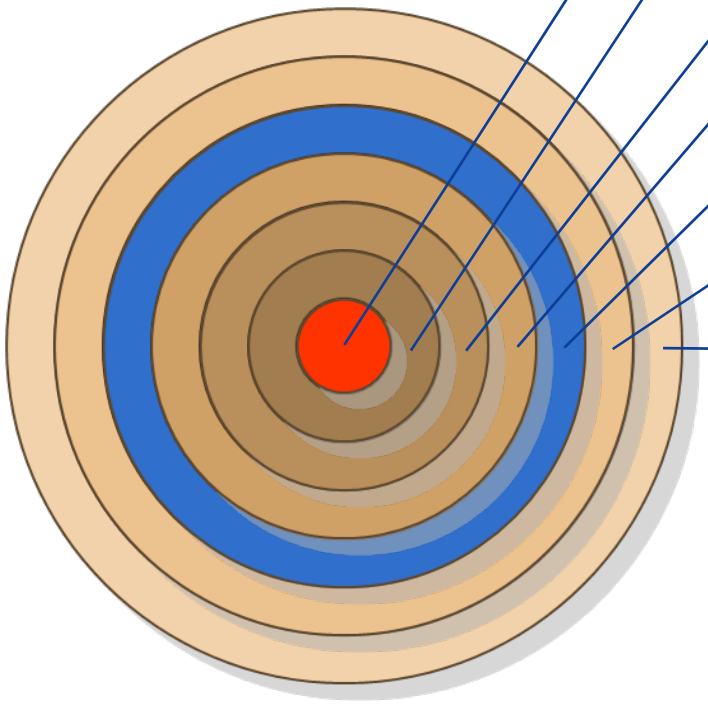



Security Triad

Security Process



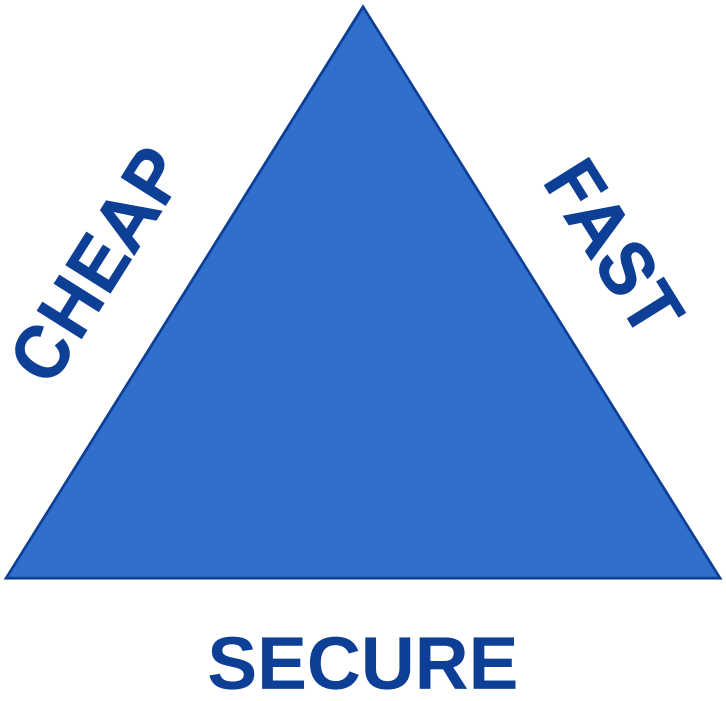
Layered Security Approach



- **Assets**
- **Policies / Procedures**
- **Physical Security**
- **Firewall / IDS**
- **Logging / Auditing**
- **Multiple Authentication Levels**
- **Data Encryption / Hiding**

Security Catch-22

Pick Two



Why Security Matters

Regulation & Legislation

- **1991 U.S. Federal Sentencing Guidelines**
  - Prudent Man Rule - requires senior officials use "due care" or "reasonable care" that ordinary, prudent people would exercise. Made degree of punishment related to due diligence.
- **1994 U.S. Computer Abuse Amendments Act**
  - Included concept of damage done with "reckless disregard of substantial and unjustifiable risk."
- **1996 Telecommunications Act**
  - Order and Further Notice of Proposed Rulemaking of April 2, 2007, the FCC adopted additional rules to strengthen its privacy rules by adopting additional safeguards to protect Customer Proprietary Network Information (CPNI) against unauthorized access and disclosure.
- **VISA CISP & PCI**
  - Compliance requirements for credit card processors.

