


Essentials of Information Security for Netcentric Organizations

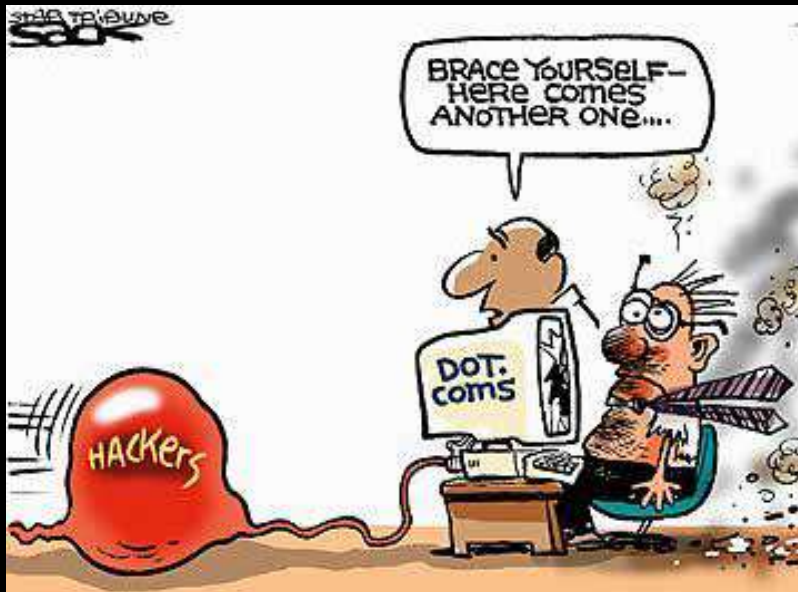


Sunil Hazari

Robert H. Smith School of Business
University of Maryland

<http://www.sunilhazari.com/education>

Seminar Agenda



- Security Infrastructure
- Risk Management
- Info. Sec. Policies
- Usability
- Future
- BMGT727 Pedagogy

Financial Impact of System Failure

(Average Hourly Cost by Type of Application)

- Brokerage Operations **\$ 6.5 million**
- Credit Cards/sales **\$ 2.6 million**
- TV Home shopping **\$ 113,000**
- Catalog Sales **\$ 90,000**
- Airline reservations **\$ 89,500**
- Package Shipping **\$ 28,000**
- ATM fees **\$ 14,500**



Information Security

PKI

Smart Cards

Access Control

LAN/WAN Security

Biometrics

Database Security

Penetration Testing

Digital Forensics

Certificate Authority

Client/Server Security

Virus Protection

Auditing Content Filtering

Encryption

E-commerce

Crypto Toolkits

Enterprise Security

Firewalls

Intrusion Detection

Wireless Security

Policies

Security Strategy

Network Security

- Online = At-risk
- Technology Solutions
- Risk Assessment
- Policy Development



*Balance risk of losing information versus
overly aggressive security solution*

Security Infrastructure

- Technical, organizational, psychological foundations on which required level of security is built and maintained.
- Components:
 - Technology (e.g. PKI)
 - Management commitment
 - Security mission statement
 - Policy Framework
 - Training and Education



Security Strategy

- Identify threats
- Assess degree of vulnerability
- Implement countermeasures
- Auditing safeguards and compare with best practices
- Associated costs



