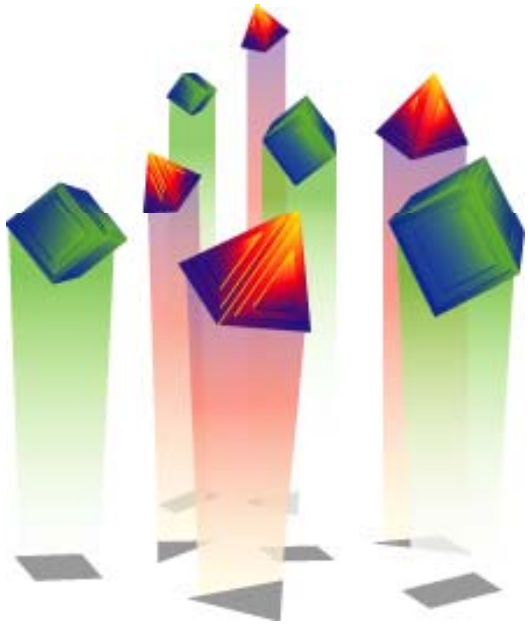
Every Network Manager Needs to Know about information Security, Compliance, and Risk Management

Share Session Boston



Laura Knapp
WW Business Consultant
Applied Expert Systems
Laurak@aesclever.com

Security as a Business Initiative

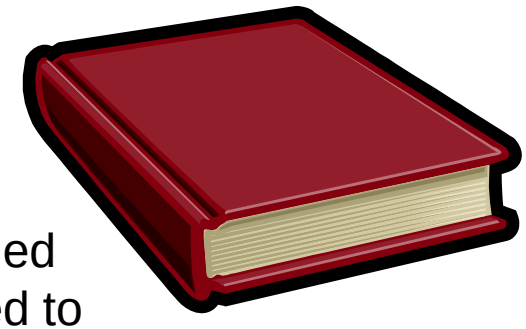
(focus on Information Security)

What needs to be secured

Security Horror Stories

Security Best Practices

Definitions



Enterprise risk management

"… is a process, effected by an entity's board of directors, management, and other personnel, applied in a strategy setting across the enterprise, designed to

– identify potential events that may affect the entity, and

– manage risk to be within its risk appetite,

– to provide reasonable assurance regarding the achievement of entity objectives." (COSO, 2004, p. 2)

Information security [& compliance] risk mgmt

– is intended to "balance the benefits gained from the use of … information systems with the risk of these … systems being the vehicle through which [threats] cause mission or business failure." (NIST, 2007, p. 1), and "is made up of *Information security incorporated into the*

- Enterprise architecture
- System development life cycle ("birth-to-death") (NIST, 2007, P.1)

Compliance Definitions

- Compliance should be a **program** based on defined **requirements**
- Requirements are fulfilled by a set of mapped **controls** solving multiple regulatory compliance issues
- The program is embodied by a **framework**
- Compliance is more about **policy**, **process** and **risk management** than it is about technology

Security is a Business Problem

Evolving Threats to Enterprise Infrastructure

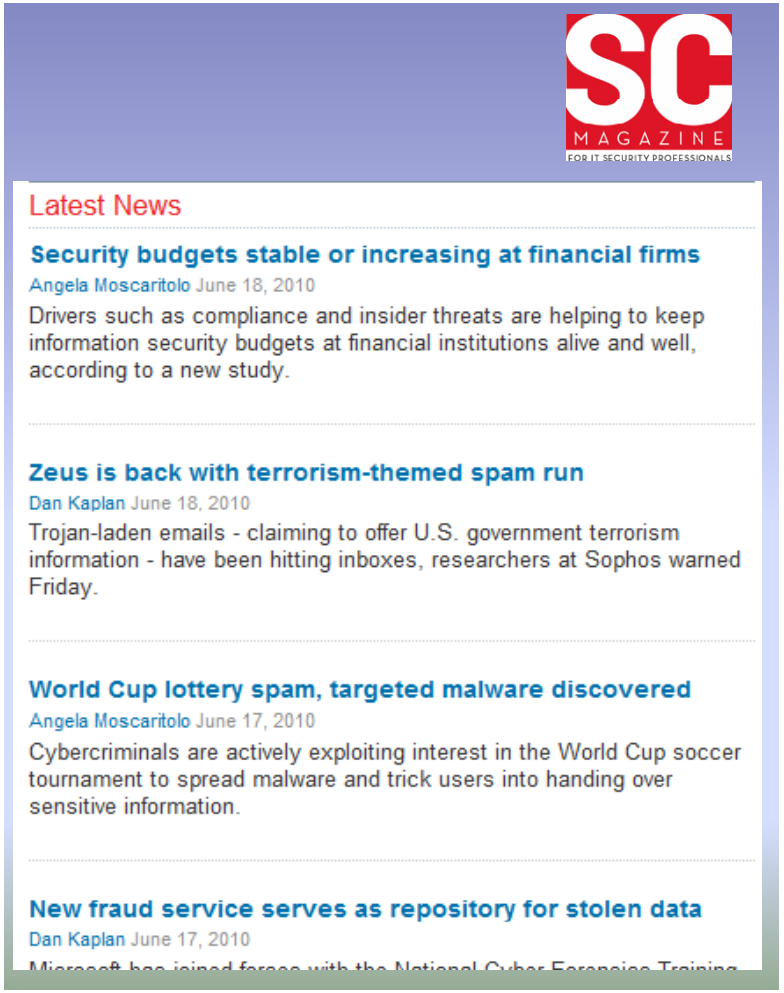
- Malicious code (Trojans, viruses, worms, spyware)
- SPAM
- Unlimited and uncontrolled access (Wireless LANs, 3G, 4G)
- Hackers and Insider sabotage
- Data stolen by employee or business partner or hacker
- Data viewed by unauthorized users
- Access controls as the definition of an employee changes

Infrastructure complexity creates exposures

- Miss-configurations
- Application vulnerabilities
- Employee errors (unintentional)
- Deployment of new technology
- Uncorrected, ongoing policy violations
- More interconnected partners, outsourcing
- Disappearance of clearly defined perimeter

