E-Commerce & Web Servers

CSH6 Chapter 30

"E-Commerce & Web-Server Safeguards"

Robert Gezelter

Topics

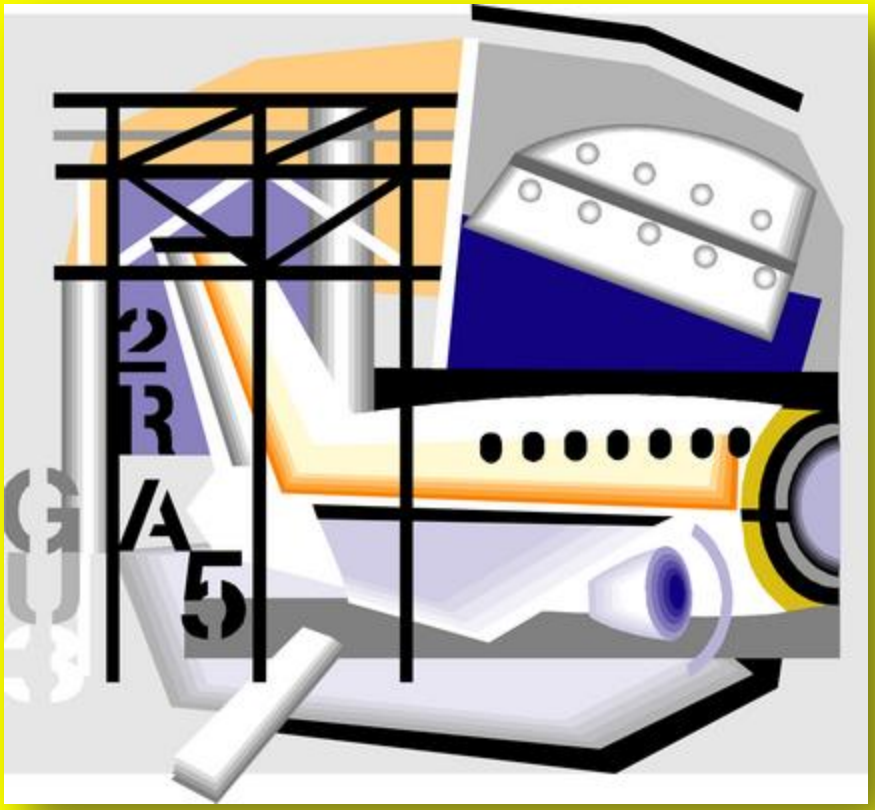
- Introduction
- Business Policies & Strategies
- Rules of Engagement
- Risk Analysis
- Operational Requirements
- Technical Issues
- Ethical & Legal Issues

VERY LONG SLIDE DECK:
USE FOR PREPARATION BEFORE AND REVIEW AFTER READING ENTIRE CHAPTER.

Introduction

- E-commerce becoming ubiquitous
- Desire for efficiency may harm security
  - Should not use same systems for brick-and-mortar business as Web-enabled
  - Don’t use wireless access from kiosks & cash registers into accounting systems
- TJX case (2007) early example
  - Inadequately secured corporate network & back-office systems hacked by criminals
  - Breach compromised >94M credit cards
  - Payouts of $40.9M in damages

Business Policies & Strategies



- Best practices evolve constantly
- Must consider & secure B2C & B2B systems
- Framework proposed:
  1. Define Information-Security Concerns
  2. Develop Security-Service Options
  3. Select Security-Service Options
  4. Ensure Ongoing Attention to Changes
- Using Security Services Framework
- Framework Conclusion

B2B = business-to-business

B2C = business-to-customer

1. Define Information Security Concerns

- Study impact of security breaches on business
- Use transactional follow-the-flow diagrams
  - Tracks transactions & data through servers & networks
  - Functional & logical view (what happens & how)
  - Identify data sources, interfaces
  - Define processing (changes)
  - See Exhibit 30.1 (p 30.4) as example

Define Information Security Concerns (2)

Usually have to study and include

- Clients
  - PCs, thin clients, PDAs, WAP-compliant phones
- Servers
  - Web, application, DB, middleware, back-end
- Network devices
  - Switches, routers, FW, network interface cardsd (NICs), codecs, modems, hosting sites
- Network spaces
  - DMZs, intranets, extranets, Internet

2. Develop Security Service Options (1)

- Consider possible security options for each component and all data types
- Factors affecting requirements
  - Industry
  - Company's tolerance for risk
  - Maturity of security group/function
  - Organizational structure ([de]centralized)
  - Past security incidents
  - Internal organizational issues
  - Politics
  - Regulations
  - Perceived strategic value of INFOSEC

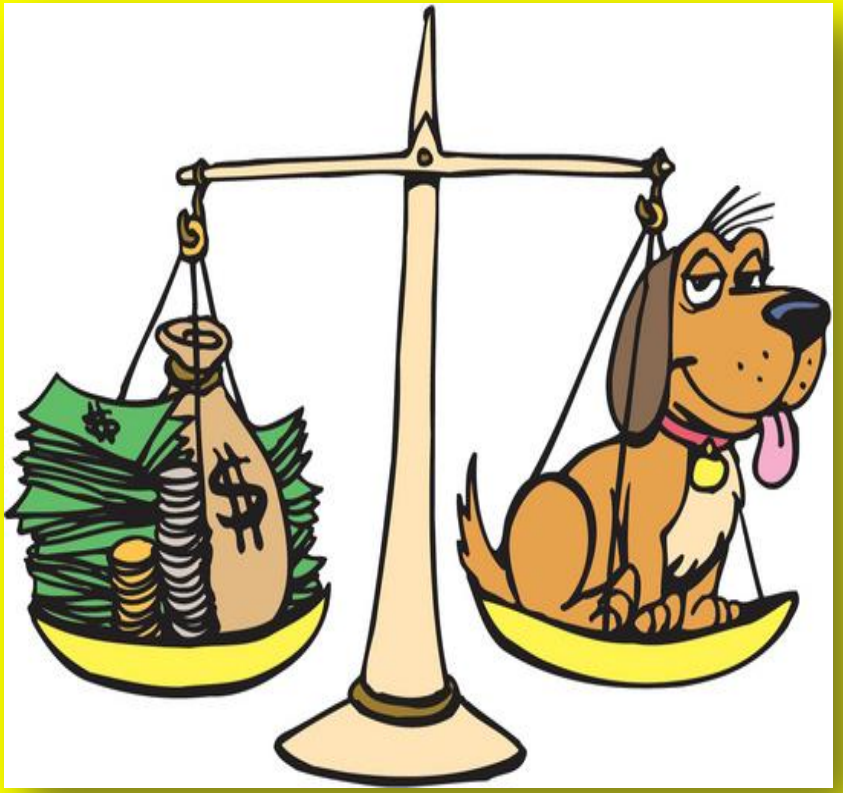
Develop Security Service Options (2)

Services to consider include

1. **Policy & procedures**
2. **Confidentiality & Encryption**
3. **Identification & Authentication**
4. **Authorization**
5. **Authenticity**
6. **Monitoring & Audit**
7. **Access Controls & Intrusion Detection**
8. **Trusted Communication**
9. **Antivirus**
10. **System Integrity Controls**
11. **Data Retention & Disposal**
12. **Data Classification**

3. Select Security Service Options

- Cost-benefit & risk-management analysis
  - ❑Final selection of security service options
  - ❑Distribute along continuum of importance
    - ✓See Exhibit 30.2, p 30.8
- Four additional factors in option selection
  1. Implementation risk or feasibility
  2. Cost to implement & support
  3. Effectiveness in increasing control
  4. Data classification



Implementation Risk or Feasibility

- Feasibility of implementing option
- Factors affecting ease of implementation
  - Product maturity
  - Scalability
  - Complexity
  - Supportability
  - Skills available (capabilities, prior experience)
  - Legal issues
  - Integration required
  - Limitations of technology

Cost to Implement & Support

- HW & SW
  - Implementation
  - Support
  - Administration
- High-level support of security service vital to success

Effectiveness in Increasing Control

- Reduction of risk
  - Impact & likelihood of harmful event
  - Compare before & after implementation of security service / mitigating strategies
- Example: theft of credit-card #s from DB
  - Losses to consumers (data subjects)
  - Negative public relations
  - Decrease future business

Data Classification

- Criticality & sensitivity of information
- Protection against
  - Misuse
  - Disclosure
  - Theft
  - Destruction
- Throughout lifecycle
- Creator usually considered responsible
  - Classification
  - Identification
  - Labeling