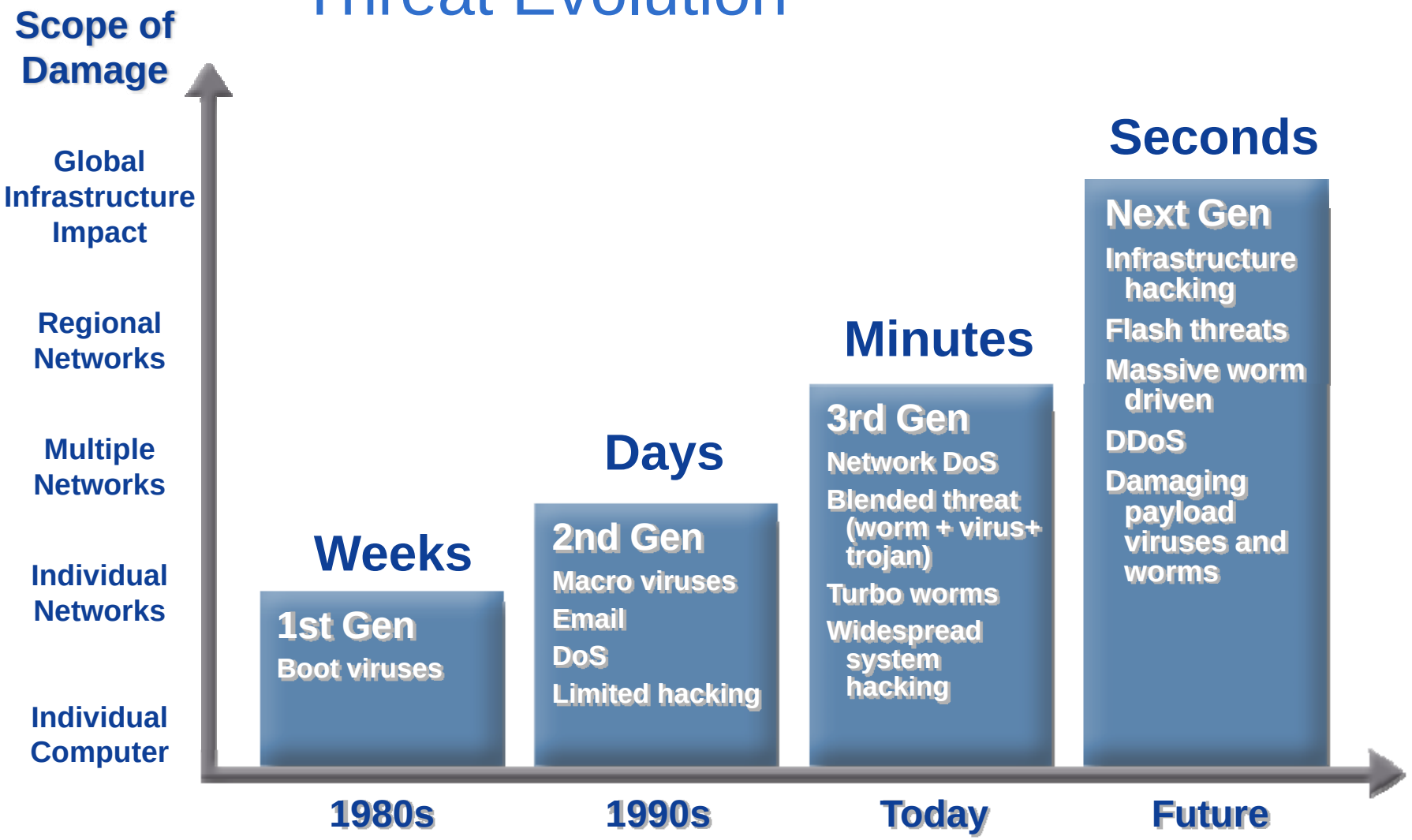
Why Security Matters

Regulation & Legislation

- **Health Insurance & Portability Accountability Act (HIPAA)**
  - Legislation related to health care industry. Primary focus to prevent unauthorized access to Protected Health Information (PHI).
- **Gramm-Leach-Bliley Act of 1999 (GLBA)**
  - Legislation related to banking industry. Primary focus to protect Non-public Personal Information (NPI).
- **Sarbanes-Oxley Act of 2002 (SOX)**
  - Legislation related to the effectiveness of internal controls over financial reporting.
- **California Information Practice Act of 2003 (SB-1386)**
  - Legislation related to personal information of California residents.
- **FCC Report & Order & Further Notice of Proposed Rule Making of April 2007 (FNPRM)**
  - Legislation related to all carriers. Primary focus to protect Customer Proprietary Network Information (CPNI).

Why Security Matters

Threat Evolution



Why Security Matters

Industry Trends

- 25% of organizations reported computer intrusions to law enforcement.
- 34% allocated > 5% of their IT budget to security.
- Over 80% of the organizations conduct security audits.
- Virus attacks(29%) continue to be the source of the greatest financial losses, followed by unauthorized access to info(20%), mobile hardware theft(12%), and proprietary info theft(11%).

