



Security Roadmap

Jason Swegle

Security Practice Manager

Mission Statement

The Root Group is a premier advisor to enterprises that consider IT systems as critical tools.

We engineer, implement and support structured, cost-effective IT solutions that advance the strategic business goals of our clients.

Our focus is *Secure IT Infrastructure*

1989

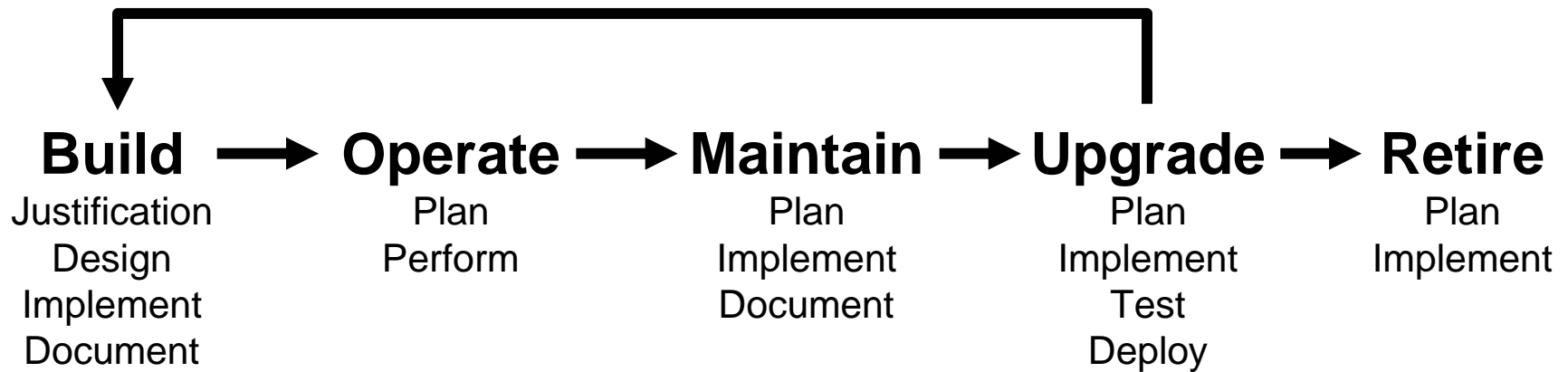


2004



information architecture @ another level

IT Life Cycle



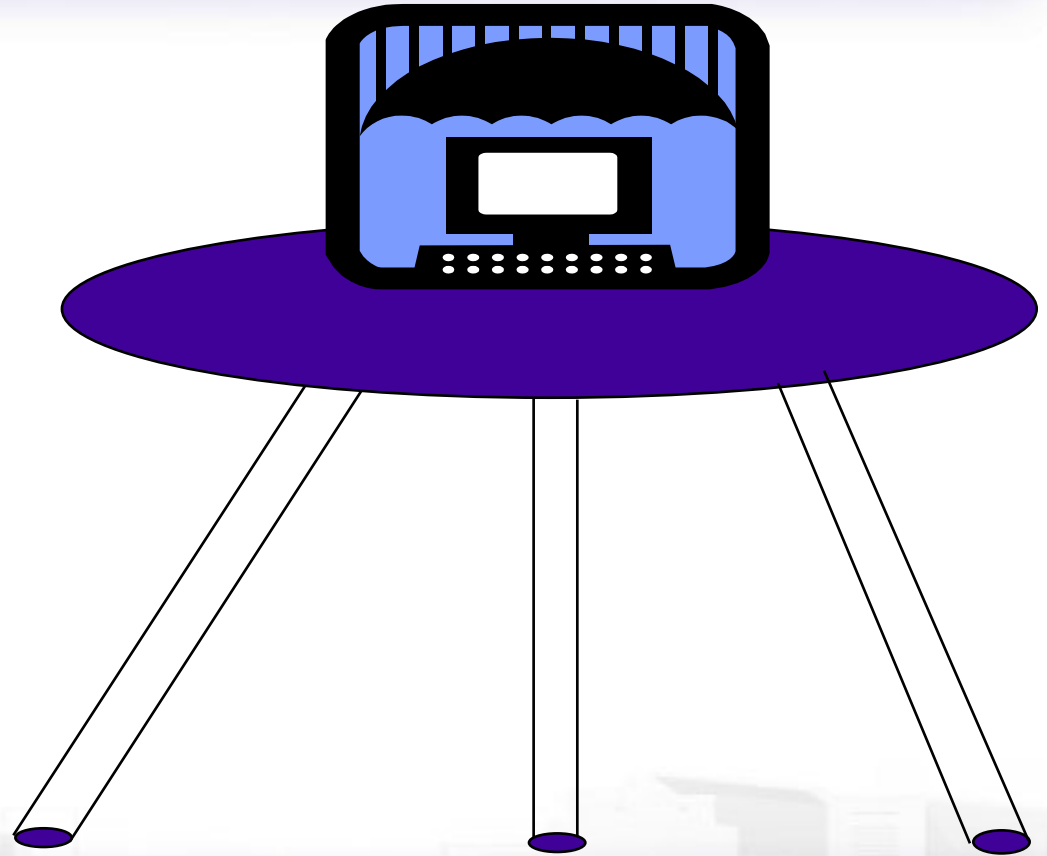
IT Security Lifecycle

- ◆ Differences from other IT operations
 - Break/fix methodologies won't work
 - Monitoring and human reaction required
 - Proactive, traceable change/configuration management crucial
 - Regularly performed auditing required by 3rd party



Security Tripod

- ❑ Policy
- ❑ Technology
- ❑ Culture



Policy: Informed Risk Management

Right-Sizing Security

- Use the risk assessment method
- Estimate your threats
- Use standard policy templates and modify to fit
- Get help and negotiate with an information security insurance company, to cap your risk, e.g.:
 - ICSA
 - AIG
 - Others

Think of information security the way you think of physical security and natural disasters – Threats you learn to live with

Right-Sizing Security Goals

- ◆ Deploy security so that the typical cost of a break-in will be less than your recurring security costs
- ◆ Deploy security so that the time it takes to break-in is longer than the time it will take to detect and shut down an attack
- ◆ Give up the "100% security" goal, it doesn't exist.

Infinite security takes infinite resources

Culture: Security Checklist

- ◆ Developed & communicated policies
- ◆ User education
 - Company security stance overview
 - User responsibilities and duties
 - Secure computing practices at work
 - How to compute safely at home & while traveling
- ◆ Appropriate legal counsel
 - Understanding of your legal liabilities and obligations
 - Legal resources familiar w/ employment law

Choices to Consider

Your approach affects your culture:

- Culture of trust or distrust?
- Explicit boundaries or “We are watching”
- Employee morale, productivity
- Employee retention rate
- Ability to align with business process
- Ability to get projects funded