Security Resources stretched by new threats

Involves information security, people security, asset security, ……

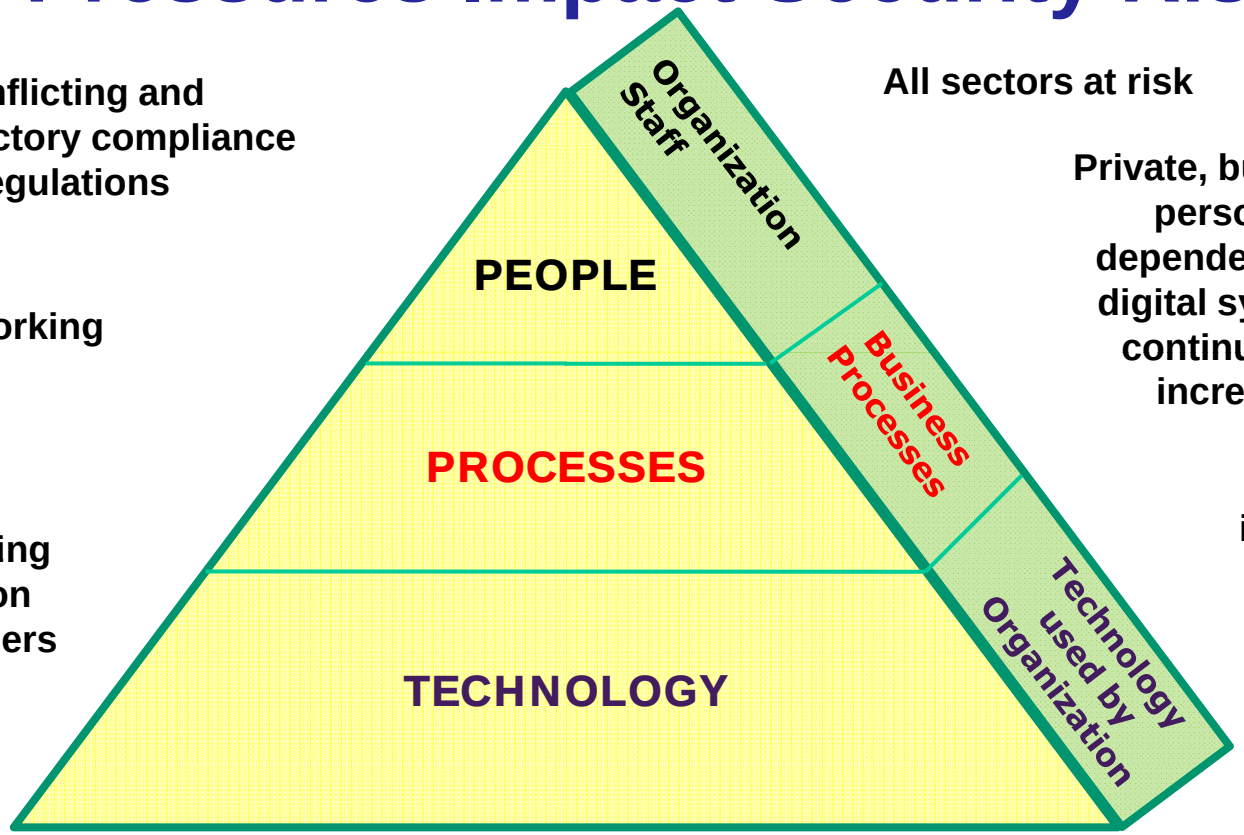


Many Pressures Impact Security Risk

Conflicting and contradictory compliance regulations

Social networking

Inconsistent information sharing and collaboration among stakeholders



All sectors at risk

Private, business, personal dependence on digital systems continues to increase

Uneven implementation of security across an increasingly complex business

Blurring of 'business/network perimeter'