* According to 2006 CSI / FBI Computer Crime and Security Survey

Why Security Matters

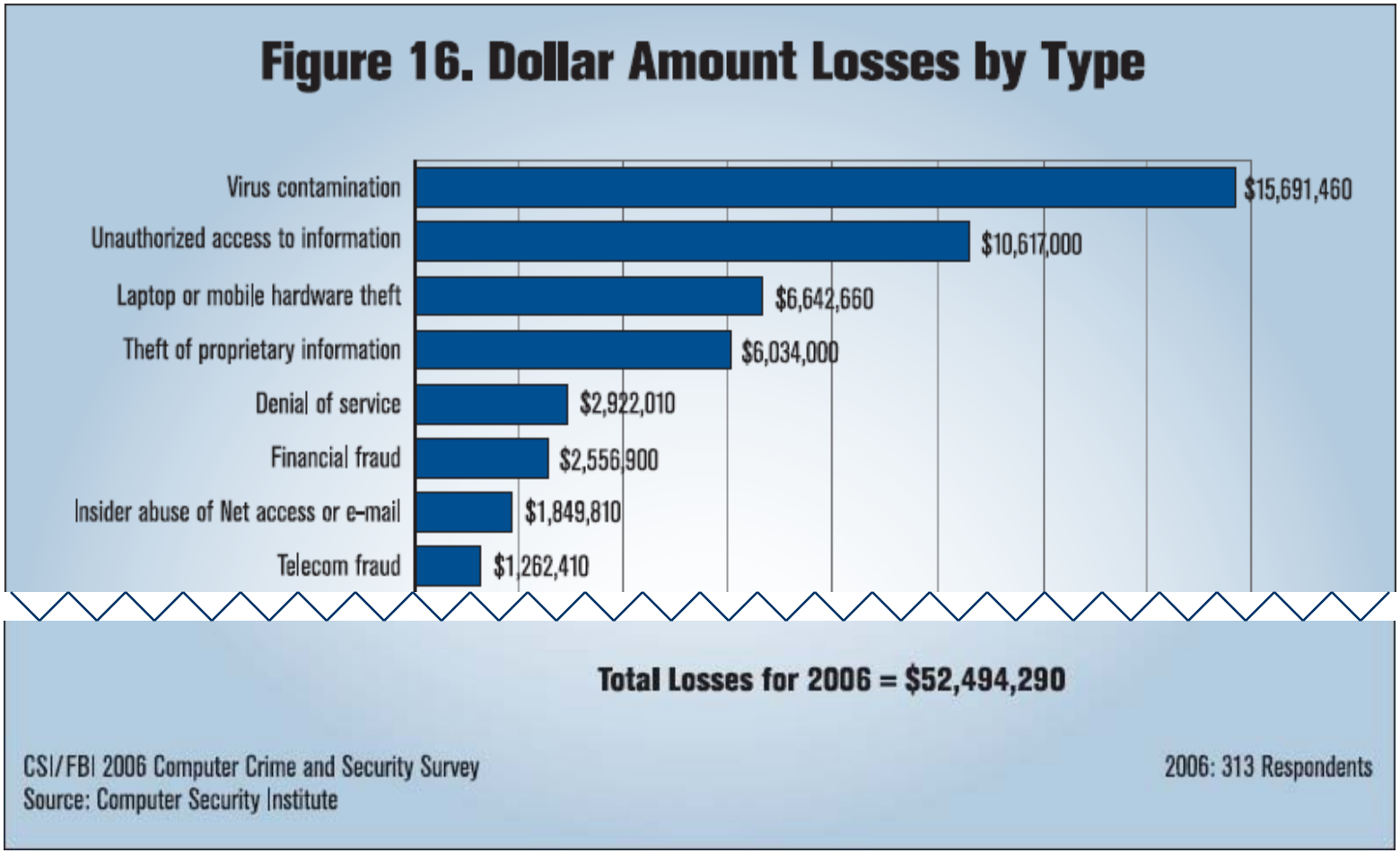
Network Complexity

Yesterday

Today

Why Security Matters

Cost



* 2006 Computer Security Institute (CSI) and FBI Computer Crime and Security Survey.

Why Security Matters

Other Reasons