4. Ensure Ongoing Attention to Changes

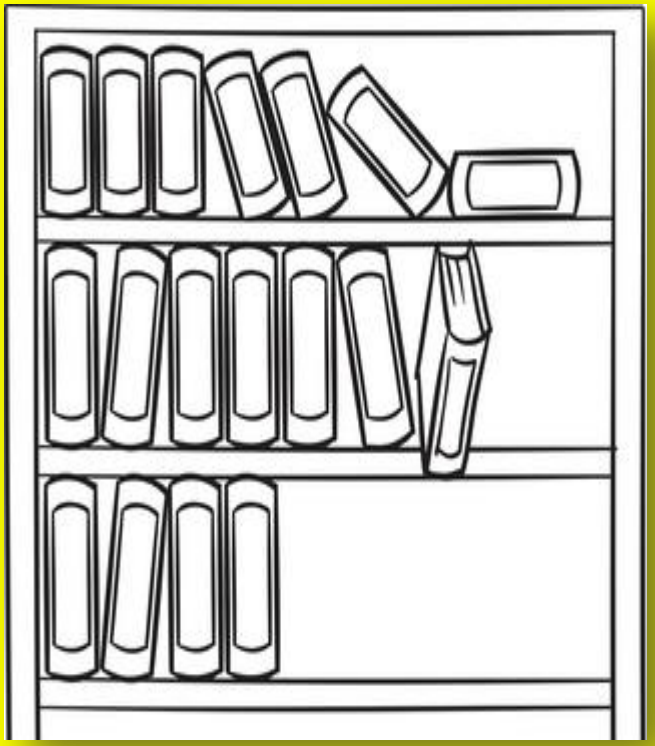
- Threats evolve
  - Therefore defenses must evolve
- Changes inevitable
  - Compliance
  - Regulation
  - Technological advances
  - New attacks
- "Security is a process, not a product."*
  - … or a static end-state

---

* Schneier, B. (2000). "Computer Security: Will We Ever Learn?" *Crypto-Gram Newsletter* (May 15, 2000).
< http://www.schneier.com/crypto-gram-0005.html#1 >

Using Security Services Framework

- Detailed examples of analyses are provided in text for
  - B2C Security Services
  - B2B Security Services
- However, these examples are not discussed in this slide presentation
- Will serve as examples for reader's / student's own analyses
- Case studies may be used as basis for exam questions; e.g., "Using the case studies in Chapter 30, analyze the different security requirements for Norwich University's public Web site (www.norwich.edu) and for its intranet site (my.norwich.edu)"



Rules of Engagement

- Web Site-Specific Measures
- Defining Attacks
- Defining Protection
- Maintaining Privacy
- Working with Law Enforcement
- Accepting Losses
- Avoiding Overreaction
- Appropriate Responses to Attacks
- Counter-Battery
- Hold Harmless

Website-Specific Measures

- Website may be most important element of interaction with outside world
  - High availability: 24x7x365 due to expectations & potentially worldwide market
  - Accuracy and confidentiality required
  - Perturbations may profoundly affect customers, cash flow, long-term reputation
- Most Website problems caused by inside technical glitches, not glamorous hacker attacks
- External events can wreak havoc; e.g., 9/11
- Best practices & scale important
  - Small organizations may succeed with less formal solutions than large ones

Defining Attacks

- Large numbers of repeated attempted connections may be attack – or not
  - Customer with technical problem
  - Problem on network
  - Attack on server

Defining Protection

- Web sites ⊂ Internet-visible assets
  - Internet-visible not intended for public use
    - ✓Easier to anticipate usage, traffic
  - Web site activity varies
    - ✓Potentially worldwide public
    - ✓Surge could be due to attack or to popularity
- Some protective measures have unexpected consequences; e.g.,
  - Requiring visitor computers to have entry in inverse DNS instead of only DNS
  - But not all legitimate sites have inverse DNS entries
  - Becomes a policy issues, not just technical

⊂ means "proper subset" (*part of* but *not the whole*)

Maintaining Privacy

- Logging interactions
  - Privacy policy
    - ✓Managerial
    - ✓Legal
    - ✓Customer relations
  - Technical staff must respect laws, regulations
- Always consult corporate privacy policy
- Discuss with corporate counsel if necessary

See *CSH6* Chapter 69 Privacy in Cyberspace: US & European Perspectives

Working with Law Enforcement

- Complexity depends on type of attack
  - Frauds easier than attacks
  - Attacks require more consideration of policy
- Status of Website
  - Easier: Local server in control of organization
  - Harder: server at hosting facility
  - Hardest: server owned by third-party
- What information can / should be logged?
  - When?

See *CSH6* Chapter 61 Working with Law Enforcement

Accepting Losses

- Security breaches should be prepared for as if inevitable despite best efforts of all
  - Increasing complexity of site content
  - Growing application code
- Reaction plans important
  - Similar to discussion of Web-based vulnerabilities
  - Difference is greater effect on customers
  - Prepare & refine computer security incident response team and plans

See *CSH6* Chapter 21: Web-Based Vulnerabilities & *CSH6* Chapter 56: Computer Security Incident Response Teams

Avoiding Overreaction

- Some reactions may cause more problems than attack
- Define decision-making authority & guidelines
- Decide *in advance* what conditions will force Website to be taken offline
- Key principles:
  - Defensive actions almost always permissible
  - Offensive actions of any kind almost always impermissible
  - Transparency (invisibility) to customer best

Appropriate Responses to Attacks

- International law recognized attacks on naval vessel = act of war
  - Fire if fired upon
  - Similar rules give citizens right to defend themselves in absence of law enforcement personnel
  - "Rules of engagement"
- Information technologists do not have legal standing for counterattack
  - Focus on appropriateness to situation
    - ✓Political, legal, business issue
    - ✓Policy, legality, public relations, feasibility
    - ✓National security vs private property

Counter-Battery

- Targeting system that has attacked
- But counter-battery is illegal in most jurisdictions
  - No legal standing for attack against a computer system
- Practical problems
  - Malefactor may not be correctly identified
  - Effects of attack may spill over to innocent victims
- Example: Canter & Siegel (1994)
  - Spammers in Arizona (2 lawyers)
  - Retaliation (protest e-mails) crashed their ISP servers
  - Innocent victims: customers of spammers' ISP

Hold Harmless

- Need fast responses
- Employees must be protected against retaliation
  - Acting in good faith
  - According to responsibilities
  - Within documented policy & procedures
- Errors
  - Lead to procedural correction
  - Not punishment of individual employee

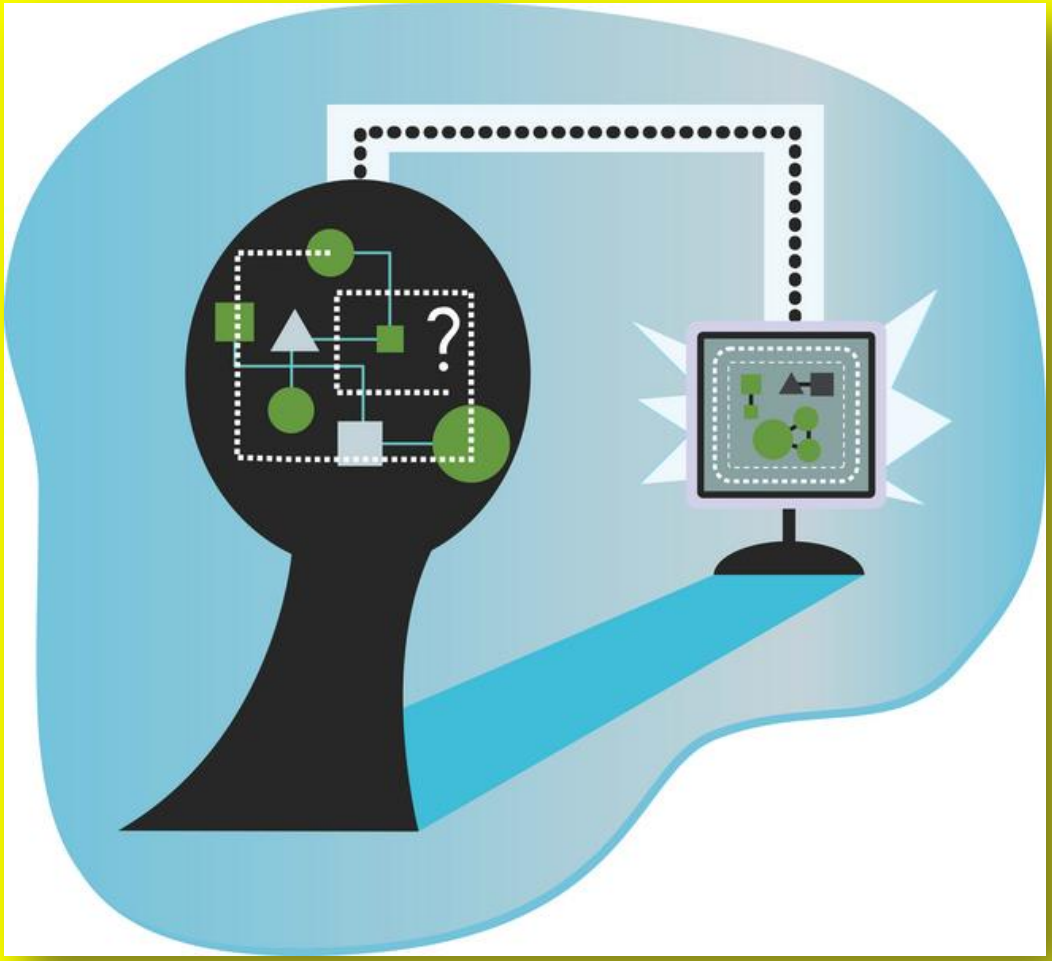
Risk Analysis

- Business Loss
- PR Image
- Loss of Customers & Business
- Interruptions
- Proactive vs Reactive Threats
- Threat & Hazard Assessment