Expanded touch points into networks/business

Growing capability of adversaries to exploit advantage

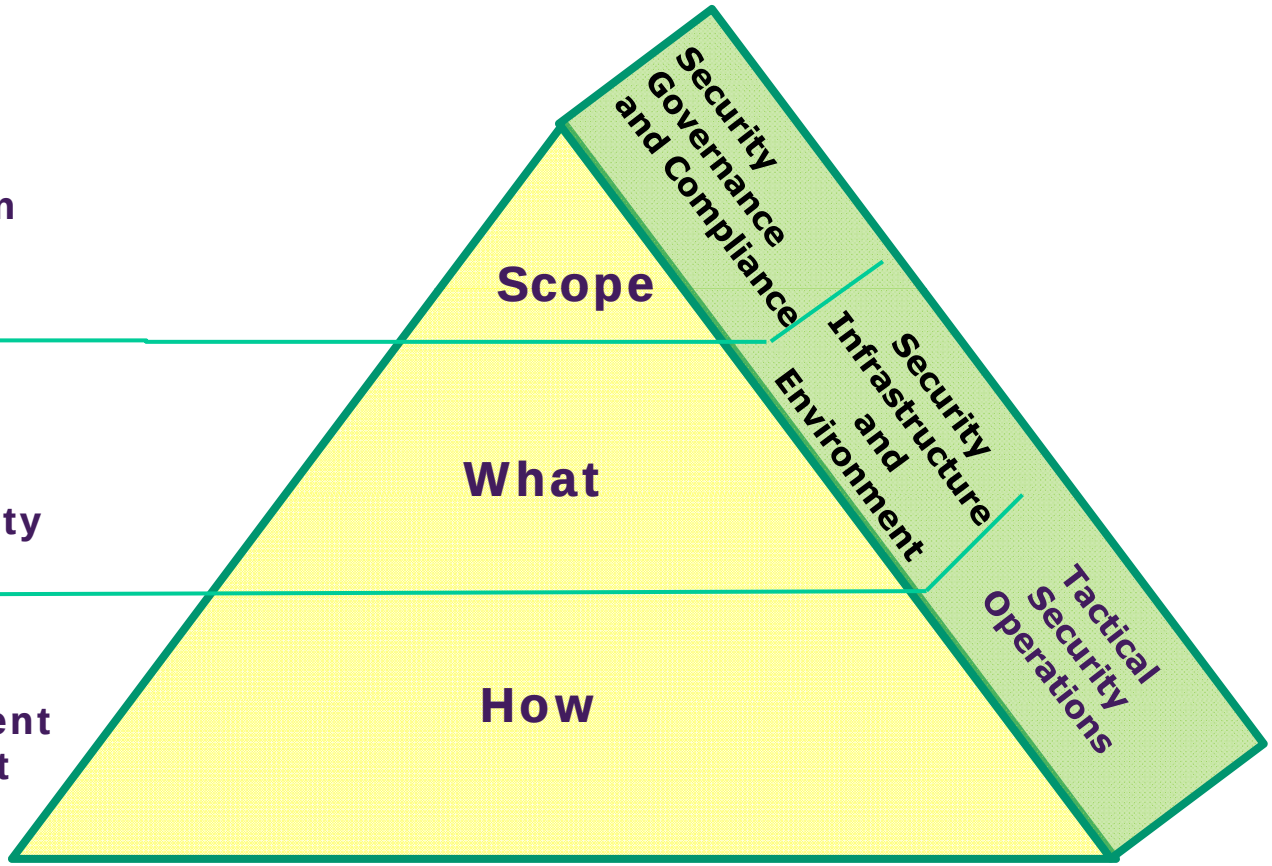
Security is a Multiple Element Problem

an ISO 27002 view

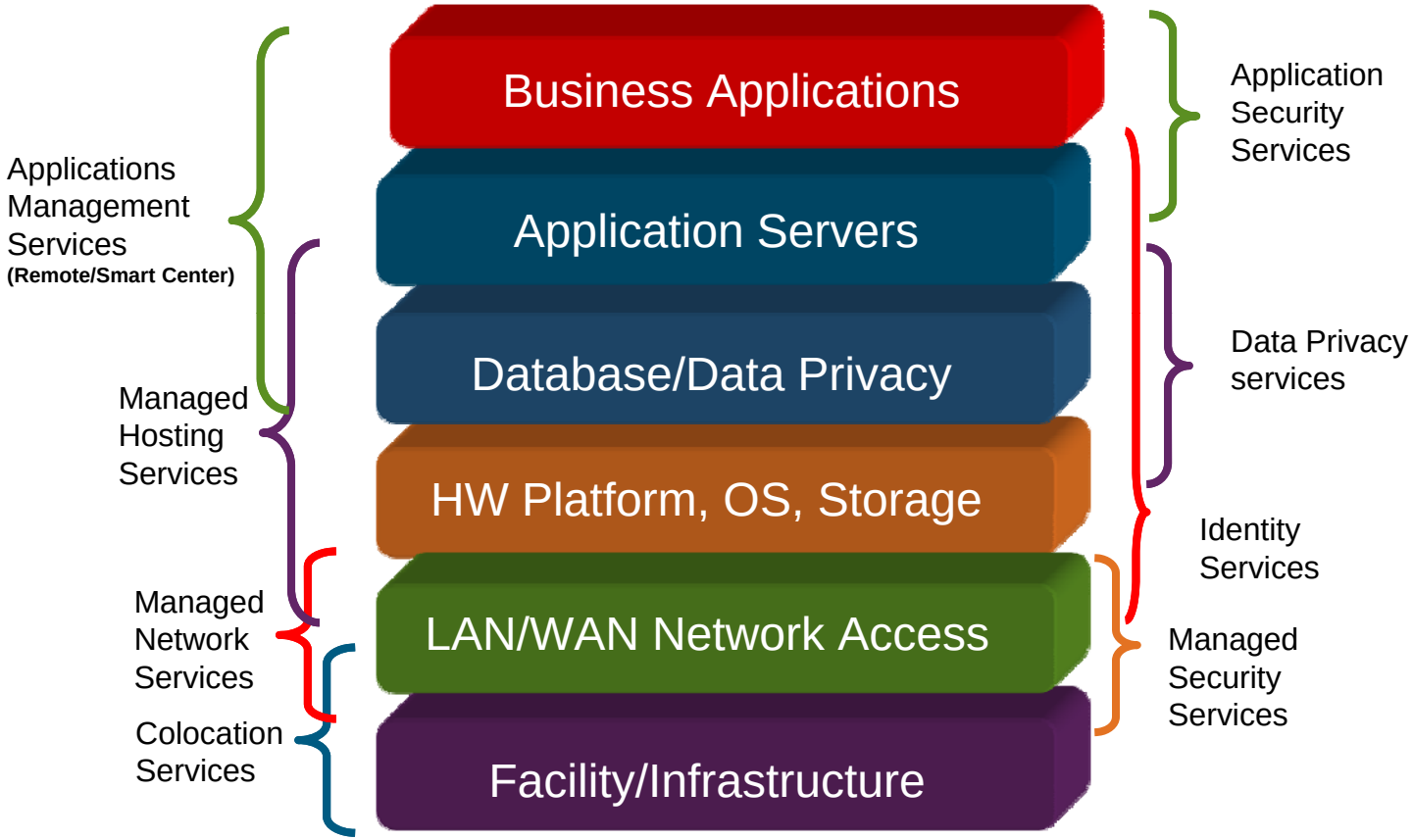
- Security Policy
- Security Organization
- Compliance
- Risk Assessment

- Human Resources
- Asset Management
- Physical and Environmental Security

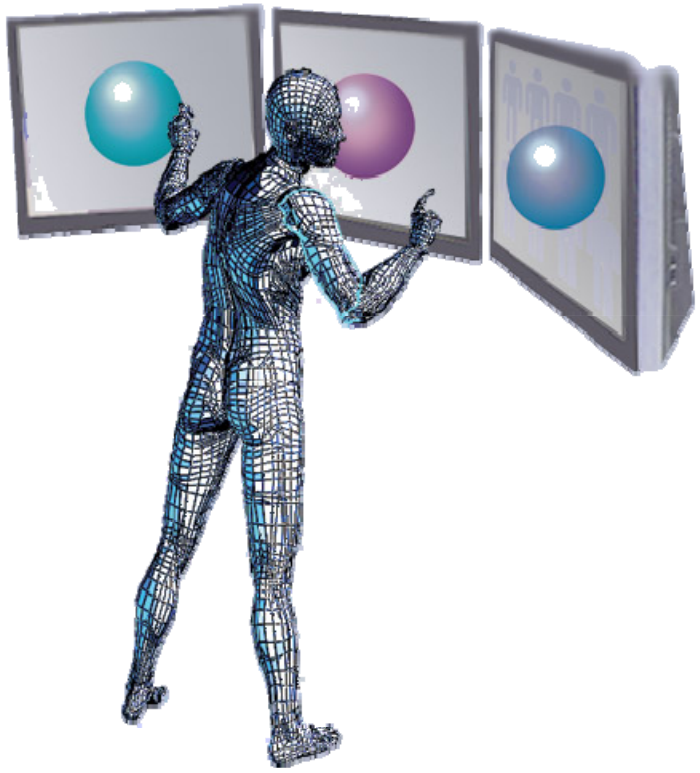
- Access control
- Communications and Operations Management
- Incident Management
- Business Continuity Management
- System Development and Maintenance



Elements of Security



A few of the Security Threats



- Imposition of legal and regulatory obligations.
- Cyber-criminals
- Malware, Trojans
- Phishers
- Spammers
- Negligent staff
- Storms, tornados, floods - Acts of God
- Hackers
- Unethical Employees who misuse/misconfigure system security functions
- Unauthorized access, modification, disclosure of, information assets
- Nations attacking critical information infrastructures to cause disruption.
- Technical advances that can render encryption algorithms obsolete

The Impact of a Security Breach

- Disruption to organizational routines and processes
- Direct financial losses through information theft and fraud
- Decrease in shareholder value
- Loss of privacy
- Reputational damage causing brand devaluation
- Loss of confidence in IT
- Expenditure on information security assets and data damaged, stolen, corrupted or lost in incidents
- Loss of competitive advantage
- Reduced profitability
- Impaired growth due to inflexible infrastructure/system/application environments
- Injury or loss of life if safety-critical systems fail
- Theft of trade secrets exceeded $1 trillion in 2008 and continues to escalate
- Over 40% of U.S. businesses have reported intellectual property losses in 2008

Security as a Business Initiative
(focus on Information Security)