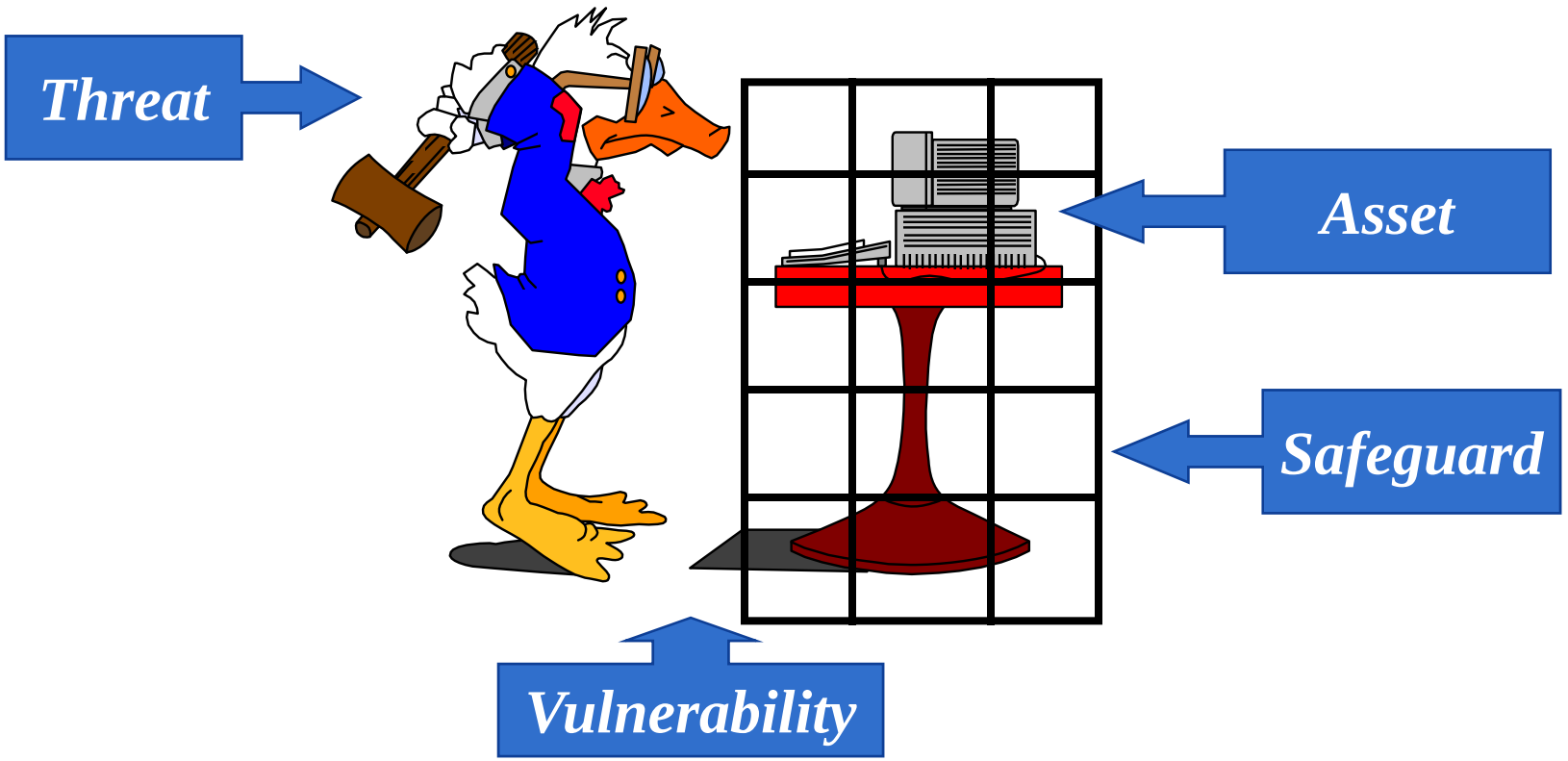
- Possible Damage to Company Reputation.
- Regulatory or Audit Compliance.
- Possible Loss of Data or Productivity.
- Limit Company Liability.
- Due Diligence (it's the responsible thing).
  - Prudent Man Rule
  - Proximate Causation
- Efficient Business Operation.