See *CSH6* Chapter 62: Risk Assessment & Management & *CSH6* Chapter 63: Management Responsibilities & Liabilities

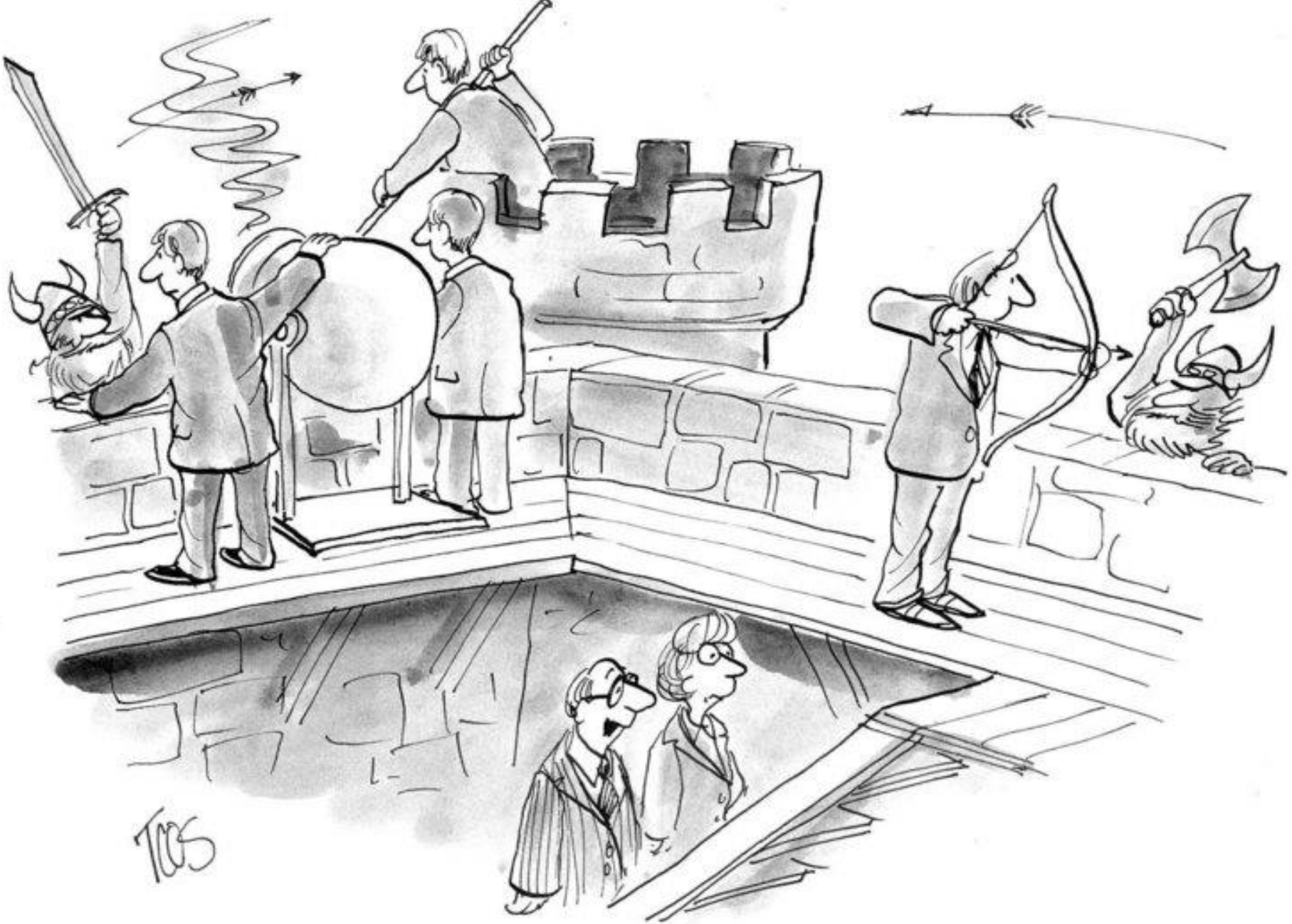
Business Loss

- ***Customers*** **should be considered as both…**
  - **Outsiders accessing Internet presence**
  - **Insiders using intranet-hosted applications**



PR Image (1)

- Web site = public face 24/7/365
  - Prime target for attack
- Many examples of hostile activity
  - US Congress “Thomas” site
  - US Dept Justice
  - Government sites around world
- Activity often surges after major public events
- Hacking contests
- Defamation by angry consumers
- Random targeting

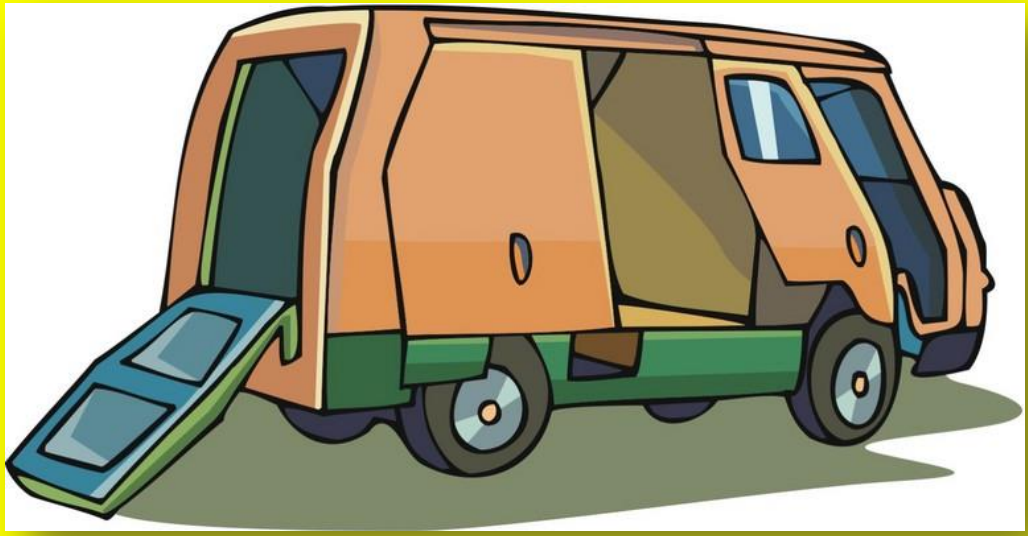


"Congratulations on the PR Director's job. Right now we have 38 lawsuits."

Loss of Customers & Business

- Internet customers highly mobile & impatient
  - May switch to competitor quickly
  - Even momentary delay may cause switch
- Competitors usually abound
- Functional degradation may cause switch
  - E.g., problems with shipment tracking

Interruptions



- Just in Time (JIT) delivery
  - Production
    - ✓Disruption may be disastrous to entire operation
  - Supply chain
    - ✓Service-oriented architecture (SOA)
  - Delivery chain
    - ✓Tracking status
- Information delivery
  - Banks, brokerages, utilities… provide services online
  - Offer reports on demand

Proactive vs Reactive Threats

- Some defensive tactics open up new potential for availability problems
- E.g., common strategy: multiple name servers for translating IP address to domain names
  - Must define ≥ 2 name servers for DNS zone
  - But updating DNS zones can cause problems
    - ✓ Error in providing name servers makes site unavailable
    - ✓ Most sites make ISP responsible for resolution of domain names
      - Increases complexity of architecture
      - Must be remembered during problem analysis & resolution