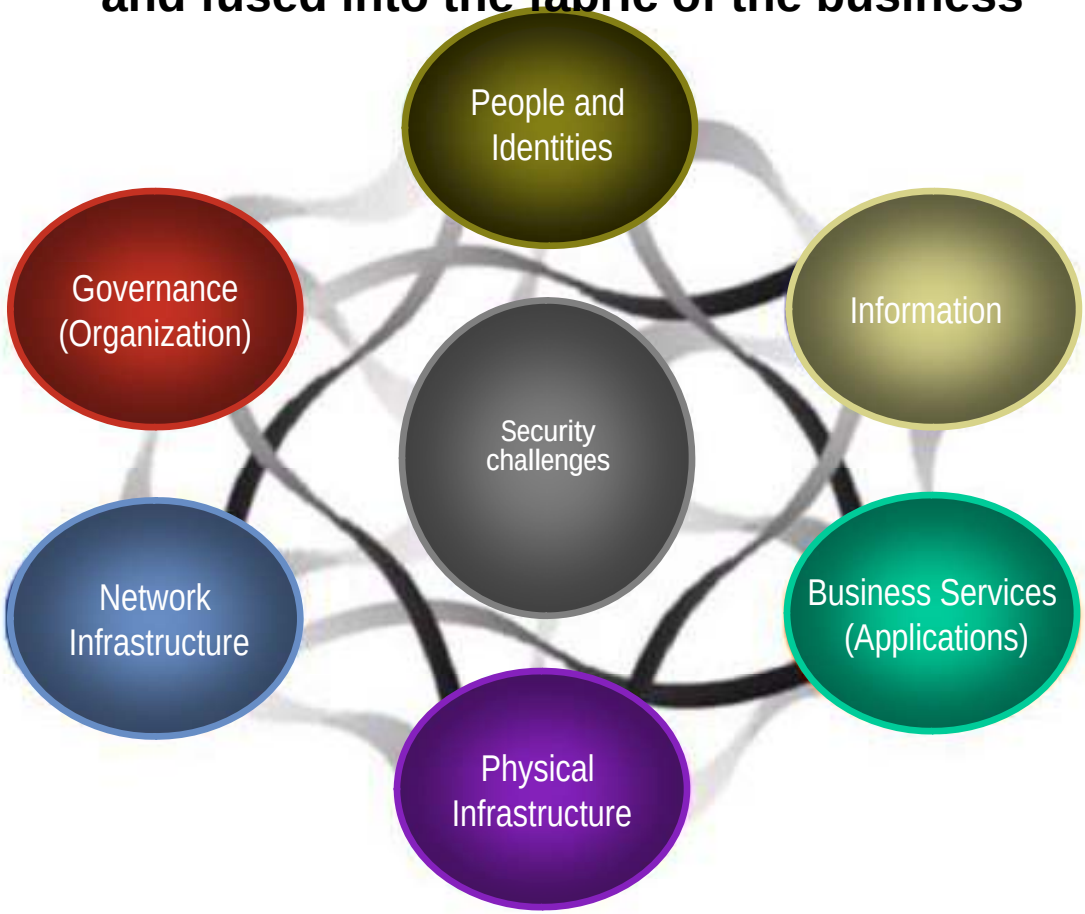
What needs to be secured

Security Horror Stories

Security Best Practices

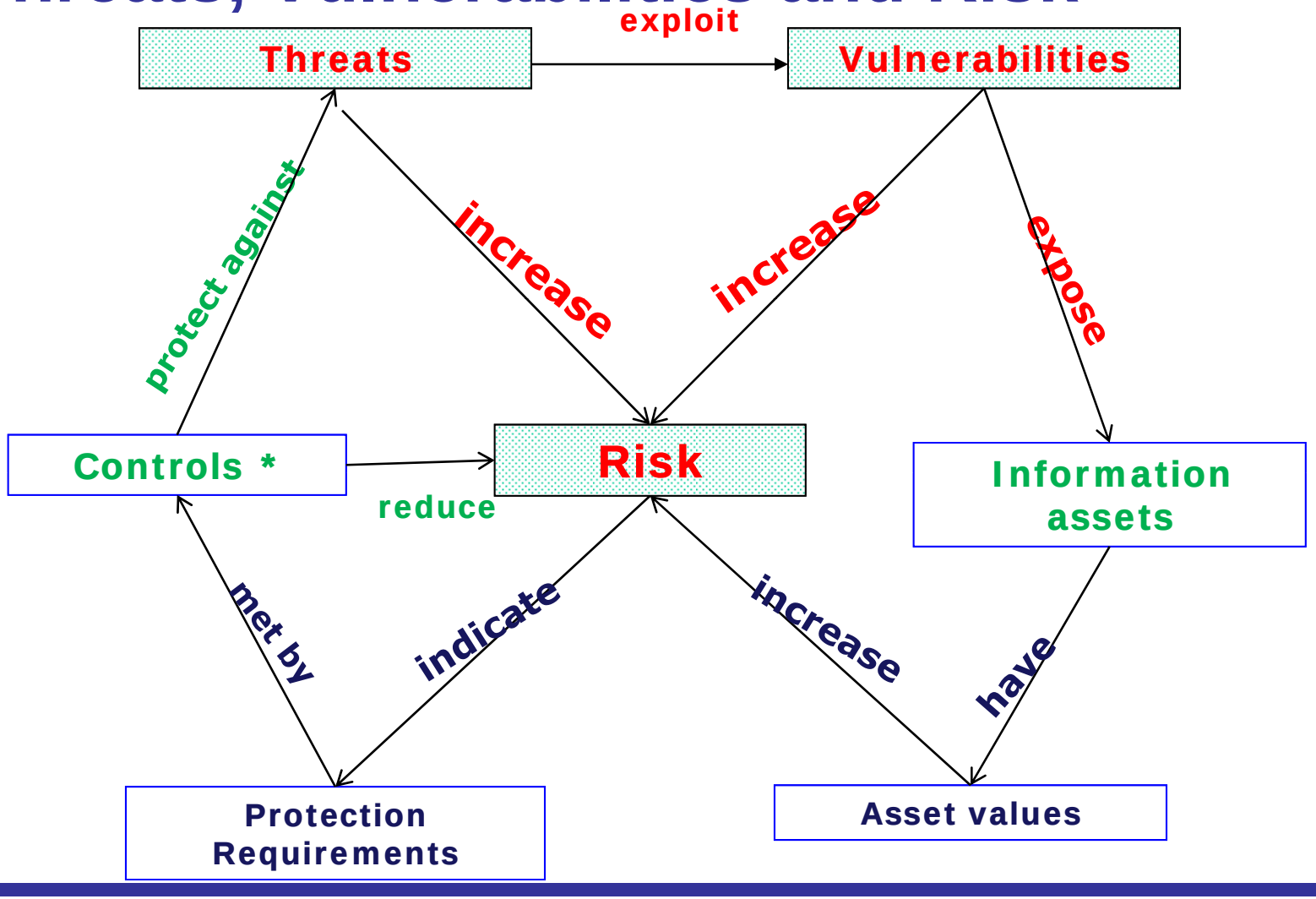
Security Focus Areas 2010

Security has to be applied within a business context and fused into the fabric of the business



Not as a widget to solve the next security threat

Threats, Vulnerabilities and Risk



Common Threats

No	Categories of Threat	Example
1	Human Errors or failures	Accidents, Employee mistakes
2	Compromise to Intellectual Property	Piracy, Copyright infringements
3	Deliberate Acts or espionage or trespass	Unauthorized Access and/or data collection
4	Deliberate Acts of Information extortion	Blackmail of information exposure / disclosure
5	Deliberate Acts of sabotage / vandalism	Destruction of systems / information
6	Deliberate Acts of theft	Illegal confiscation of equipment or information
7	Deliberate software attacks	Viruses, worms, macros Denial of service
8	Deviations in quality of service from service provider	Power and WAN issues
9	Forces of nature	Fire, flood, earthquake, lightening
10	Technical hardware failures or errors	Equipment failures / errors
11	Technical software failures or errors	Bugs, code problems, unknown loopholes
12	Technological Obsolesence	Antiquated or outdated technologies

Data Breach - Breakdown of Direct Costs

	2007	2008	2009 Q1
Direct Costs*	$/record	$/record	$/record (est.)
•Detection/Escalation	9	8	7
•Notification	15	15	15
•Ex-Post Response	46	39	33
Total Direct Costs	**70**	**62**	**55**
# of Records			
•ITRC	127,717,243	35,691,255	1,552,955
•OSF	164,461,103	83,695,422	516,463
Total Direct Cost Range	$B		
	11.2 - 16.7		