Why Security Matters

Examples

- E-mail Confidentiality.
- Information on Your PC.
- Cost of Equipment.
- Child Pornography.

What is Risk?



Ways to Deal with Risk

Ten Ways to Reduce Risk

1. Risk Assessment

- Analysis of vulnerability or risk.
- Identify assets, threats, and safeguards.
- A step in the risk management process.
- Key step in DR/Business Continuity.
- Involves review of
  - Systems & Documentation.
  - Policy & Procedure.
  - Vulnerability Scan.

Ten Ways to Reduce Risk

1. Risk Assessment

- Quantitative based on risk formulas.
- Qualitative based on general terms.
  - High, Medium, Low.
- Risk Assessment adds the identification of the potential and probability for loss.
- Prioritize risk and mitigation measures.
- Build security into new projects.
- Periodic Review and Assessment.

Ten Ways to Reduce Risk
2. Policy

- Solid policy foundation is a must.
  - General Security Policy.
  - Acceptable Use.
  - Password.
  - Remote Access.
  - Electronic Monitoring.
  - Data Retention.
  - Incident Response.
  - Media Disposal.
  - Data Classification.

Ten Ways to Reduce Risk

3. Perimeter Security

- Firewall.
  - Enterprise Class.
  - Application Inspection.
  - Egress Filtering.
  - Remote Access Virtual Private Network (VPN).
- Intrusion Detection / Prevention (IDS/IPS).
  - Network Based.
  - Signature, Behavioral, Anomaly.
  - Tuning and Monitoring are key.

Ten Ways to Reduce Risk

3. Perimeter Security

- Anti-Spam.
  - Appliance vs. Managed Service.
  - Mail (SMTP) Relay.
  - Malware protection.
- Email Encryption.
  - Digital Certificates and PKI.
  - Secure Email Portals.
  - Hosted solutions.

Ten Ways to Reduce Risk

4. Endpoint Security

- Centrally Managed Anti-Virus.
  - Monitor & enforce compliance.
- Anti-Spyware.
  - Centrally managed.
  - Host based.
  - Also can be at the perimeter.
- Laptop Drive Encryption.
  - Protect data in event of theft.
- Host based Intrusion Detection / Prevention.

