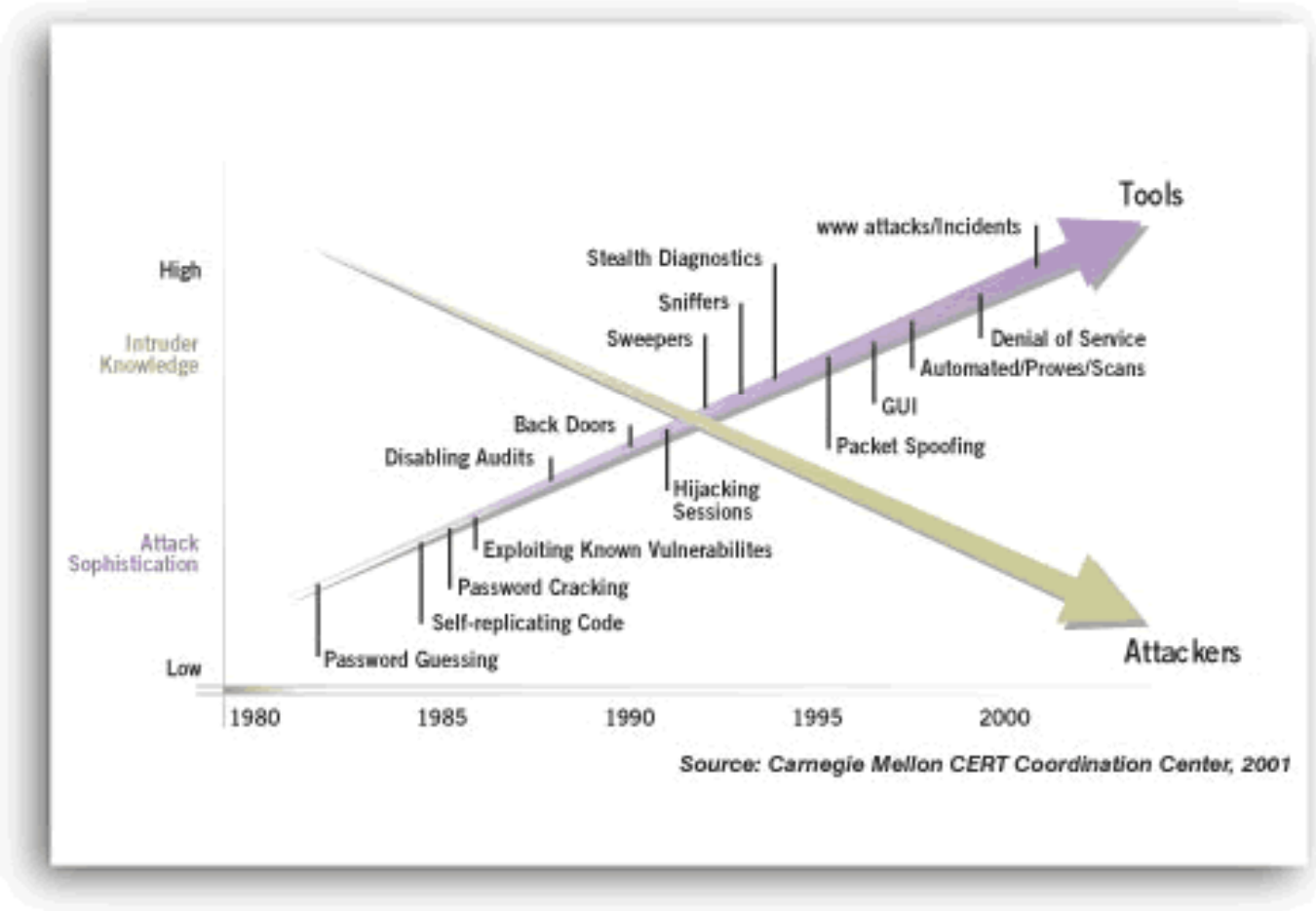
Intrusion Detection and Threat Vectors

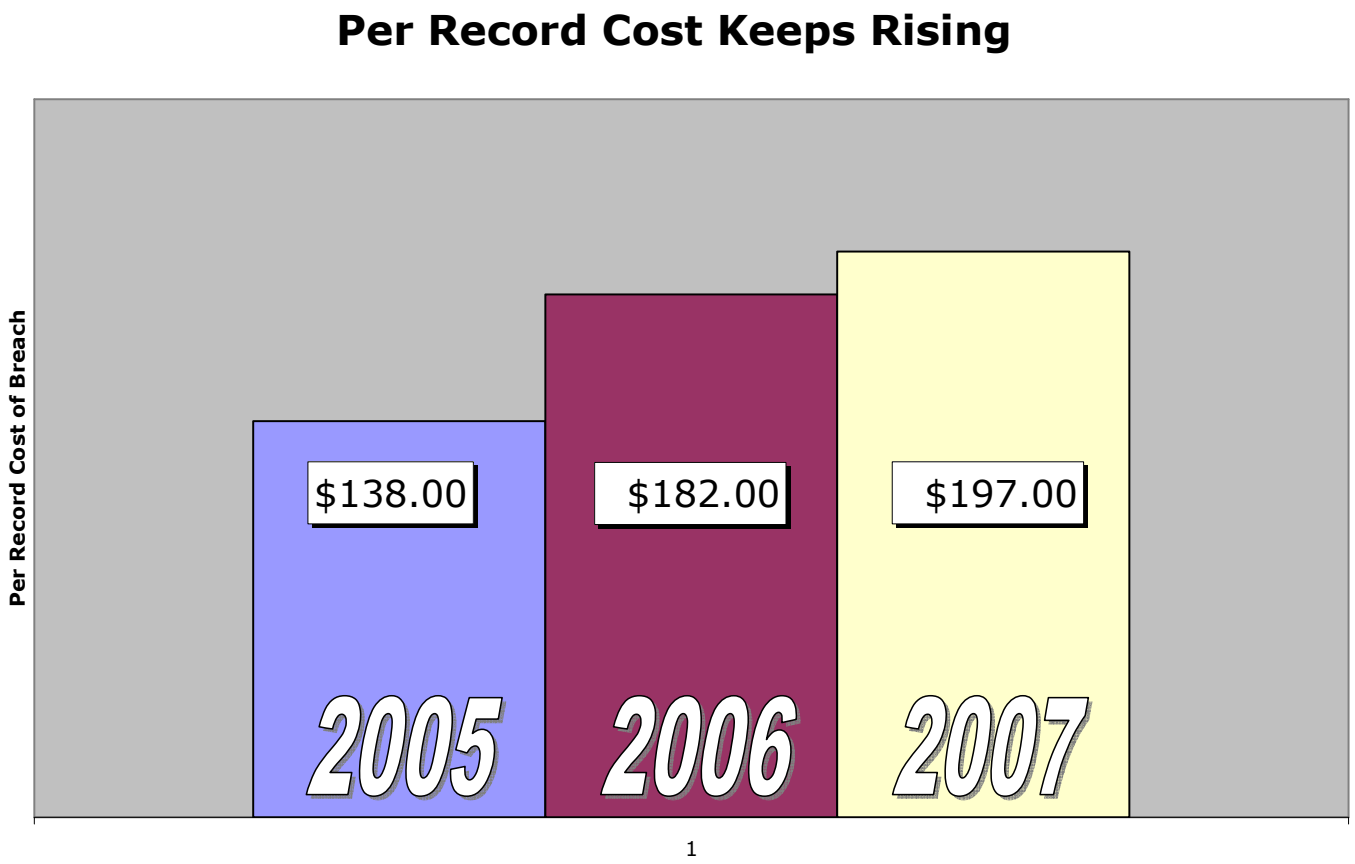
Michael Arent
EDS-Global Information Security

EDS
EXPERTISE. ANSWERS. RESULTS.

The direction is changing. . . .