Threat & Hazard Assessment

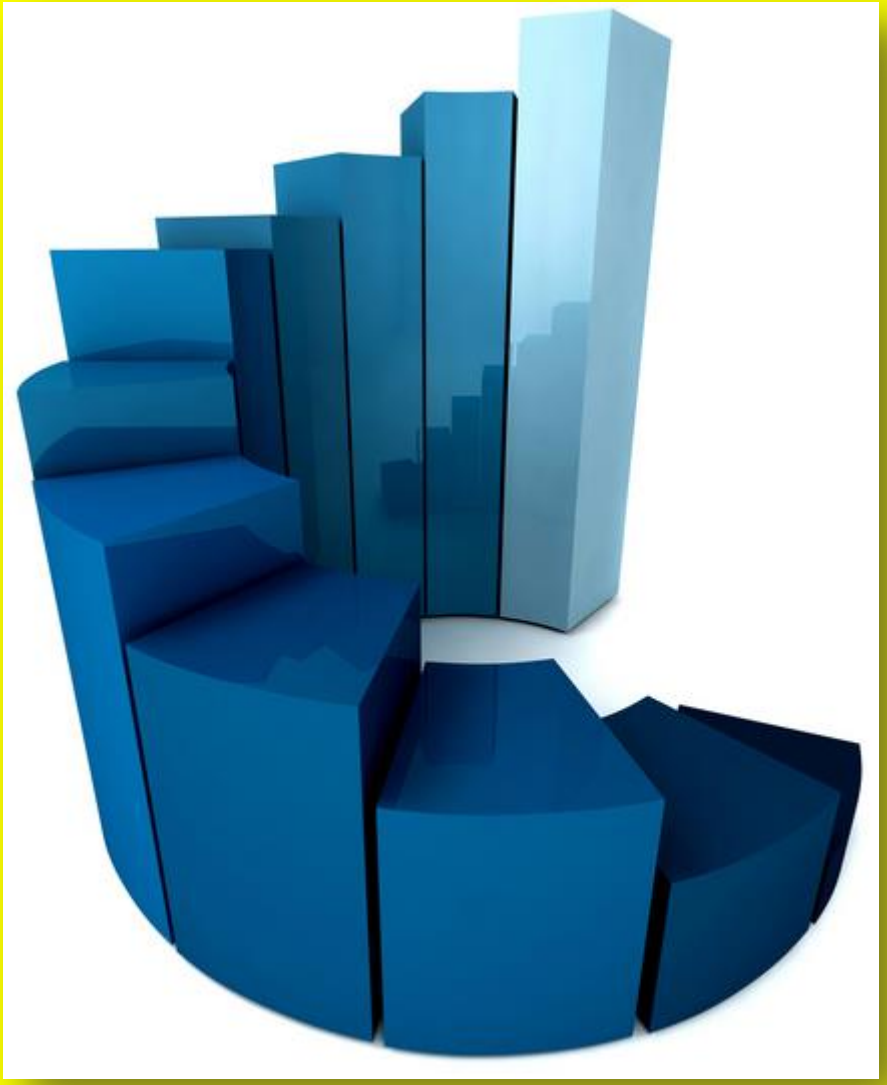
- Threats may be universal or specific
- Threat analysis
  - Deliberate vs accidental
    - ✓Acts of G-d
    - ✓Acts of clod
  - In risk analysis & planning, deliberate attacks may be equivalent to acts of G-d
- No enterprise is immune to accident or attack

Operational Requirements (1)

- Protection not purely technical issue
- Degree of exposure to Internet: risk-management issue
  - Cannot set technical solutions without business context
  - Cannot evaluate risks without knowledge of technical issues
- Outsourcing introduces additional complexity
- Protecting Web site is lifecycle process
  - Ongoing system evolution
  - Monitoring, detection, correction
  - Analysis, changes in underlying causes

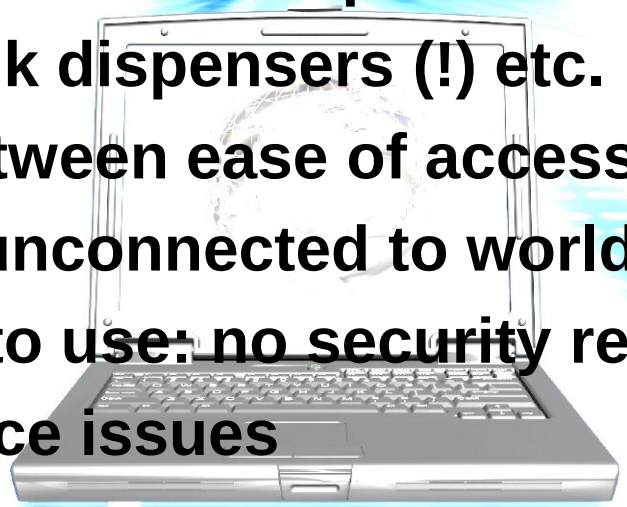
Operational Requirements (2)

- Ubiquitous Internet Protocol Networking
- Internal Partitions
- Critical Availability
- Accessibility
- Applications Design
- Provisioning
- Restrictions
- Multiple Security Domains
- What Needs to Be Exposed
- Access Controls
- Site Maintenance
- Maintaining Site Integrity



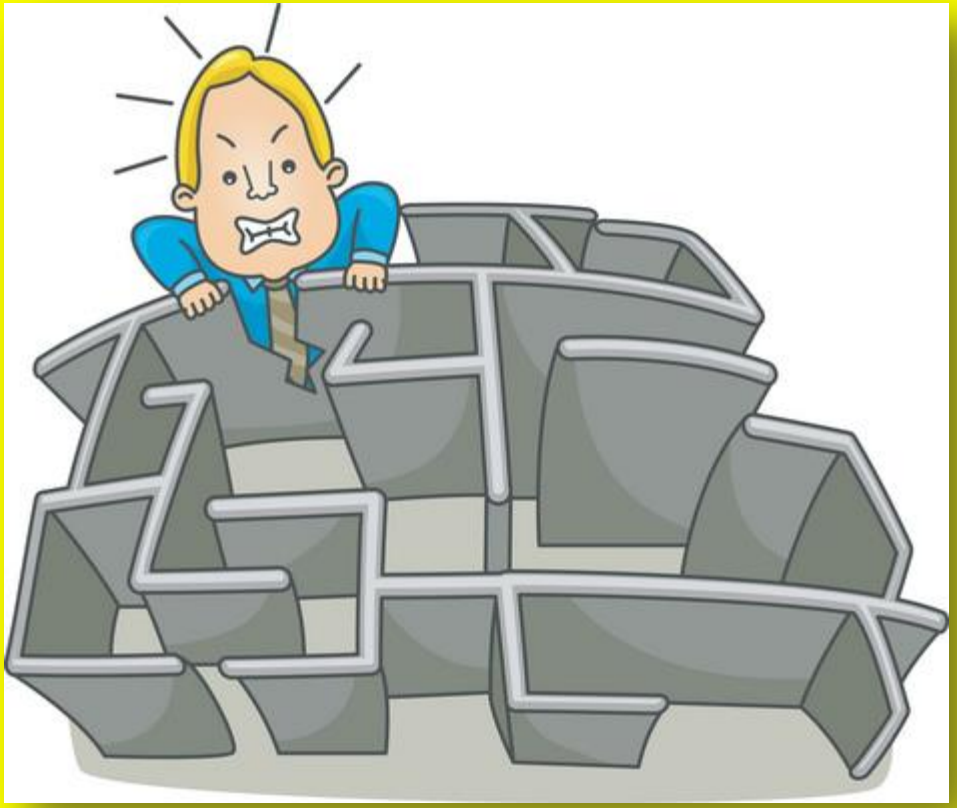
Ubiquitous Internet Protocol Networking

- Switch from locally controlled networks to Internet greatly increased exposure to attack
- Wider range of connected equipment
  - VoIP telephones
  - FAX
  - Copiers → network printers
  - Soft drink dispensers (!) etc.
- Conflict between ease of access & security
  - Safest: unconnected to world
  - Easiest to use: no security restrictions
- Must balance issues



Internal Partitions

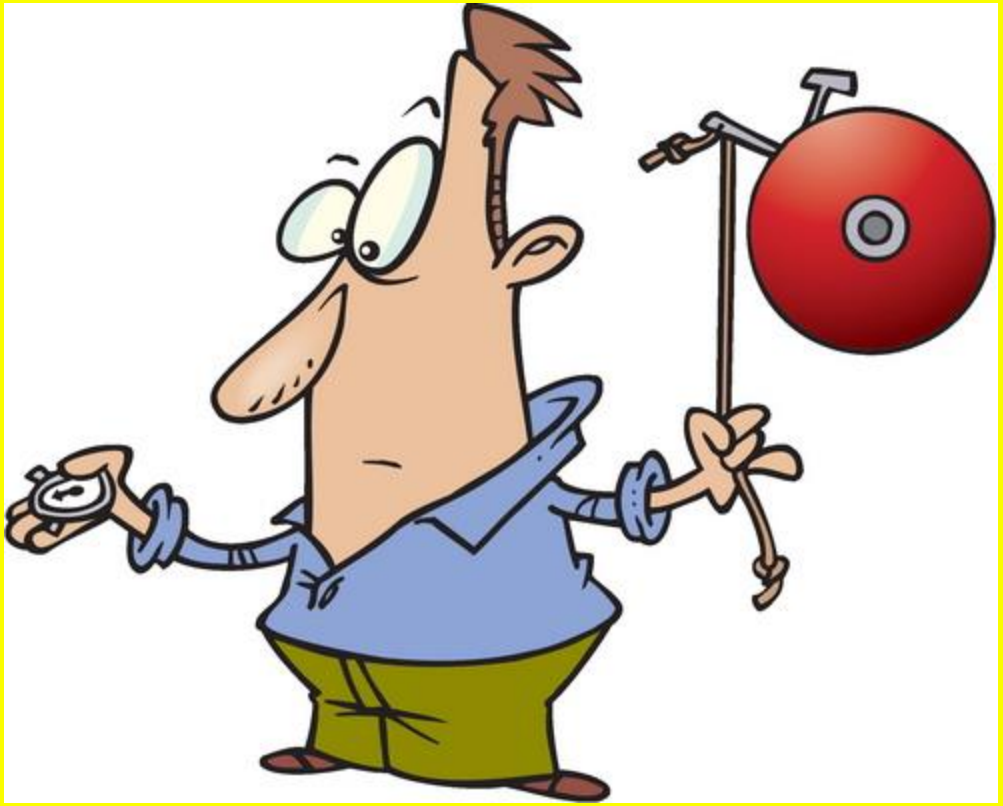
- Complex corporate environments
  - Often best protected by including partition
  - Define separate security domains
    - ✓Own legal, technical, cultural needs
    - ✓E.g., medical records, CRM, SCM, ERP
  - Often require separate policies for firewalls, access controls….
- Damage control improved by partitions
  - E.g., malware attack may be contained
  - *Defense in depth*