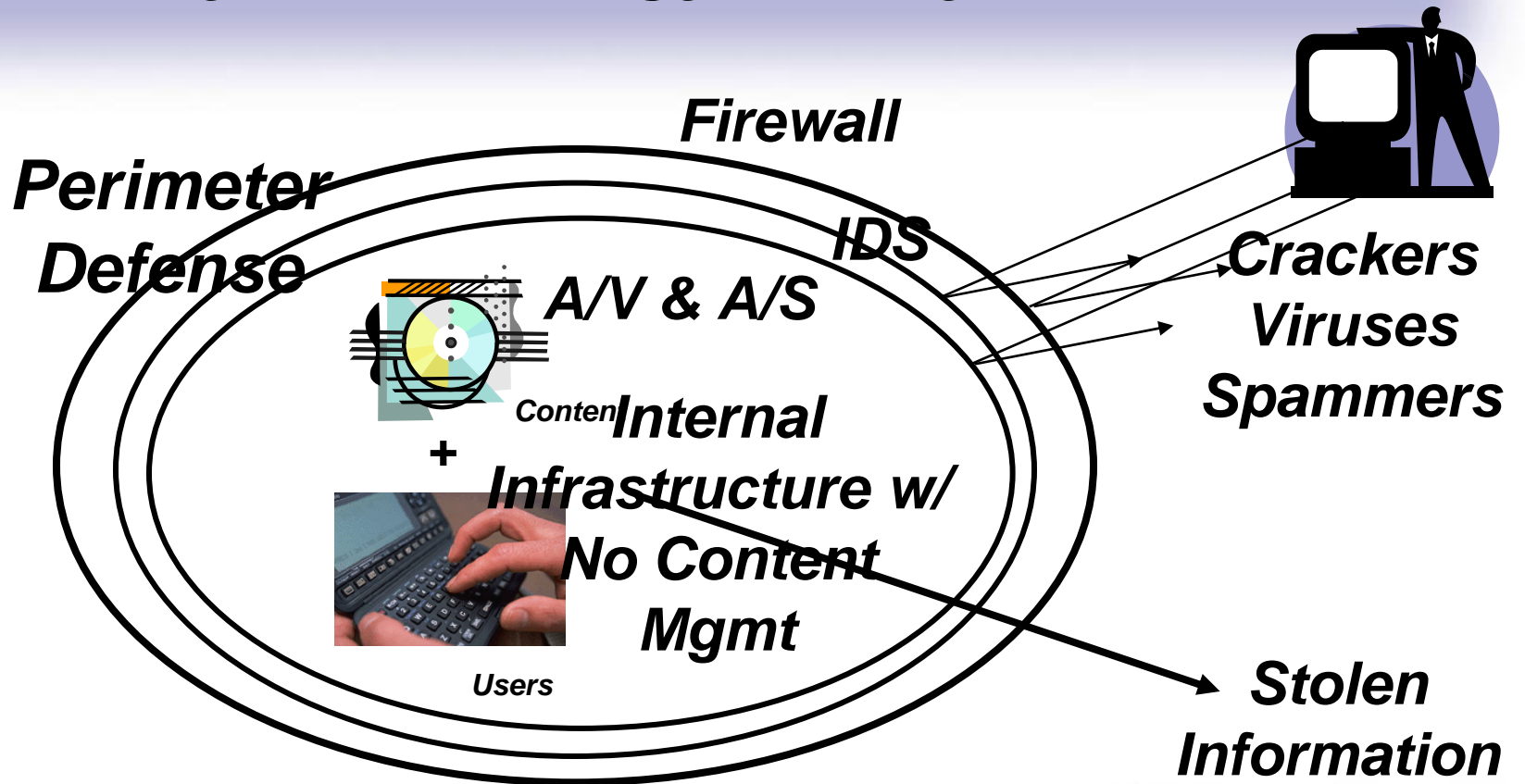
Technology: Security Roadmap

- ◆ Many point products with a high rate of change
- ◆ Integration with operational systems a challenge
- ◆ Low signal to noise ratio on alerts, with high tuning needs
- ◆ Integration across security devices a challenge
- ◆ Confusing landscape, competing vendor strategies