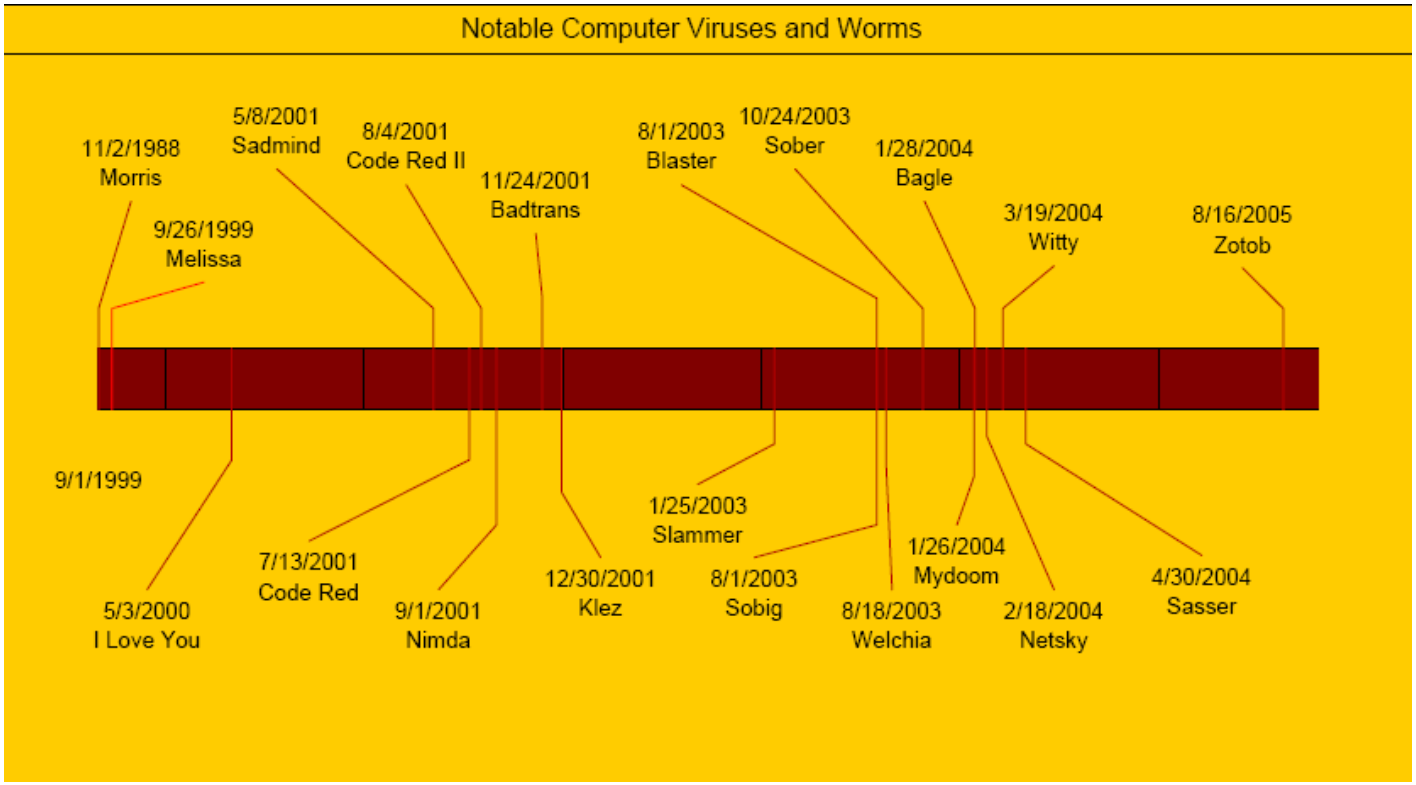
Intrusion costs are rising



Data from Ponemon Institute (survey of 35 companies that have experienced breaches)

Changing Motivation and Attack Vectors

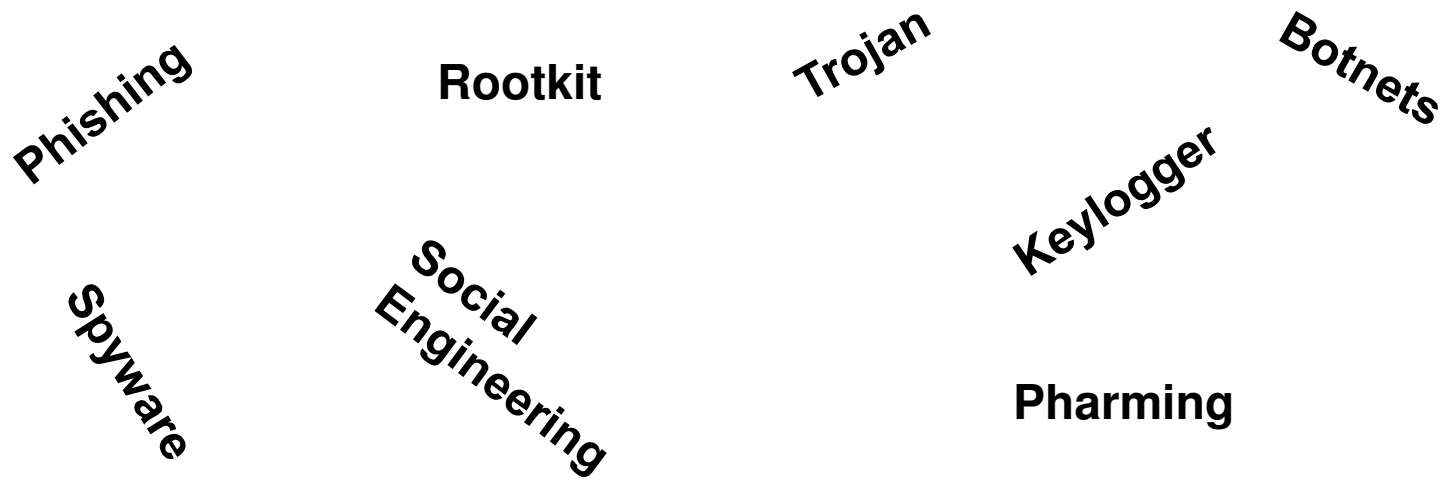
•During the 90's and early 00's the motivation was notoriety and Denial of Service.



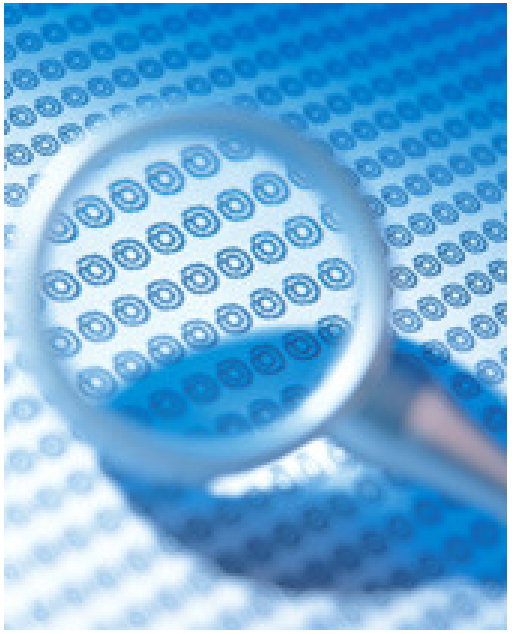
EDS
EXPERTISE. ANSWERS. RESULTS.