CRM: customer relationship management
SCM: supply-chain management
ERP: enterprise resource planning

Critical Availability

- Different sectors may have different needs for availability
  - Second-to-second (e.g., real-time production controls, SCADA)
  - Minute-to-minute (e.g., customer Web functions, Help desk)
  - Hour-to-hour (e.g., shipping, scheduling)
  - Day-to-day (e.g., line management reports, billing)
  - Week-to-week (e.g., regulatory reporting, management accounting)



- Poorly planned shutdowns can cause more problems than attack

SCADA: supervisory control and data acquisition

Accessibility

- Users must be involved in defining rules
  - But users need awareness & education
    - ✓E.g., university faculty often insist on removal of all security rules
- Some individuals & functions do *not* need Internet access for their work
  - Individuals may resent being blocked
  - But need to define business case for access or exclusion

Applications Design

- Site processing confidential information
  - Must support HTTPS
  - Typically through port 443
  - Requires valid digital certificate
- In case of uncertainty about security requirements, err on side of security
  - Enable HTTPS anyway
  - Encryption best/only way of protecting potentially sensitive traffic
- Use encryption within organization too
  - E.g., for sensitive transactions involving employee information
- Suppress display of confidential info
  - E.g., full credit-card numbers
  - Be sure not to vary in parts that are suppressed
    - ✓ Prevent inference by collecting parts from different screens

Provisioning

- Plan for disruption
- Use redundancy
- High-availability public-facing Web site may need 2 geographically separated facilities
- Evaluate degree of functional duplication required by applications / services
- Costs of unavailability may be orders of magnitude > cost of redundancy

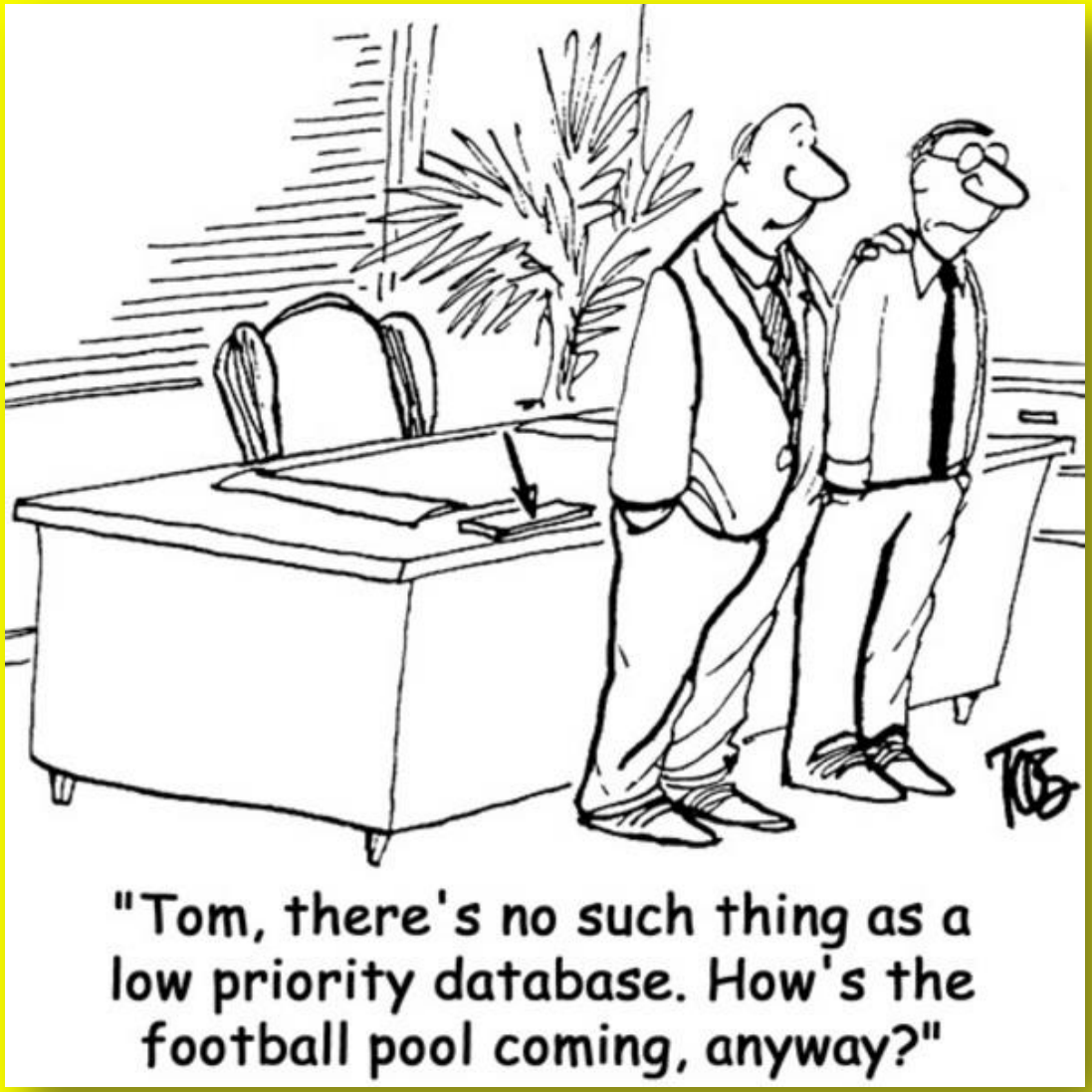
See *CSH6* Chapter 58: Business Continuity Planning & *CSH6* Chapter 59: Disaster Recovery

Restrictions

- Web servers must be behind firewall
- Incoming / outgoing services restricted using specific protocols (e.g., HTTP, HTTPS, ICMP)
- Disable unused ports
- Block disabled ports by firewalls
- Store customer information on separate systems (not Web server)

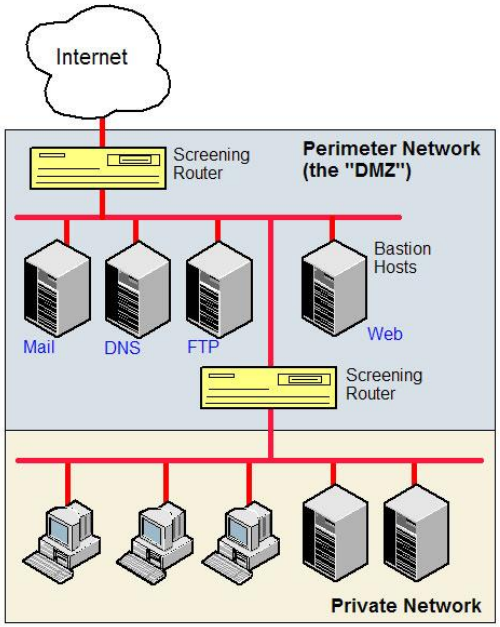
Multiple Security Domains

- Web servers ≠ database servers
- Link Web server to DB
  - Dedicated & restricted-use protocol
  - Prevents hijacked Web server from allowing access to DB
- Segregate DB servers behind additional firewalls



What Needs to Be Exposed (1)

- Despite public access to Web server, must prevent exploitation for subversion
- All connections to Internet go through firewall
  - Firewall restricts traffic to Web-related protocols only
- DMZ: demilitarized zone (devices with firewalls in front of and behind them)



The DMZ

All servers exposed to the Internet (the bastion hosts) are located in the DMZ, which is isolated from the public Internet and the private LAN by screening routers.