**Data Source: Ponemon Institute*

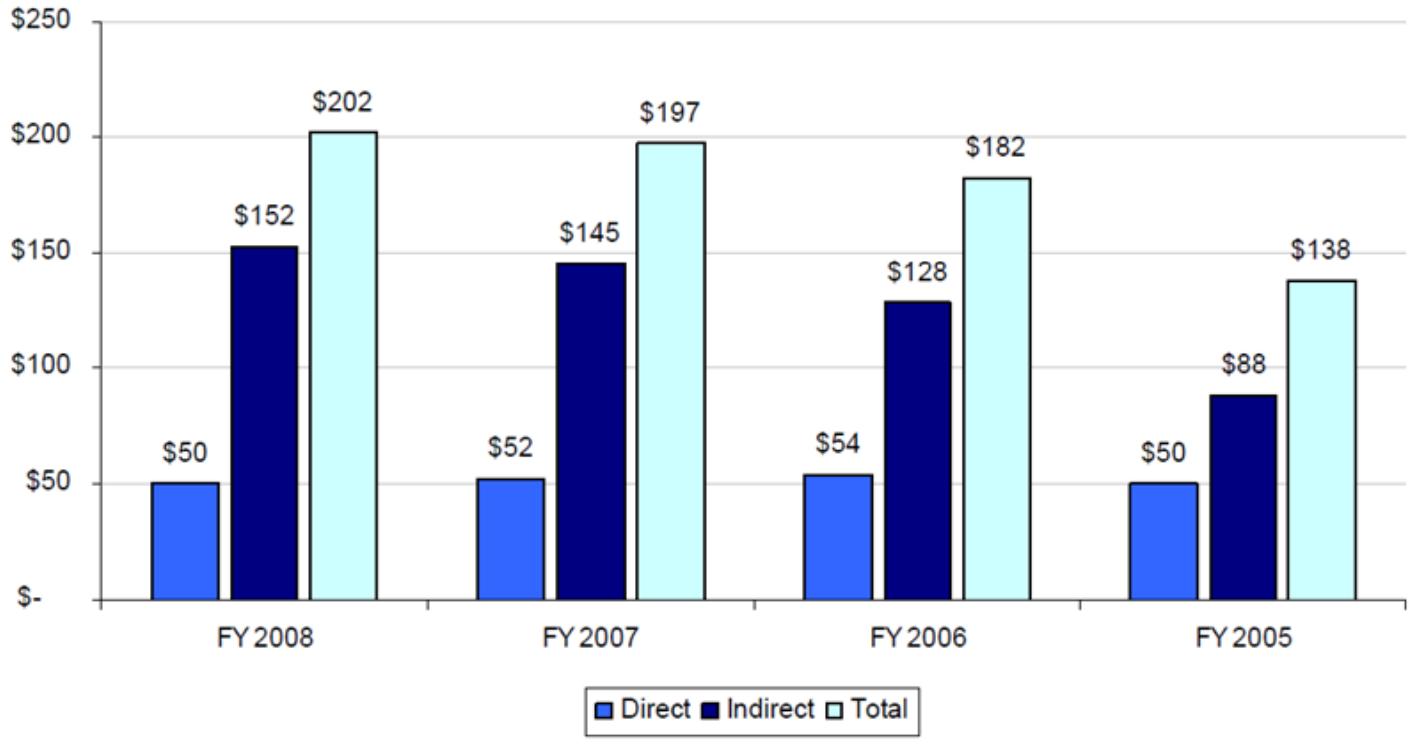
Data Breach - Indirect Costs

	2007	2008	2009 Q1
Indirect Costs	**$/record**	**$/record**	**$/record**
• Lost Business (Churn)	98-128	128-139	139-151
• Loss of Shareholder Value	(See Below)	(See Below)	(See Below)
• Lowered Productivity	15-30	15-30	15-30
• Opportunity Cost	20-100	20-100	20-100
• Miscellaneous Liabilities	0-25	0-25	0-25
• Additional Security	0-10	0-10	0-10
• **Total Indirect Costs**	**133-293**	**163-304**	**174-316**

Note that the cost data for 1st QTR 2009 are an estimate based on the percentage change from 2007-2008