Ten Ways to Reduce Risk

5. Patch Management

- Keep current on security patches.
- Major source of vulnerabilities.
- Management Systems.
  - Software Update Services (SUS).
  - Systems Management Server (SMS).
- Vulnerability Management.
  - Auditable verification of patch management.
  - Automated rapid identification of vulnerable systems to minimize administrative effort.

Ten Ways to Reduce Risk

6. Security Monitoring

- Security Information Management.
  - Event correlation between different devices.
  - Reduces administrative burden of log monitoring.
  - Decreases response time to threats.
- In-house vs. outsourced.
- Provides auditable data of the organizations security stance in an easy to generate and interpret report.

Ten Ways to Reduce Risk

7. Backup & Recovery

- Design a comprehensive backup strategy for all critical systems.
- Routinely verify data can be restored from backups.
- Secure backup media in a secure location.
  - Secure in vault away from primary data center.
  - Store in locked container in vault.
  - Tape encryption provides protection of data when in transit and at rest.
- Limit tape handling to trusted staff and use logging sheets for all tape movement.

Ten Ways to Reduce Risk

8. Disaster Recovery

- Disaster Recovery vs. Business Continuity.
  - Recover from a Disaster.
  - Continue business operation during disaster.
- Risk Assessment.
- Business Impact Analysis.
  - Identify Critical Resources.
  - Identify Outage Impacts & Max Time Down (MTD).
  - Develop Recovery Priorities & Requirements.
- Plan Creation.

Ten Ways to Reduce Risk

9. WiFi / New Technology

- Wireless (WiFi) Security.
  - Use secure wireless protocols (WPA/WPA2).
  - Use professional grade equipment installed and audited by experts.
  - Routine physical & electronic sweep for rogue access points.
- Stay informed on new technology
  - USB Drives (U3).
  - Instant Messaging (IM).
  - Voice over IP (VoIP) & Skype.

Ten Ways to Reduce Risk

10. Awareness Training

- Provide yearly security awareness training.
  - Can be tied in with required yearly physical security awareness training.
- Develop a meaningful security awareness program.
  - Develop fun employee newsletter articles.
  - Develop formal training that relates to both the employee's home and work computers.
- Keep materials in layman terms, but don't insult peoples intelligence.
  - Key policy items especially acceptable use.
  - Email security.
  - Counter social engineering
  - Password security.

Strategic Partnerships

- Build Security into Solutions.
- Build Strategic Partner Solutions.
- Build Strategic Client Relationships.
- Understand Your Business.
- Understand Security Issues and Risks.
- Understand “NO” is Not the Answer.

Subject Matter Experts

- Certified Information System Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- GIAC Certified Intrusion Analyst (GCIA)
- Cisco Certified Security Professional (CCSP)
- Cisco Certified Voice Professional (CCVP)
- Cisco Certified Network Professional (CCNP)
- Microsoft Certified Systems Engineer (MCSE)
- GIAC Certified Windows Security Administrator (GCWN)
- Check Point Certified Security Expert (CCSE)
- VMWare Certified Professional (VCP)
- Cisco Certified Design Associate (CCDA)

Core Services and Solutions

Business Analysis • Security Consulting • Project Management
Process Improvement • Technology Assessment • IT Management

- Email and Collaboration Systems
- Database Administration
- Storage Solutions
- Server Virtualization
- Application Management and Deployment
- Architecture Design & Migration
- Mobility

- IP & Legacy Telephony
- Wide Area Networking
- Information Security
- Wireless
- Network Health and Performance Monitoring
- Datacenter Services

EMC² where information lives | VMware VIP Enterprise Partner | Microsoft Gold Certified Partner | Cisco Systems Premier Certified Partner | Citrix | Check Point | RSA | BioPassword | Barracuda Networks

ISSA Information Systems Security Association — Central Plains Chapter

Ten Ways to Reduce Risk

Questions