What Needs to Be Exposed (2)

- Exposed systems
  - Minimize
  - Consider roles, not just machines
  - May prefer to have several different servers rather than one larger server
    - ✓Impact of downtime grows
  - But new trend of virtualization pushes towards single server with multiple functions

- Hidden Subnets
  - Hide servers *supporting* Web site from visibility
  - Can use *private Internet* IPv4 & IPv6 addresses
    - ✓See RFC 1597 http://www.ietf.org/rfc/rfc1597.txt

Access Controls

- Restrict # individuals with access to Web server
  - Apply controls
  - Analyze reports
  - Monitor
- Cleared individuals need individual accounts (IDs)
  - Not generic functional account
  - Essential for audit trail
- Immediate termination of access upon
  - Change of responsibilities within organization
  - Termination of employment

Site Maintenance

- Even single-character error in public Web site can harm function and reputation
  - E.g., in link
- Content changes move through Web in minutes
  - Search engines
  - Archival capture
- Change-control procedures essential

See
***CSH6* Chapter 40: Managing Software Patches & Vulnerabilities**
***CSH6* Chapter 47: Operations Security & Production Controls**
***CSH6* Chapter 52: Application Controls**

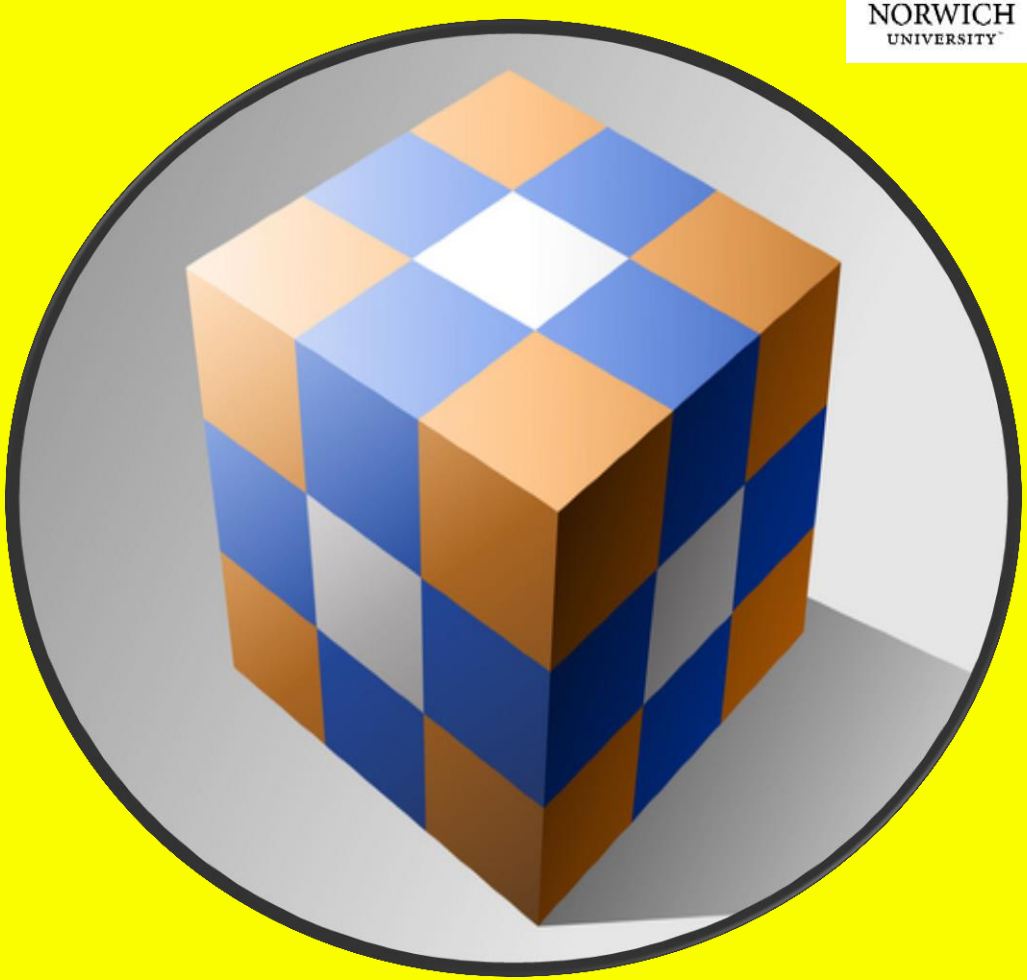
Maintaining Site Integrity

- Restrict write-access to Web server
- Use secure methods for accessing servers
  - Do not use unsecured access via Web
- Secure mechanisms for update:
  - Secure FTP
  - FTP from specific node within inner firewall
  - KERMIT on directly wired port
  - Logins & file transfers via SSH
  - Physical media transfers (*air gap*)

KERMIT: A file transfer protocol developed at Columbia University, noted for its adaptability to noisy lines, enabling transfers to succeed under the worst conditions. Kermit supports streaming over the Internet, sliding windows for links with long round-trip delays, record and character conversion of text files, restart/recovery from point of failure and platform-independent transfer of directory trees with a mix of text and binary files.
Computer Desktop Encyclopedia v22.3 (3rd quarter 2009). Copyright © Computer Language Company. Used with permission.

Technical Issues

- Inside / Outside
- Hidden Subnets
- What Need be Exposed?
- Multiple Security Domains
- Compartmentalization
- Need to Access
- Accountability
- Read-Only File Security
- Going Off-Line
- Auditing
- Emerging Technologies



Inside / Outside

- Fundamentals
  - Inside: trustable systems
  - Outside: untrustworthy systems
  - But not absolute distinction
    - ✓ May be trustworthy for one application or context but not another
    - ✓ Majority of harm done by authorized users
      - Incompetence or malfeasance
- Router tables must prevent IP spoofing
  - Inside to outside
  - Outside to inside

Preventing IP Spoofing

- ***Inbound*** **packets from outside cannot have *originator* addresses within *target***
- ***Outbound*** **packets to public network must have *originator* addresses within *originating network***
- ***Outbound*** **packets to public network must *not* have *destination* addresses within *originating* network**
- **Exception: stealth internal networks**
  - **Internal addresses correspond to external addresses**

Hidden Subnets

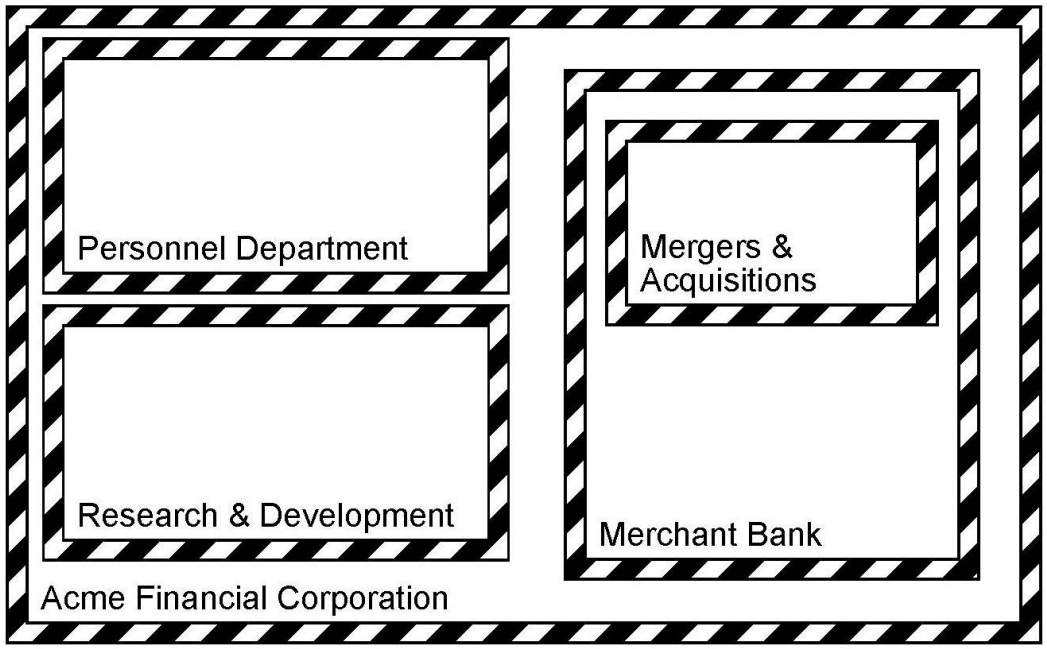
- Firewalls funnel network traffic through 1 or few chokepoints
  - Likelihood of security breach of entire NW rises with # independent access points
  - If p = P(access point will fail) then
  - P(access point will not fail) = (1 - p) and
  - If n = # access points then
  - P(all access points will not fail) = $(1 - p)^n$
  - P(at least one access point will fail) = $1 - (1 - p)^n$
- Use RFC 1918 internal addresses
  - For IPv4 within protected networks
  - Never occur in public Internet
  - Similar to addresses used in NAT (dynamic network address translation)

What Need be Exposed?