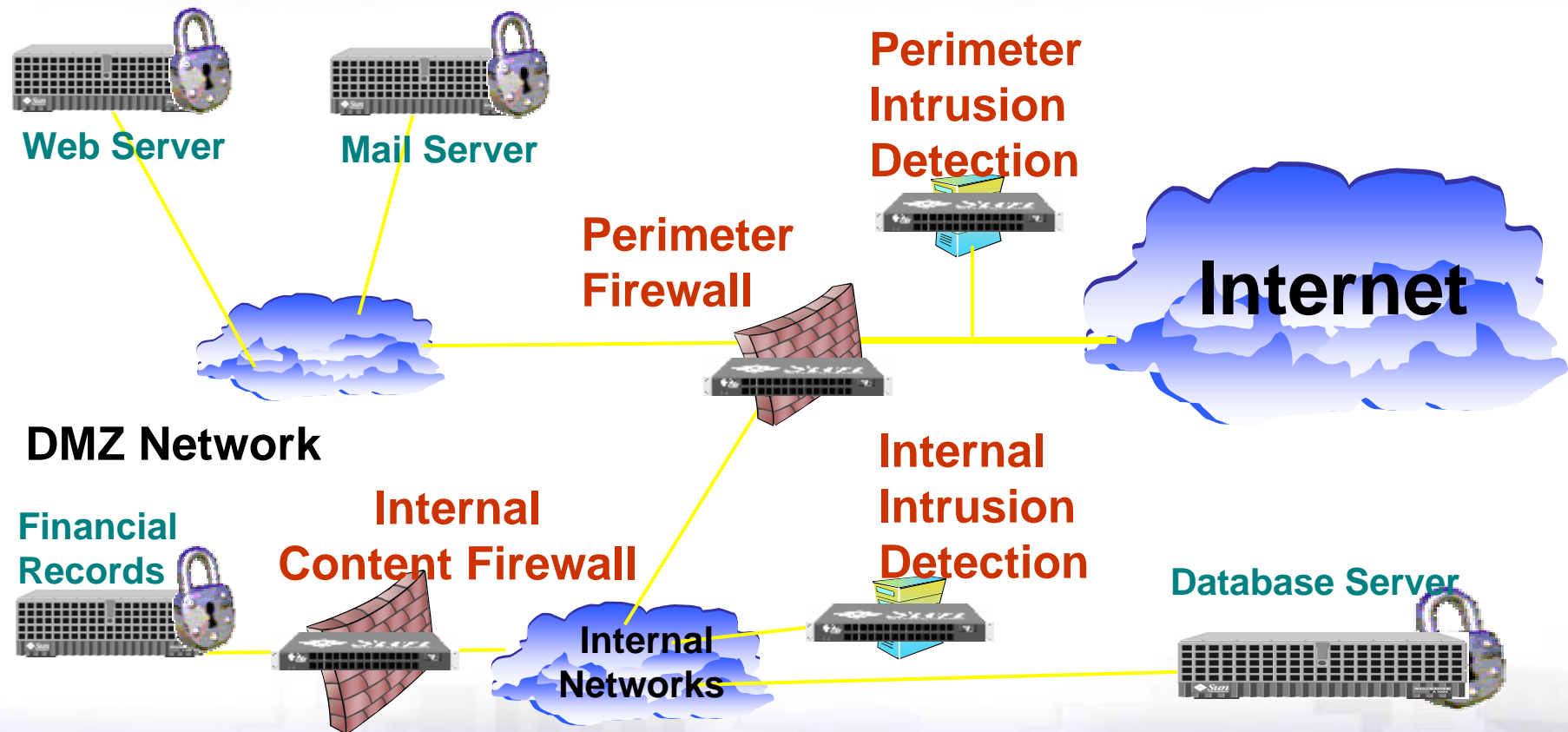
That Elusive Security Roadmap

- Matches business priorities to security infrastructure architecture requirements
- Offers a baseline model of security capabilities needed and options available at each layer of the infrastructure against which you can compare your enterprise
- Sets basic standards for management and integration of security components and base IT infrastructure that is being protected
- Considers what other IT issues can be addressed by the security solution, providing more benefits to you