New Motivation and Attack Vectors

- In 2005 the focus started changing
  - A shift from notoriety motives to financial motives
  - A shift from global attacks to targeted attacks
  - A shift from denial of service to stealth components
- We started hearing new words:



Threat Landscape



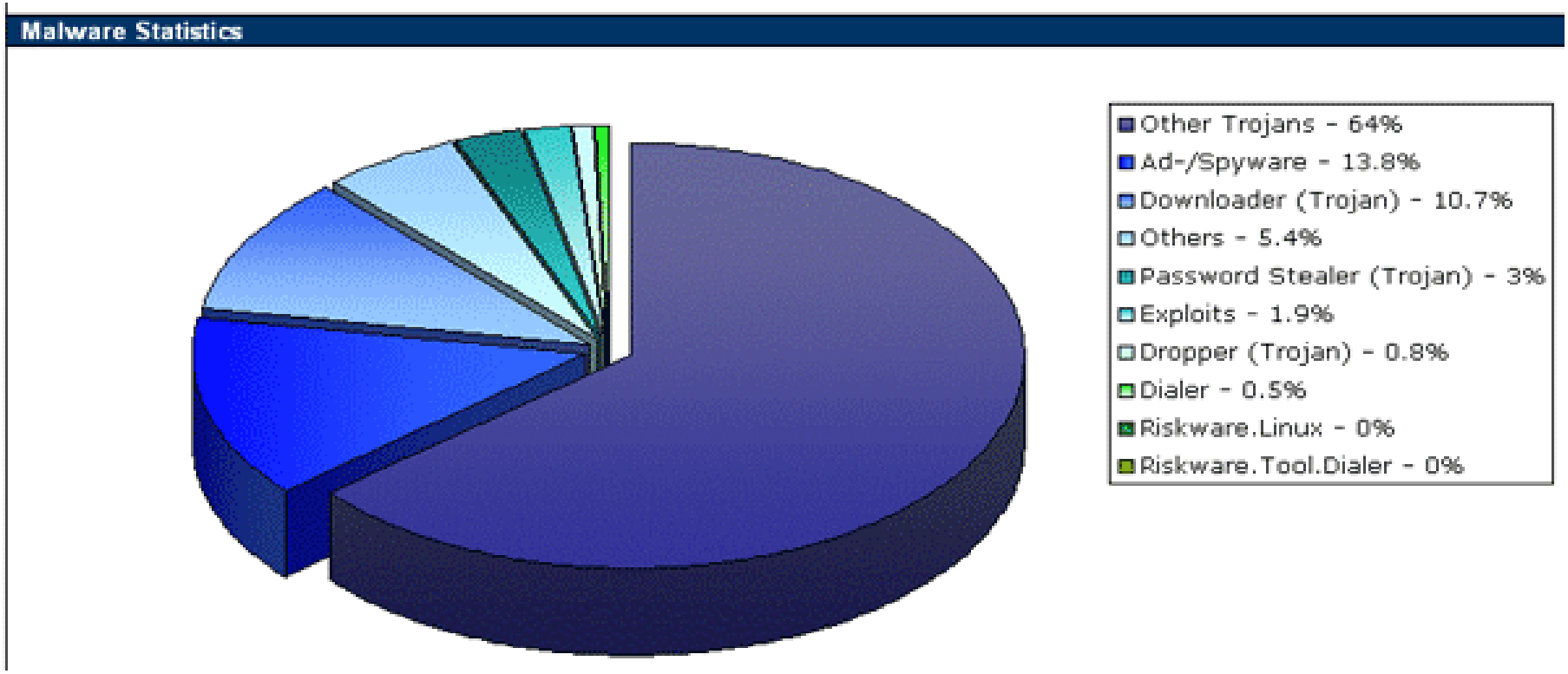
- **Mail/Spam Volume -** spam making up **89%** of all email.
- **Malware -**Trojans accounted for over **78%** of all newly discovered malware, followed by Adware and Spyware that made up almost 14%. **97%** of all new malware came in the form of Windows Executable files.
- **Zombies** An average of **264,133** new zombies are detected daily, many associated with the new infections caused by the Storm worm.
- **Web Threats** An average of **11,906** total new malicious websites are detected daily.

New Threats

- For the past 2 years, we have seen a dramatic increase in the number of stealth malicious codes.
- 11074 families of malicious codes newly identified

Malcode Type	Count
Adware	268
Bot	378
Spyware	187
Backdoor	828
Clicker	20
Dialer	22
Downloader	1755
Dropper	501
Keylogger	64
Trojan	6304
Proxy	89
RootKit	41
Stealer	617
Total	**11074**

Malware Snapshot – Feb.2008



The most prevalent targets as of late are; government, education, and financial.

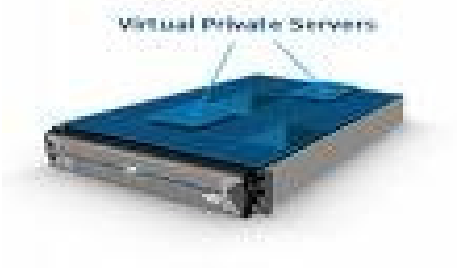
Exploits are now shorter

Typical Costs To Business of Delayed Detection / Containment

Attack - Vector normalized	Damage Cost Factor (1-10) 1=low,10=high	Response Cost Factor (1-10) 1=low, 10=high
Root via Buffer Overflow	2	2.7
Remote Root	2	4
Root via Single Event	10	1.3
Single event Crash	6	.3
DoS (SQL Slammer) per environment	6	10
Port Scan	.4	3.4
"Low and Slow" Probe	.4	4.7

New Threats – New Technologies – New Vulnerabilities

- Introduction of new technologies are providing some challenges for the security professional