A false sense of security is worse than a true sense of insecurity

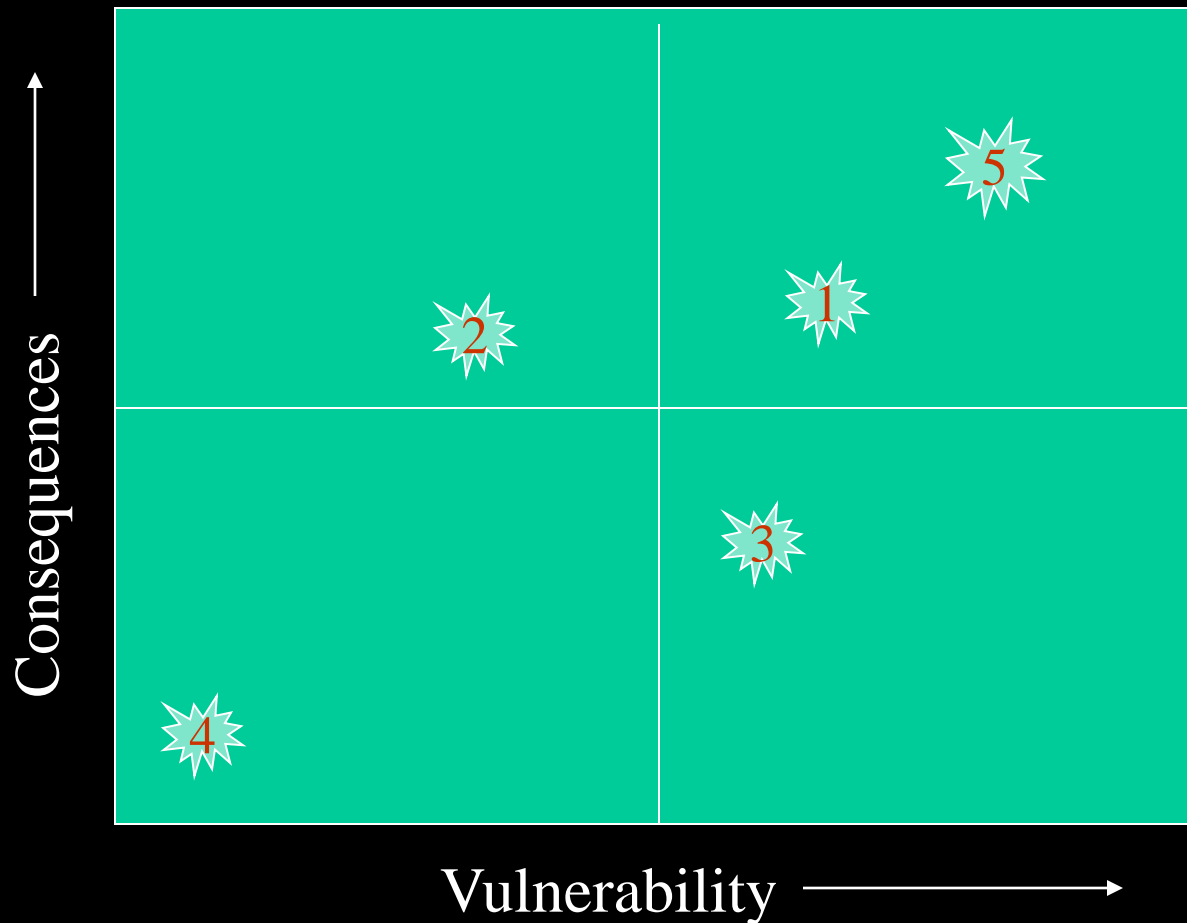
Risk Assessment & Management

- Analysis of what may happen to network assets AND impact on business objectives
- Plan designed at enterprise level to mitigate risks



The cost of protecting against a threat should be less than the cost of recovering if the threat were to strike

Risk Management



$$\text{Risk} = (\text{Threat} * \text{Vulnerability}) - \text{Countermeasures}$$

Public Key Infrastructure



- Issuing and managing certificates for the purpose of authentication, encryption, and digital signatures
- Goal: Design technical architectures, policies and organizational structures that meet interoperability needs of multiple entities

Will PKI address my business requirement for increased security?

Standards



- BS7799 (ISO 17799)
 - Best Practices
 - Std. Specification for Info Sys Mgmt.
 - Certification
- Visa (U-commerce)
 - Best Practices
 - Data Security Standards

InfoSec Policies

- Employees: "Policies are a nuisance and infringe on our privacy"
 - Management: "Policies are drain on budget & time"
-

Effective Policy Development

- Primary uses of system
- Freedom of Expression
- User Privacy
- Personal Responsibility
- State and Federal laws and regulations
- Monitoring
- Actions and Consequences

Security & Usability

- “User Interface for security products tends to be clumsy, confusing, or non-existent”
- There is a need for domain specific UI design principles and techniques.

Source: Why Johnny can't Encrypt: Usability Evaluation of PGP 5.0. Alma & Tyger (CMU)

Firewall Demo

- [Related Study] Gefen, D & Straub, D. “Relative Importance of Perceived Ease of Use in IS Adoption: A Study of E-Commerce Adoption”. *Journal of the Association for Information Systems, October 2000.*

Home Offices

Threats

- Virus
- Downloaded Software
- E-mail
- Misconfiguration
- No Backup



Hazari, S. (2000). Personal Firewalls for SOHO users.
<http://www.SecurityFocus.com>

m-Commerce



- Use of PDAs, cell-phones, wireless devices
- Transaction based wireless services
- More revenue opportunities
- Additional service to existing customers
- Example: Check e-mail, flight information, travel reservations, trade stocks, e-banking

m-Security



- Use of WAP as defacto global standard.
- WAP 1.1 defines WTLS using PKI
- Use of WAP Gateway to interface between WTLS and SSL
- Microbrowser -> **WAP Gateway** ->Server
- Divergent Standards?
(WAP 1.x, Microsoft/Qualcomm, Palm)

Implementation

- Chief Information Security Officer
- Security policies holistically defined
- Buy-in from all business units
- Effective working relationship between IT and other units
- Use open standards
- Think ahead !!



BMGT 727 Pedagogy



- Lecture
- In-class Discussion
- Online Discussions
- Streaming Video
- Simulations
- Group Presentations
- Research Paper