Security Technology Today



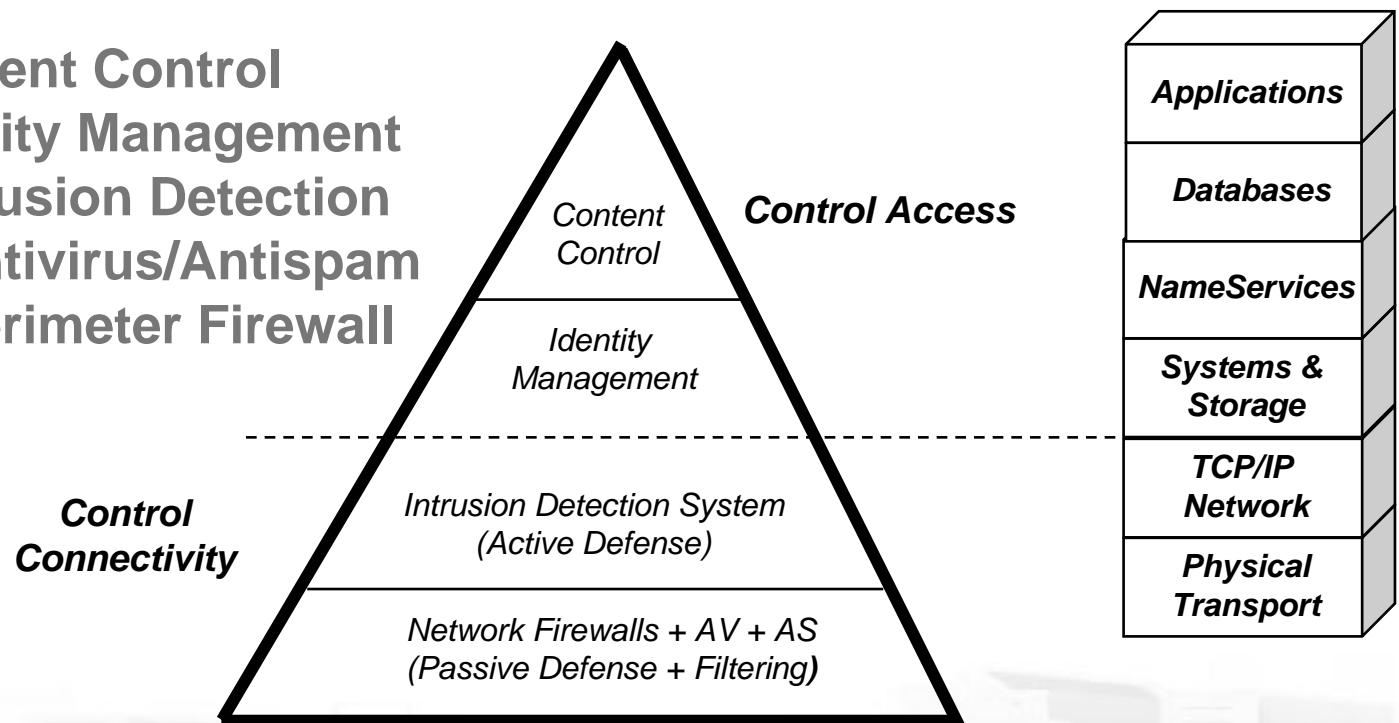
Typical Security Architecture



Basic Security Definitions & Progress

~ Percentage of Adoption:

- 1% Content Control
- 5% Identity Management
- 60% Intrusion Detection
- 80%+ Antivirus/Antispam
- 99%+ Perimeter Firewall



Available Security Controls

- ◆ Application Access Control
 - User account permissions, multi-factor authentication, AAA
- ◆ Database Access Control
 - Access controls by user or host to ODBC, SQLnet
- ◆ System Access Control
 - User account permissions, multi-factor authentication, AAA
- ◆ Storage Access Control
 - Filesystem permissions, security groups, Content Management
- ◆ Network Connectivity Control
 - Firewalls, IDS, Sandboxing, Payload monitoring, 802.1x
- ◆ Physical Location Control
 - Locks, Keypads, Cameras, Card Swipes

Security Technologies

Infrastructure

- ◆ Content Management
 - Content Monitors
 - Policy Verification
- ◆ Intrusion Detection
 - Network-based
 - Host-based
- ◆ Perimeter Defense
 - Firewall
 - AV/AS/Spyware/Adware
 - Secure Remote Access

Foundation Prerequisites

- ◆ Identity Management
 - Password and account management
- ◆ Sufficient Resources
 - Tuning
 - Internet Threat Tracking
- ◆ Connectivity Policy
 - AAA Services

Up and Coming Security Technologies

- ◆ Security event correlation, managed response
 - Lurhq, MCI, AT&T, Sun/Verisign, Applied Watch, Cisco's "Protego"
- ◆ Identity management
 - Web SSO, A/D and LDAP integration, password management, account provisioning, federalization
- ◆ Network access control
 - Cisco

Security Technology Selection

Will it work for you over the long-haul:

- Is it really manageable, scalable?
- Will it integrate?
- What does it report; How many false alerts?
- How much effort is it to operate, maintain?
- Does it offer any benefits to my O & M needs?

Security technologies that fail these tests often may not be good choices.

Cisco's "Self-Defending Networks"

- ◆ PIX and IPSEC Firewalls
- ◆ IDS host and network sensors
- ◆ Endpoint security
 - CSA for zero-hour protection
 - CTA (NAC) + Perfigo for network access control
- ◆ Anomaly detection and mitigation
- ◆ VPN software and appliances
- ◆ Event and data correlation, remediation

Q & A

Jason Swegle

jason@rootgroup.com



information architecture @ another level

Key information and who owns it

Your Company

- Customer Lists
- Customer Information
- Patient Information
- Employee Information
- Company Financials
- Company Strategy
- Technical Innovations
 - Trade Secrets
 - Patent Applications
 - Research in Progress
- Company Financials
- Company Strategy

Customers

- Identity Information
- Credit Card Information
- Health Information
- Employment Status
- Personal Financials
- Company Strategy
- Technical Innovation
 - Trade Secrets
 - Patent Applications
 - Active Research
- Company Financials
- Company Strategy

Strategic Partners

- Customer Information
- Patient Information
- Employee Information
- Company Financials
- Company Strategy
- Technical Innovation
 - Trade Secrets
 - Patent Applications
 - Research in Progress
- Company Financials
- Company Strategy

This is all information you hold or could access!