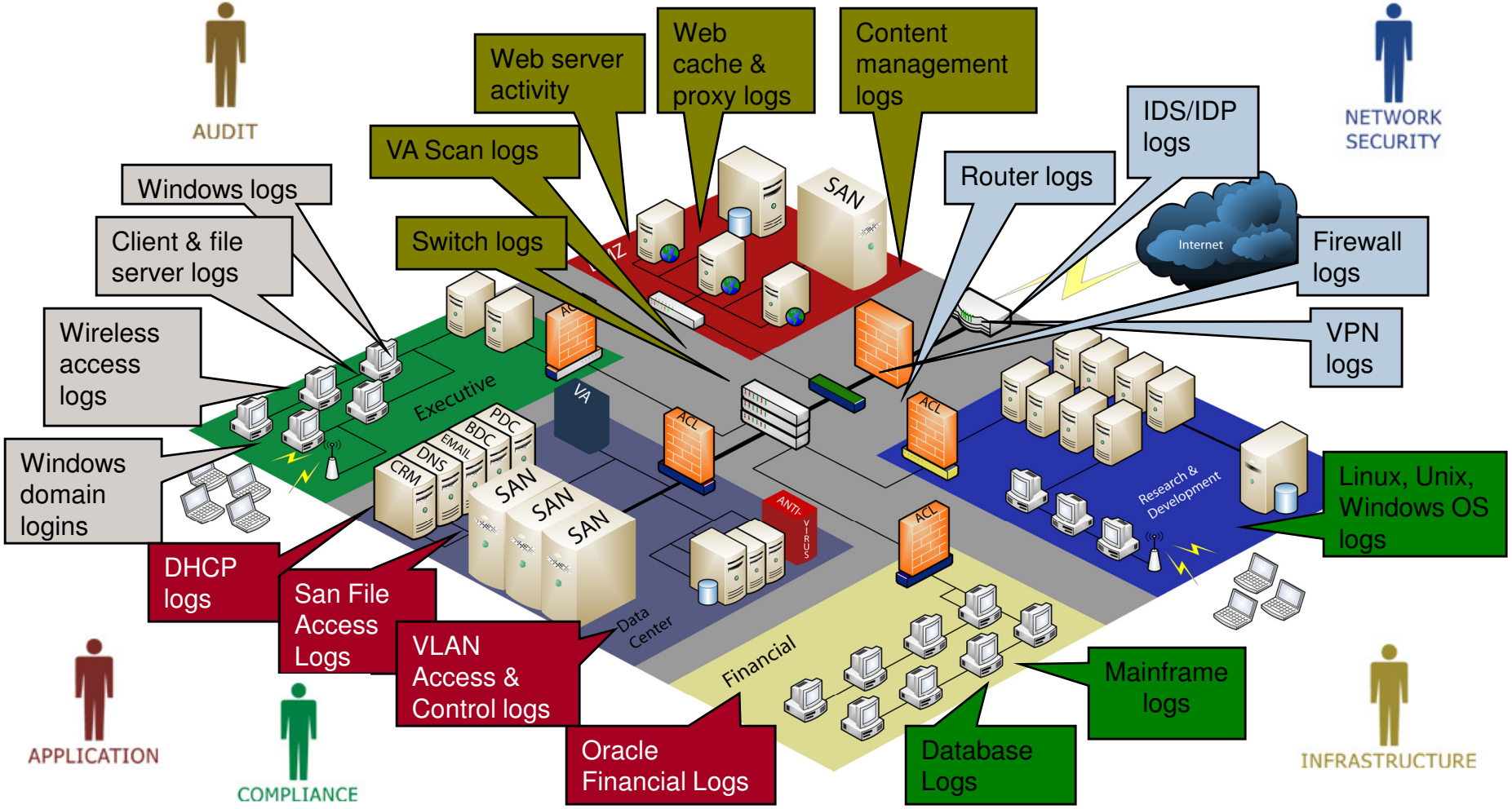




Survivable Systems best practices require the ability to *Recognize* threats, *Resist* attacks, provide for *Rapid Recovery* if the attack cannot be resisted, and quick and accurate *Root Cause Analysis* that is effectively integrated into infrastructure and management practices