- Air gaps (total disconnection) can be useful
  - Industrial real-time control systems
  - SCADA
  - Life-critical systems
  - High-confidentiality systems
- Publishing information to Web servers
  - Media exchange
  - Controlled one-way transfers
- Restrictions on protocols
  - E.g., library can allow HTTP but block FTP
- Beware of tunnels through firewalls
- Or convert LAN to untrusted network
  - Use VPNs to connect internal corporate systems

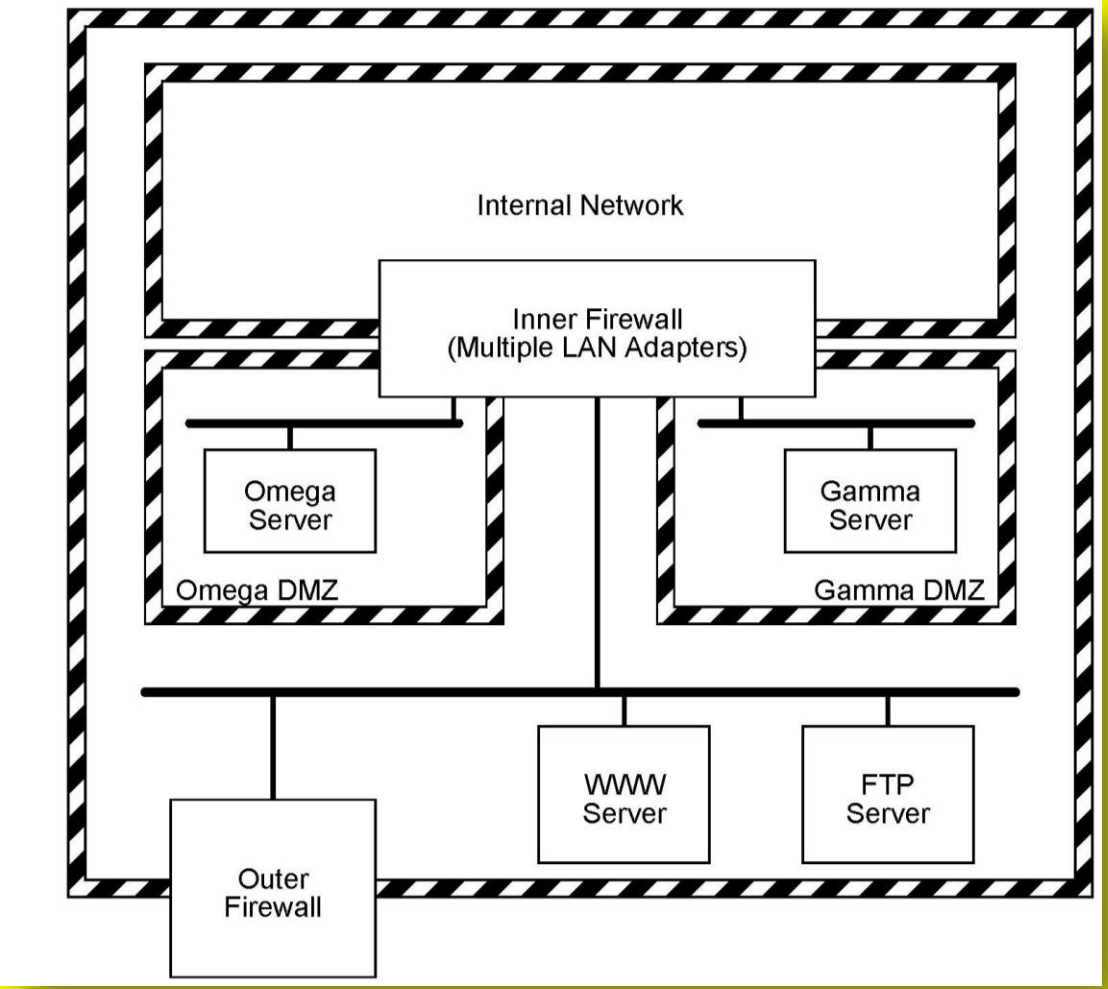
Multiple Security Domains (1)

- Monolithic firewall defines only outside & inside
- But better is Outside / DMZ / Inside
- Can also attach DMZ to single port on outer firewall
- May find internal compartmentalization useful



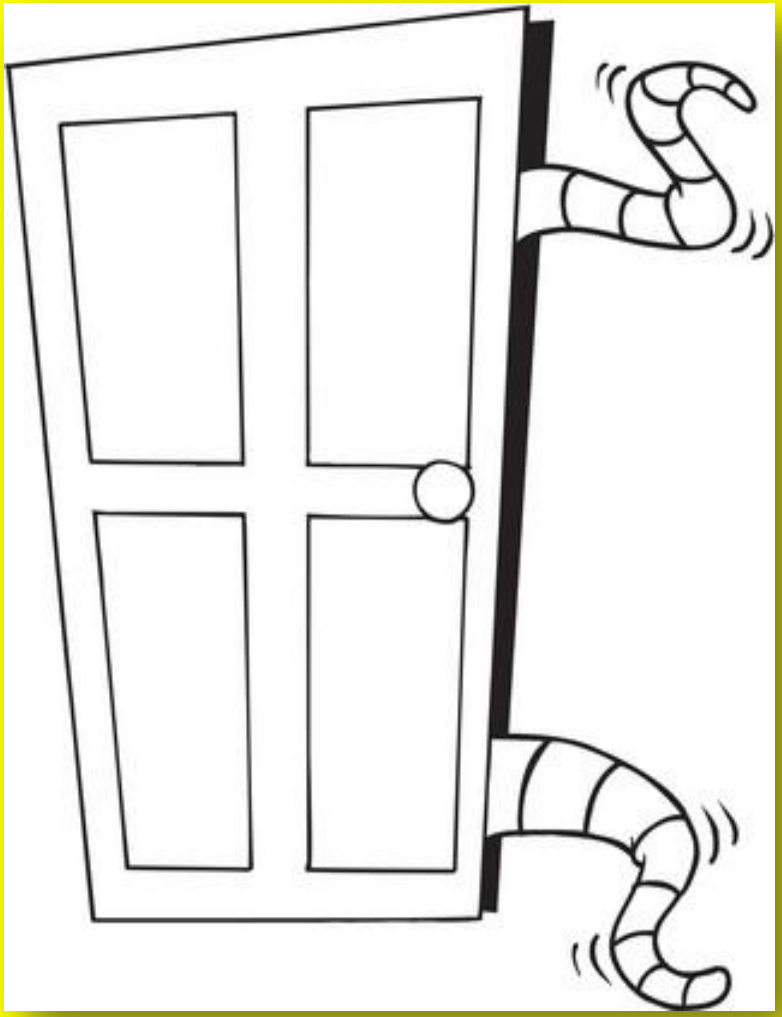
Multiple Security Domains (2)

- Brokerage with 2 trading networks, Ω & Γ
- Each gateway could
  - Monitor communications with Web server
  - Monitor traffic with competing trading NW
  - Attack other gateway
  - Disrupt communications with other gateway
  - Attack brokerage's internal network



Compartmentalization

- Reduces potential for complete network meltdown
- Prevent accidents from cascading
- Prevent infection by malware
- Portable storage devices
  - Including USB memory / disks
  - Make situation worse
  - Increase value of compartmentalization



Need to Access

- Careful analysis required for determining need to access to which resources
- Physical & logical access controls
  - Needed to protect Internet-accessible systems
  - Must be understood, respected & enforced
- Regular audits necessary
- Internal communications should also be secured
  - Encryption (e.g., SSL, VPNs)
  - Access by employees outside organization must be secured using VPNs

See *CSH6* Chapter 32: Virtual Private Networks & Secure Remote Access

Accountability

- No perimeter is likely to be perfect
- Encourage employees to report security vulnerabilities & accidents
  - Avoid pressures to hide such problems
  - Want early warning
  - Fix problems before they are exploited
  - Analyze root causes & resolve
- Do not punish people for false alarms

Read-Only File Security

- Many sites permit downloads (HTTP, FTP) of forms, manuals, instructions, maps, service guides
- Must ensure that
  - Servers supporting FTP are secure
  - Contents of public file store are read-only & have change-control procedures
  - Entire contents can be restored quickly if compromised
  - Designated (named) party responsible for maintaining, protecting & restoring public store

Going Off-Line

- Out-of-service costs critical to determine
  - Loss of business
  - Waste of professional time (e.g., salaries)
  - Damaged PR
  - Lowered morale
- Disconnection may be rational & required
  - E.g., FORD cut connection to Internet during May 2000 ILOVEYOU attack
  - Must establish WHO can disconnect for what reasons
  - Have written procedures & delegation of authority

Auditing

- Monitoring (logging) provides essential information on
  - Normal (baseline) behavior
  - Peaks (design for maximum expected needs)
  - Trends (plan for expansion before problems hit)
- Audit & analysis should include
  - Physical communications infrastructure
  - Firewalls, router tables, filtering rules
  - Host security
  - File security
  - Traffic patterns on backbones, DMZ, etc.
  - Physical security of systems & comm infrastructure

"We're going to parachute in and do a surprise audit, but I want to keep the whole thing low key."