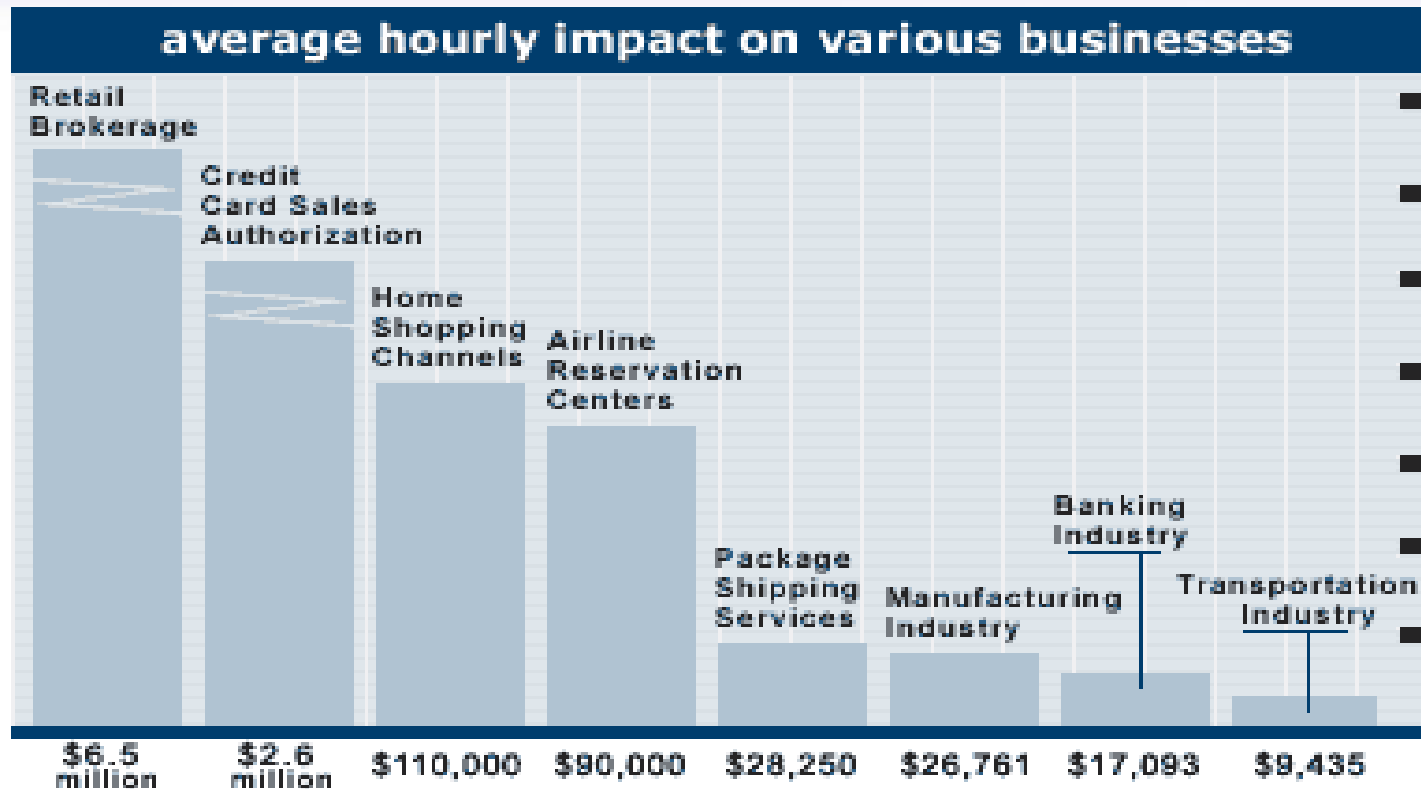
information architecture @ another level

Location of Information Assets

Places to Look:

- Data Warehouses
- Enterprise Databases
- Application Specific Databases
- Subsidiary Databases
- Server Fileshares
- Mail Servers
- Your Application Service Providers
- Desktop or Portable Databases
- Desktop or Portable Files
- Backup Tapes

The Cost of Data Loss



Source: Contingency Planning Research & Strategic Research Corporation



information architecture @ another level

The Consequences of Data Loss

The staggering statistics!

- 40 percent of respondents to a computer security survey had detected and verified incidents of computer crime during the previous year. (NCSA Annual Worry Report)
- Computer crimes cost firms who detect and verify incidents of computer crime between \$145 million and \$730 million each year. (NCSA Annual Worry Report)
- Most companies value 100 megabytes of data at more than \$1 million
- 43 percent of lost or stolen data is valued at \$5 million or more
- 43 percent of companies experiencing disasters never reopen, and 29 percent close within two years. (McGladrey and Pullen)
- It is estimated that 1 out of 500 data centers will have a severe disaster each year. (McGladrey and Pullen)
- A company that experiences a computer outage lasting more than 10 days will never fully recover financially. 50 percent will be out of business within five years. ("Disaster Recovery Planning: Managing Risk & Catastrophe in Information Systems" by Jon Toigo)



information architecture @ another level