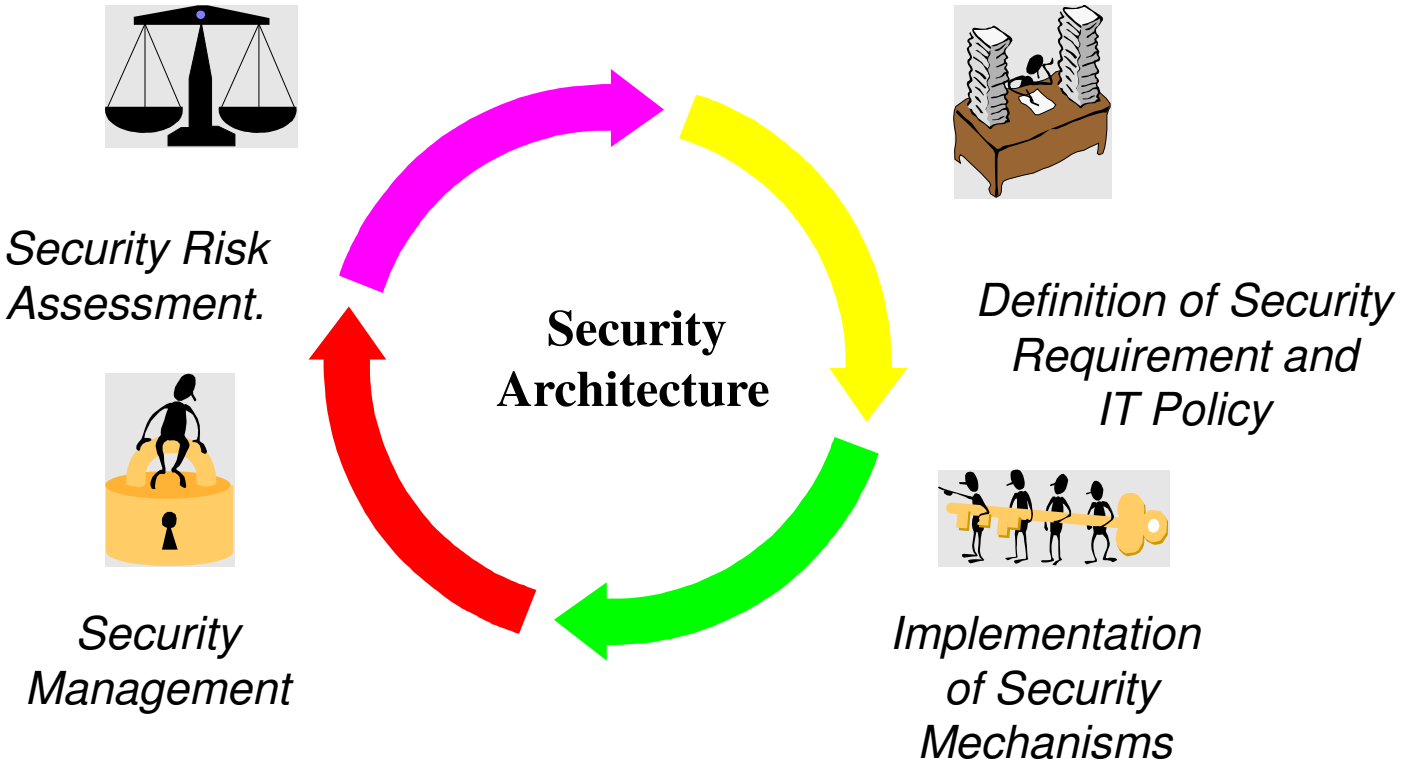
The Enterprise Today . . .
Mountains of Data

How do you collect & protect all the data necessary to secure your network and comply with Sarbanes Oxley, GLBA, HIPAA, VISA CISP, …..



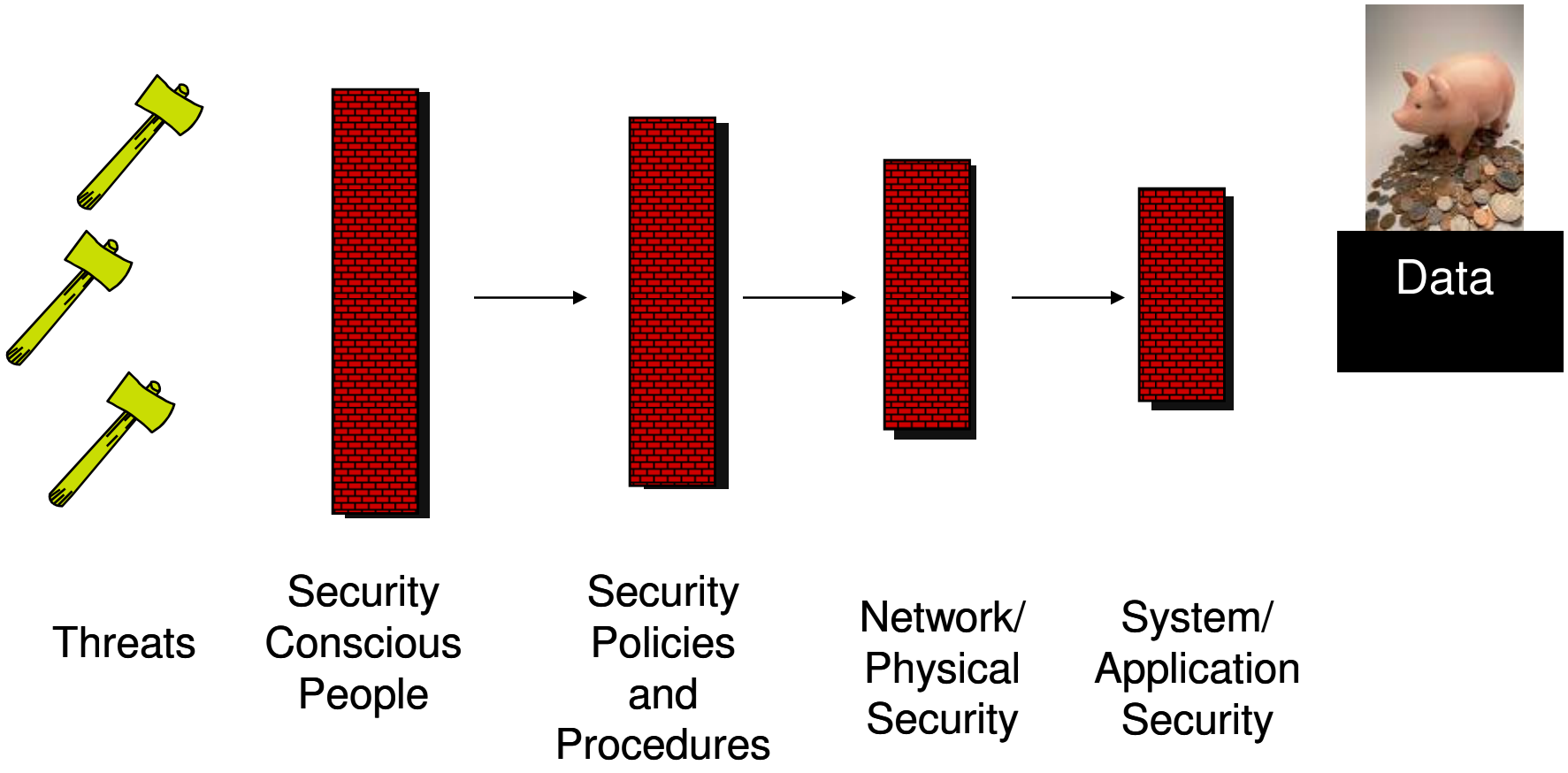
Next Steps...