Emerging Technologies

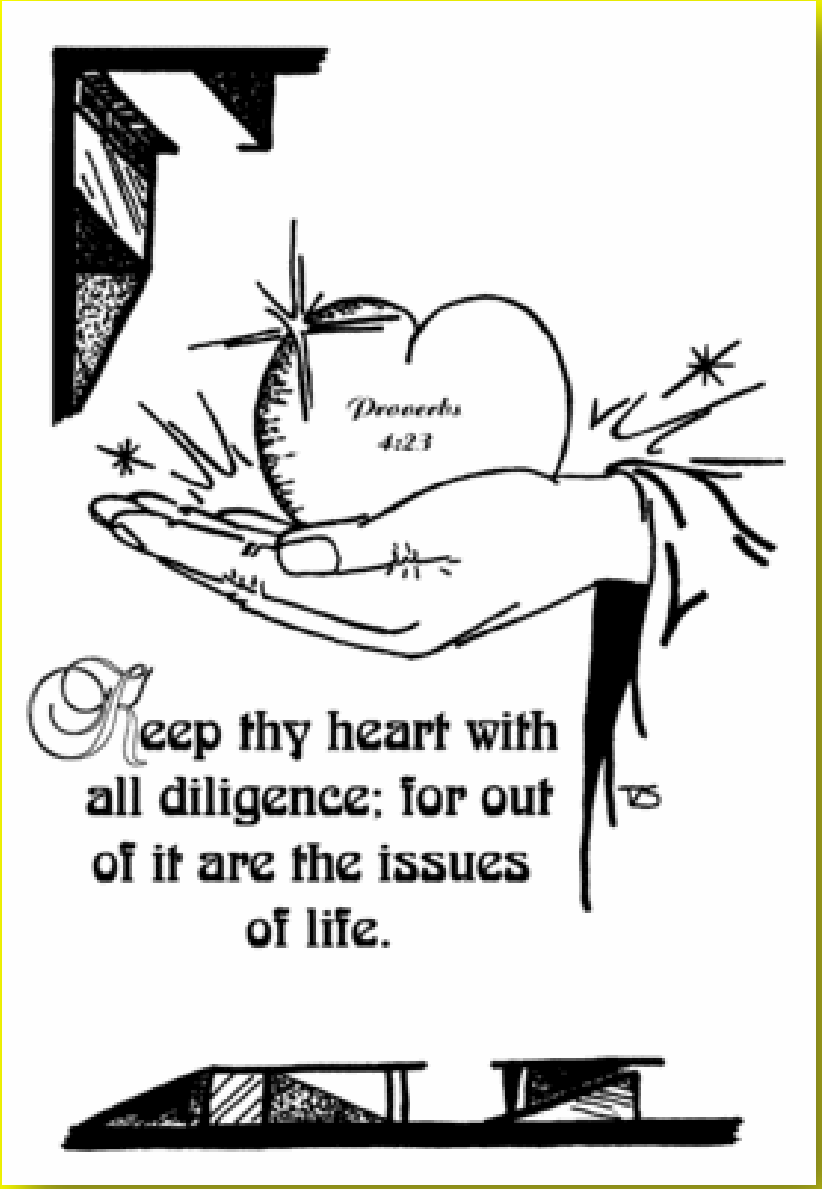
- New technologies alter challenges
- E.g., HTTPS for encrypted tunnels
  - Useful to authorize use of TCP port 443
  - Allow connection to Web sites needing secure information
- BUT HTTPS for tunneling also creates vulnerabilities
  - Compromised desktop can monitor network
  - Send data to system outside network using SSL
  - IDS may need to spot HTTPS connections that do not fit profile of normal Web access

Ethical & Legal Issues

- Liabilities
- Customer Monitoring, Privacy & Disclosure
- Litigation
- Application Service Providers

Liabilities

- Many laws affect disclosure of personally-identifiable information (PII)
- Web sites increasingly manage sensitive information
- E-mail also carries confidential data
- Must establish practice of due diligence
  - Show reasonable steps
  - Ensure integrity, safety, confidentiality

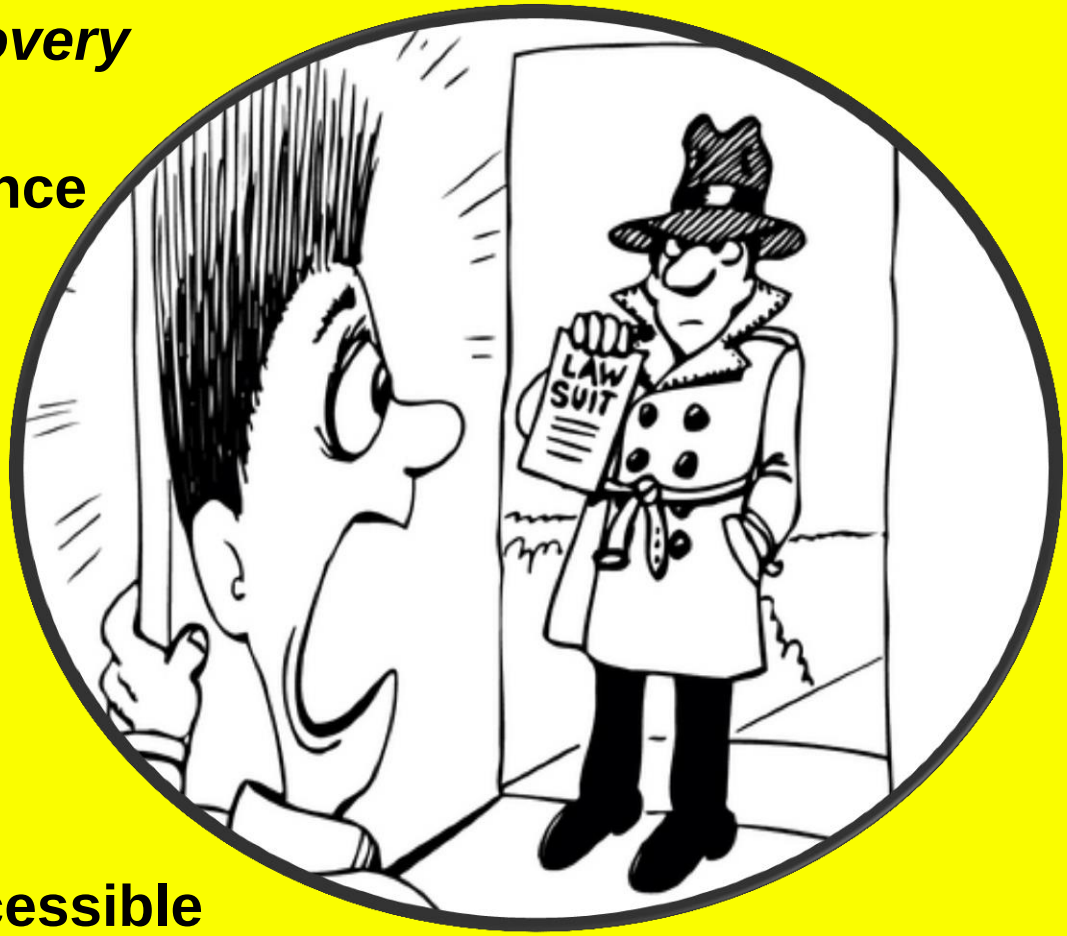


Customer Monitoring, Privacy & Disclosure

- Customer monitoring a sensitive subject
  - Can accumulate spending profiles
  - May show interesting products
  - But could assemble dossier for blackmail
  - Turn over data to hostile / paranoid government agencies
- Many organizations fail to encrypt PII on servers
- Data mining may lead to incorrect conclusions
  - Do not confuse *casual* associations with superficial interpretations
  - E.g., businessman who meets young woman in hotel – his daughter!

Litigation

- Increasing volumes of Web-related litigation
- Civil: be prepared for *discovery* procedures
- Regulatory: verify compliance with records retention requirements for all appropriate agencies
- Criminal: safeguard evidence, cooperate with law enforcement & courts
- Logs, Evidence, Recording Facts
  - Key to success
  - Accurate, complete, accessible (right software available!)
  - Be sure you know which records are stored where



Application Service Providers (ASPs)

- External organizations providing specific applications (e.g., accounting, manufacturing)
- Enterprise, not ASP, bears responsibility for security failures
- Due diligence
  - Choosing ASP
  - Defining contracts
  - Monitoring quality of service (QoS)

Now go and study