Data Source: Ponemon Institute, Forrester Research, and OSF

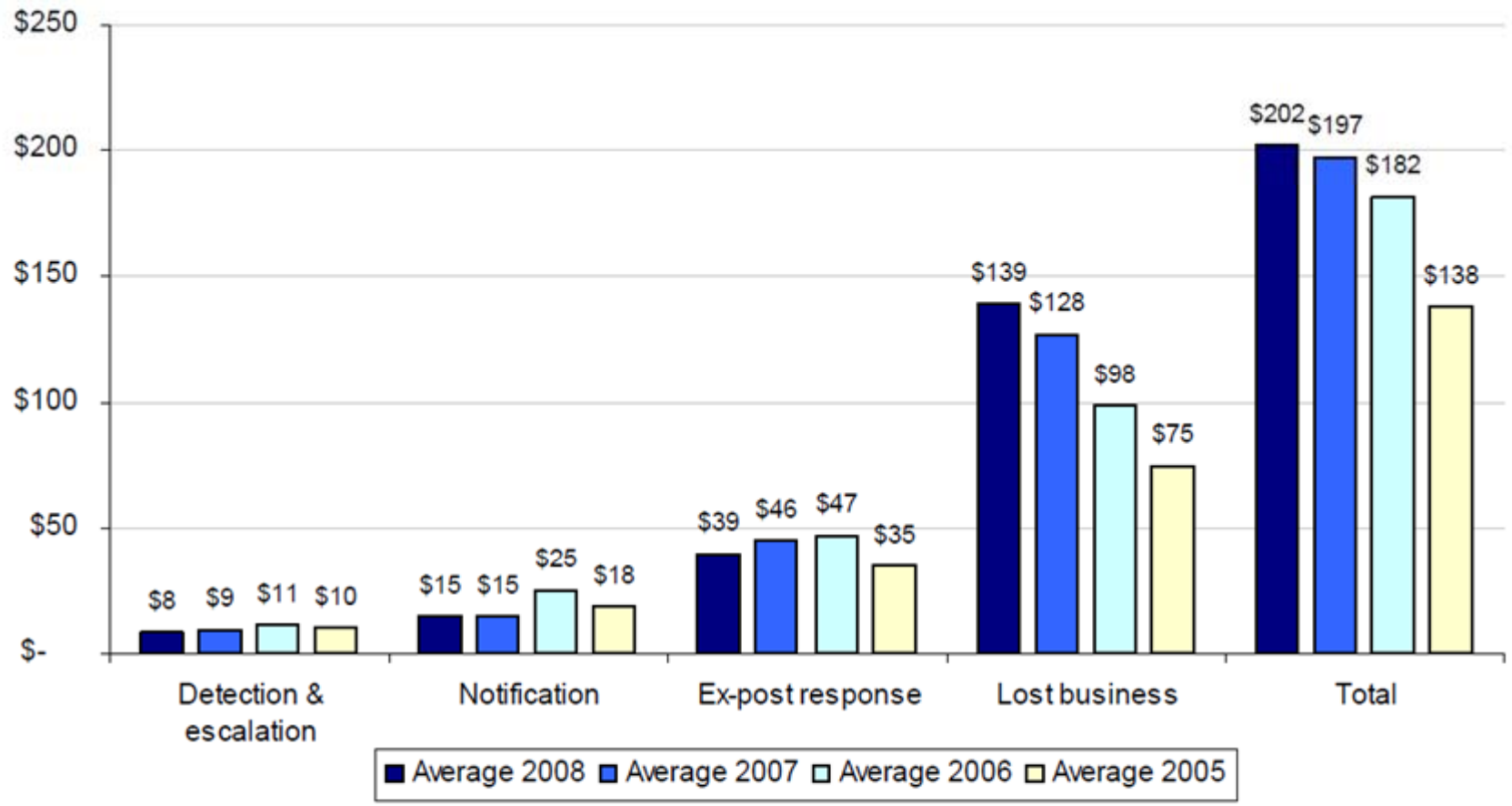
Overall Costs - Trends



- Direct costs have moderated
- Indirect costs have continued to increase

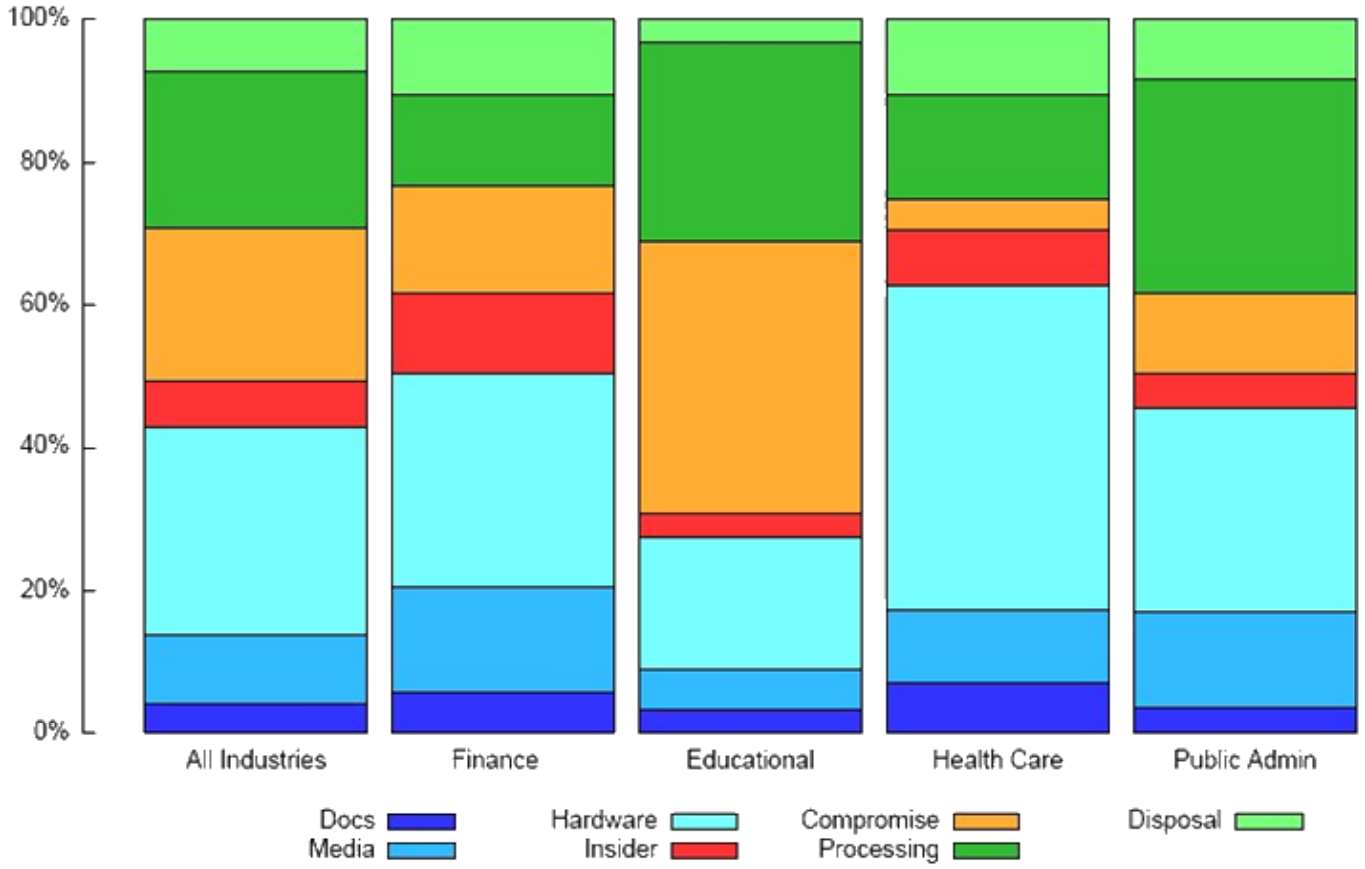
Data Source: Ponemon Institute

Data Breach - Overall Costs - Breakdown



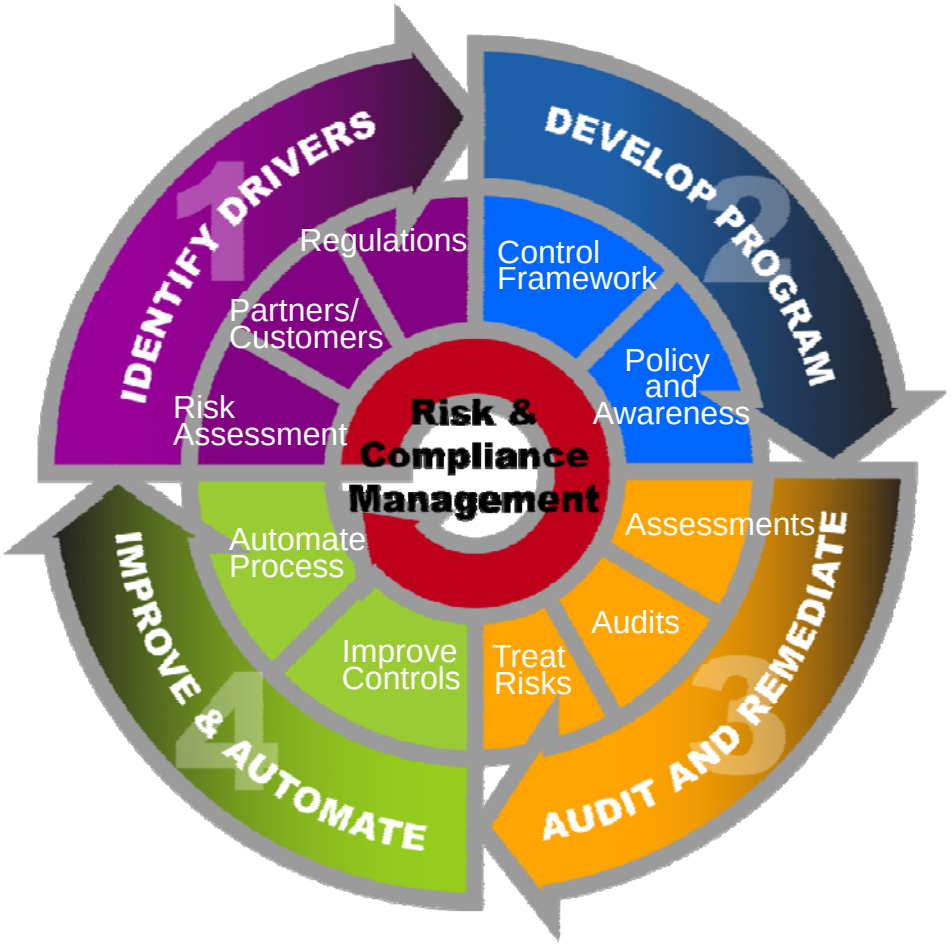
Applications AES aesclever.com

Cause of Data Breaches by Industry



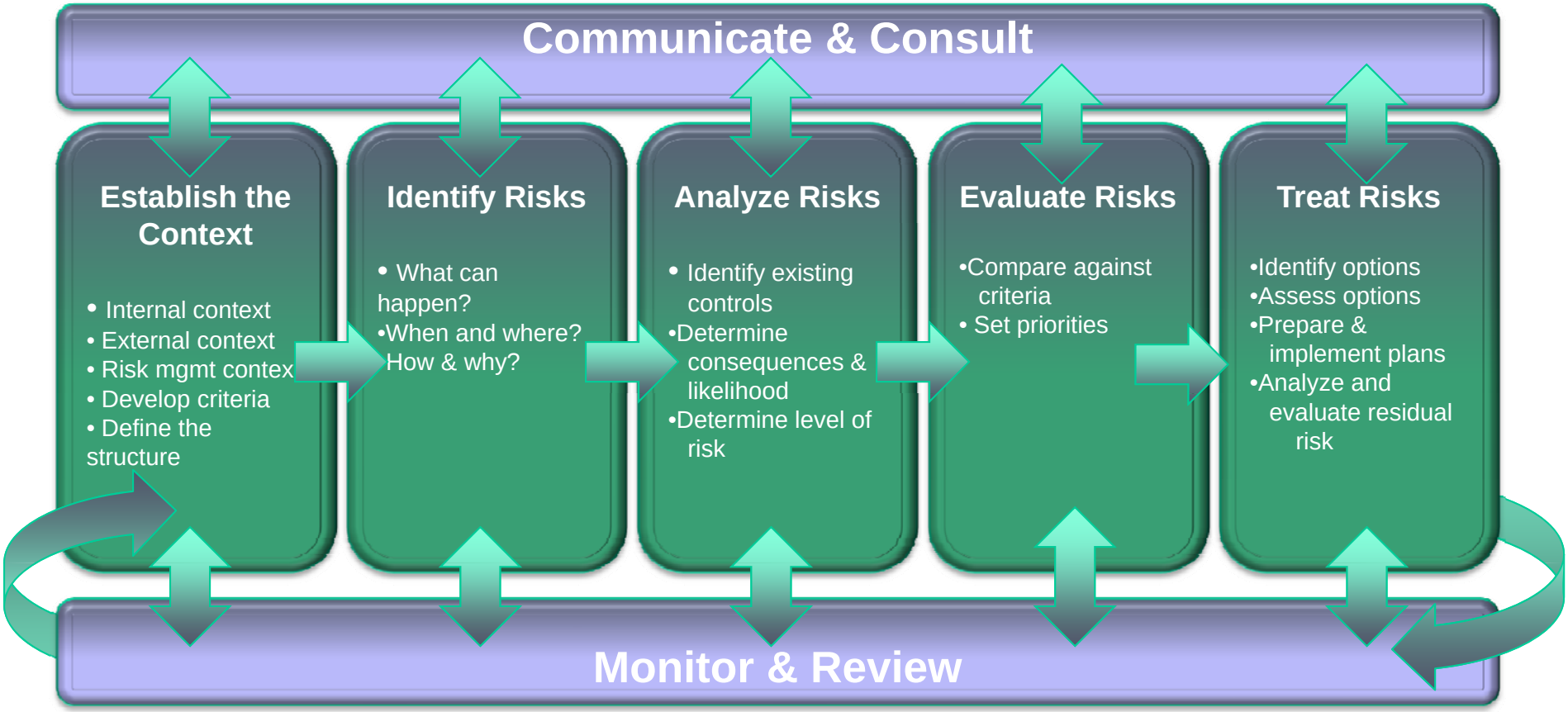
Data Source: DataLossDB

Prevention is the key



Minimal	Sustainable	Optimized
• Annual / Project-based Approach • Minimal Repeatability • Only Use Technologies Where Explicitly Prescribed in Standards and Regulations • Minimal Automation	• Proactive / Planned Approach • Learning Year over Year • Use Technologies to Reduce Human Factor • Leverage Controls Automation Whenever Possible	• Regulatory Requirements are Mapped to Standards • A Framework is in Place • Compliance and Enterprise Risk Management are Aligned • Process is Automated

Risk Assessment



Source: AS/NZS 4360:2004

Did Your Risk Assessment Include?

Core Functions

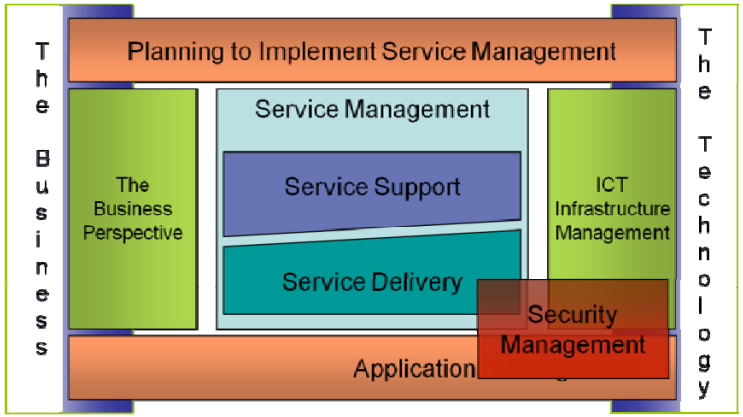