The Security Process Cycle



A Balanced Approach to Security

Size Denotes Effectiveness



Approach to Security

- A Balanced Approach to Security
- Assessing the Risk
- Enterprise Security Policies & Standards
- Securing an Environment
- Security Compliance Challenges
- Some Lessons Learned

Guiding Principles for a Security Program

Use of Security to enable success in the digital economy

- Security Program must:
  - Be driven by the Business Strategies and Policies
  - Complement Information Technology Strategies and IT Infrastructure and Business Applications
  - Be presented clearly, concisely, and be easy-to-use
  - Based on a Need-to-Protect philosophy
  - Be mapped to industry 'standards', e.g. ISO17799, CoBIT
- Security Program based on concepts of:
  - Defense-in-depth
  - Least-privilege
  - Need-to-know

Assessing the Risk

Nature of Threats

- Viruses/Worms
- Hackers
- Denial of Service / Web Site Defacement Attacks
- User Errors
- Internal Attacks / Abuse / Un-authorised Access
- Non-compliance with laws / regulations
- Intellectual/Corporate Property Theft and Extortion
- Fraud / Laundering
- Complacency

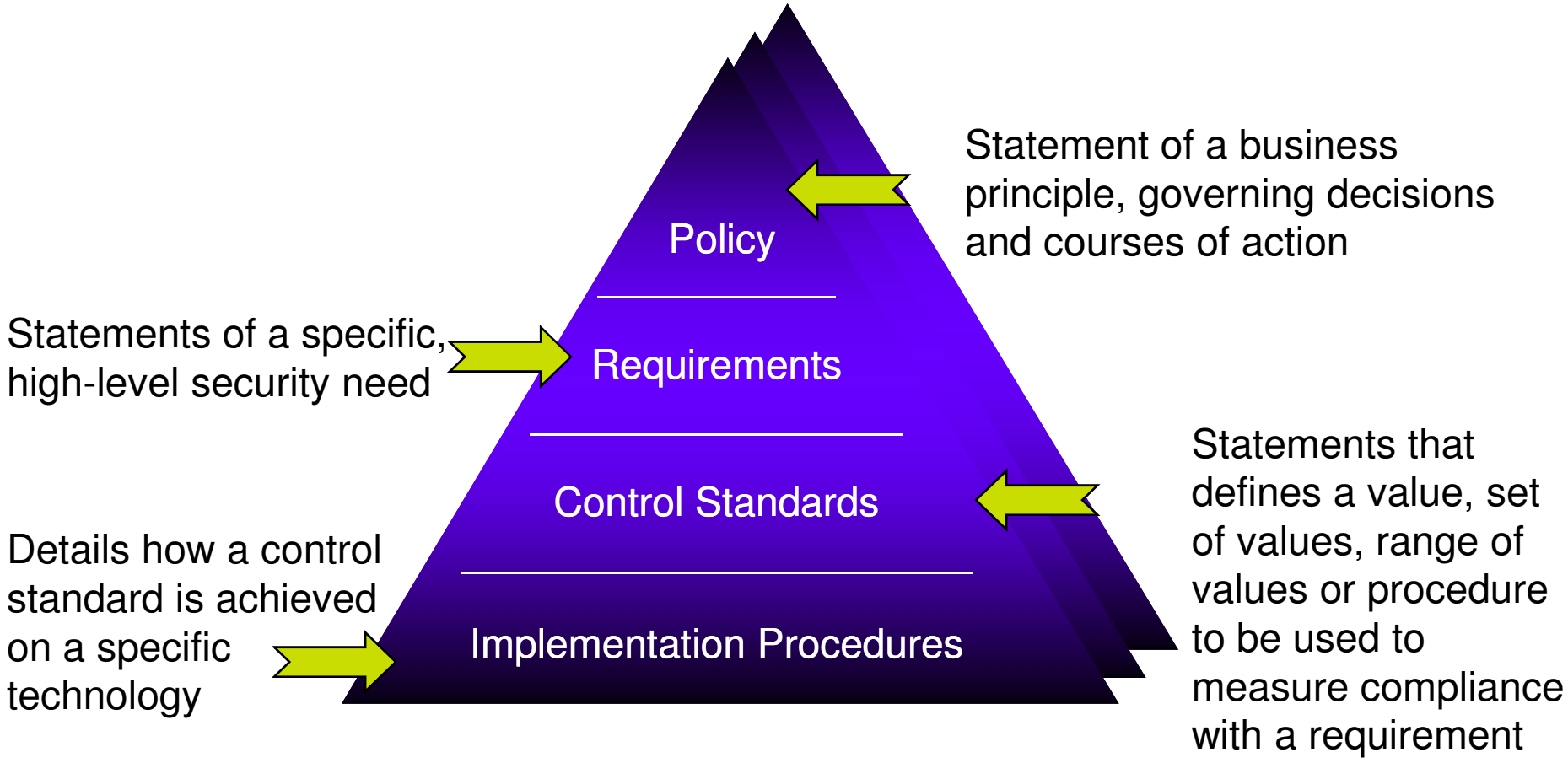
Assessing the Risk

Business Impact

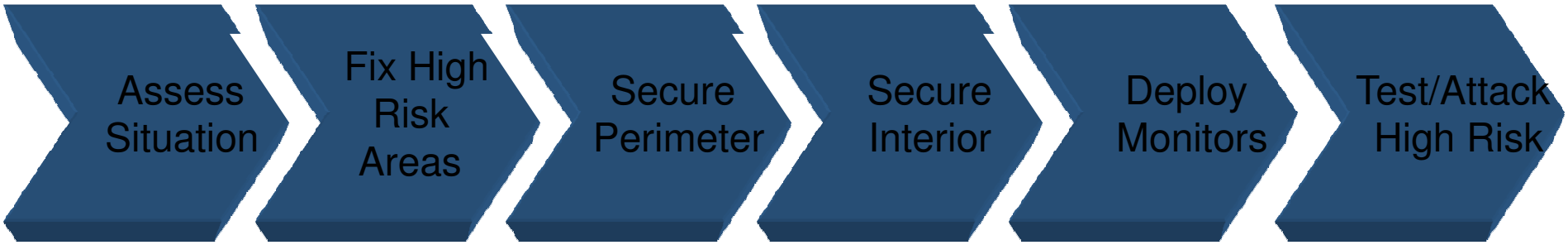
- Loss of Revenue
- Cost of Recovery
- Loss of Productivity
- Loss of Shareholder / Customer confidence
- Loss of reputation
- Legal / Regulatory / Contractual non-compliance penalties
- Competitive Disadvantage

Security Policy: Framework

Enterprise Security Policies & Standards

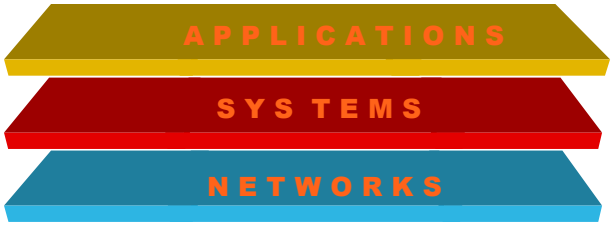


Securing an Environment



Securing an Environment

Defense in Depth



- Network View
  - Restricts access to the enterprise
  - Centrally Administered
- System View
  - Restricts access to specific hosts, applications
  - Centrally Administered
- Application/Data View
  - Restricts access to specific business processes and data
  - Locally Administered