- Capability that allows for granular protection of unstructured and structured data, as well as leak prevention and acceptable use policy monitoring
- Managed security operations center or in-house Service Desk solutions designed to assure incidents are escalated and addressed in a timely manner. Forensics teams ready to respond to an emergency and reporting on security and compliance posture across the enterprise

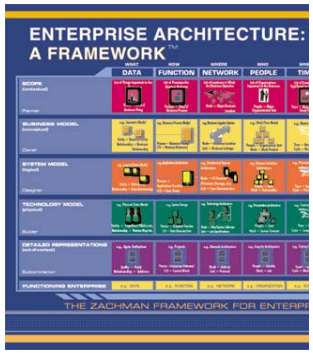
Process

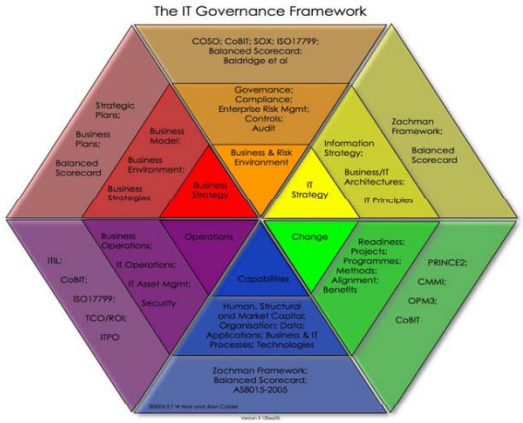
- Process for assuring routine, emergency and out-of-band changes are made efficiently, and in such a manner as to prevent operational outages
- Process for assuring efficiency and integrity of the software development lifecycle
- Process and capabilities designed to protect enterprise infrastructure from new and emerging threats
- Process for assuring access to enterprise resources has been given to the right people, at the right time

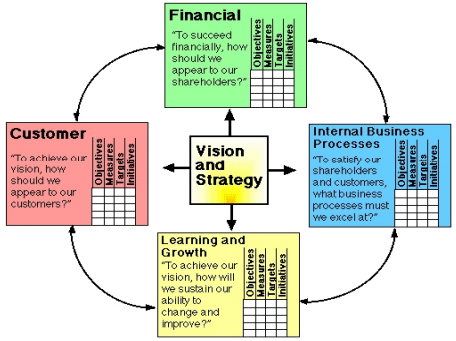
22

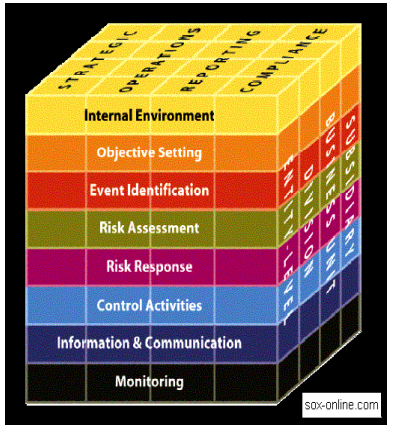
Many Frameworks Exists











- No framework best for all
  - no one-size-fits-all in security
- No framework sole source for any enterprise
  - multiple frameworks, multiple perspectives
- Which one addresses a viewpoint you haven't used?