  - Re-visit the "need to know" on a recurring basis

Securing an Environment

Defense in Depth – Another Perspective (from SANS Institute)

- **Defensive Wall 1 – Blocking Attacks: Network Based**
  - Firewalls, intrusion detection/prevention systems, Network Admission Control (NAC)
- **Defensive Wall 2 – Blocking Attacks: Host Based**
  - Personal firewall, host intrusion detection/prevention, anti-virus, anti-spam
- **Defensive Wall 3 – Eliminating Security Vulnerabilities**
  - Vulnerability management, patch management/vulnerability remediation, security configuration compliance, application security testing
- **Defensive Wall 4 – Safely Supporting Authorized Users**
  - ID & access management, file encryption, VPN, SSL VPN
- **Defensive Wall 5 – Minimize business losses and maximize effectiveness**
  - Security information management, security skills development, integrity monitoring, back up, business recovery, forensics tools

Security Challenges

- Overall security awareness
- Windows/Unix logical security controls
  - ID & access management, logging/monitoring
- Disaster recovery/business continuity plans
- Security Information Management
- Network security management
- Multiple and contradicting regulations

Some Lessons Learned

- New technologies are adopted in the field
  - e.g. wireless networks, mobile computing, …
  - Manage them centrally
  - Deploy protection centrally
- Respond by need, not fear
  - Base decisions on security policies, *business value* and risk
  - *Due care* is not the same for all resources
  - Does everything need an Intrusion Detection System?
- Secure the network completely!

Summary

Key Factors in Intrusion Detection

- Create a consistent, viable security policy
- Develop *awareness* among team members
- Have thorough, well-defined controls
- Secure the network
- Test the environment regularly
- Be proactive about risk management

eds.com

EXPERTISE. ANSWERS. RESULTS.