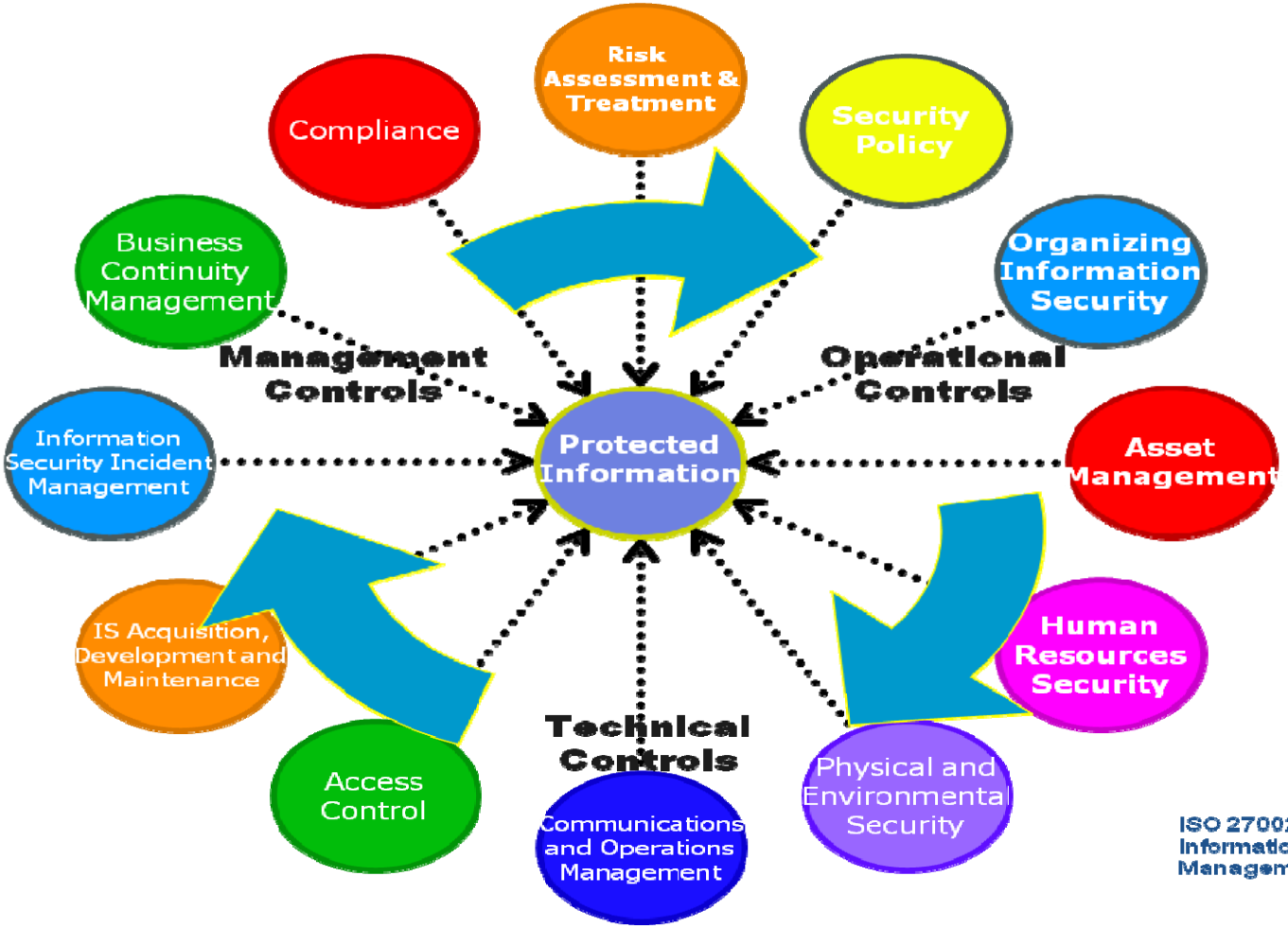
What is in a Framework?

Guidelines, Principles,Standards, Frameworks/breakdowns/structures,Checklists,Software,"Best Practice",Audit guidelines/outlines,Legislation,Reporting standards, Product evaluation

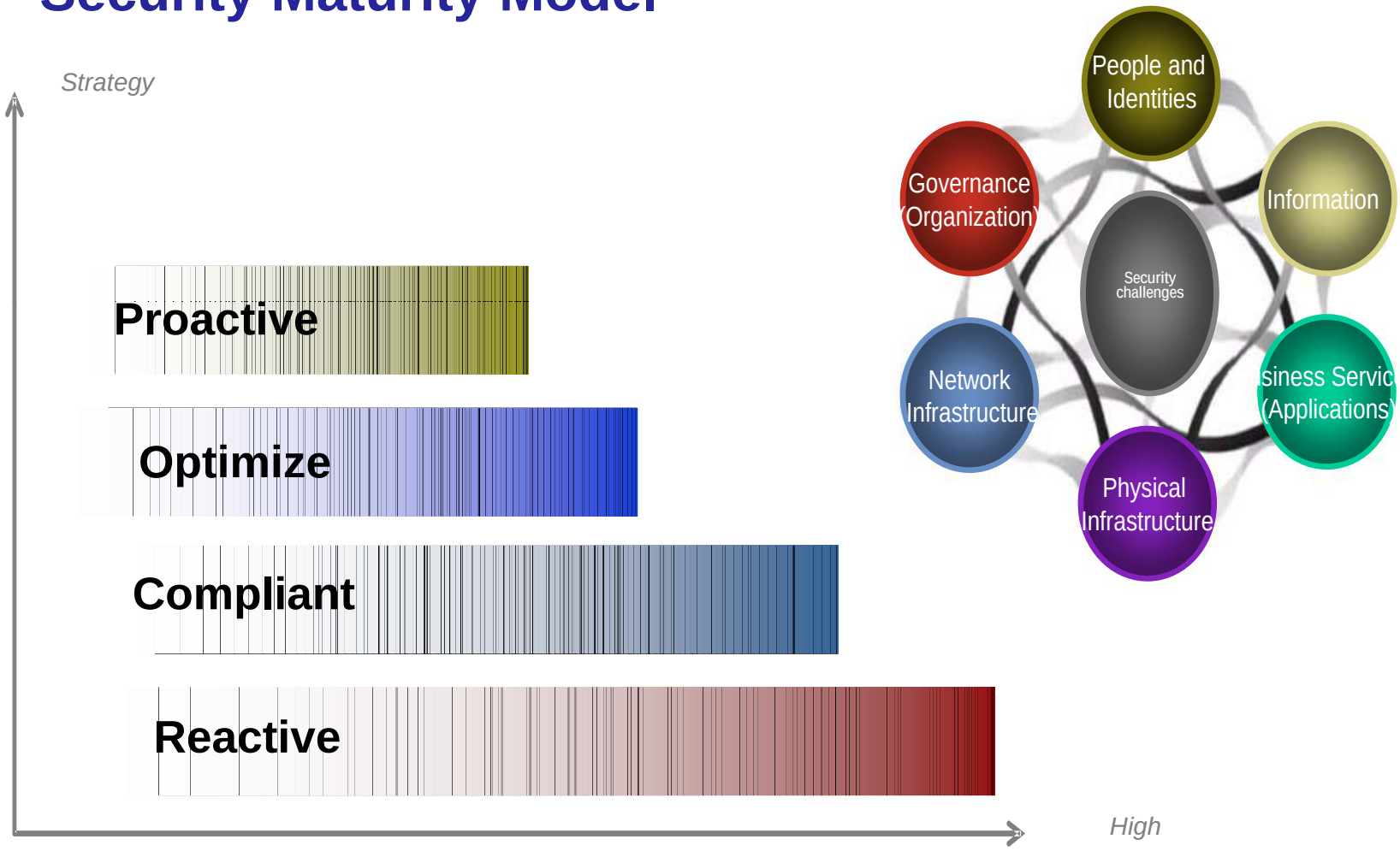
	Deterrent	Preventive	Detective	Corrective	Recovery	Compensating
Administrative	Policy	User registration procedure	Review violation reports	Termination	DR plan	Supervision, Job rotation
Technical	Warning banner	Password based login, IPS	Logs, IDS	Unplug, Isolate, Terminate connection, Checkpoint restart	Tape backups, fault tolerance, RAID	Diskless workstations, thin clients
Physical	Beware of dog sign	Fence	Sentry, CCTV	Fire Extinguisher	Reconstruction, Rebuild	Layered defense

Process Oriented (CMMI, Cobit, ISM3, ISO10000, ITIL)
Controls Oriented (BSI-ITBPM, ISO27001, ISO1335-4)
Product oriented (Common Cirteria)
Risk Management Oriented (AS/NZS, CRAMM, Octave, SOMAP)
Best Practice Oriented (IASO 27002, ISF)

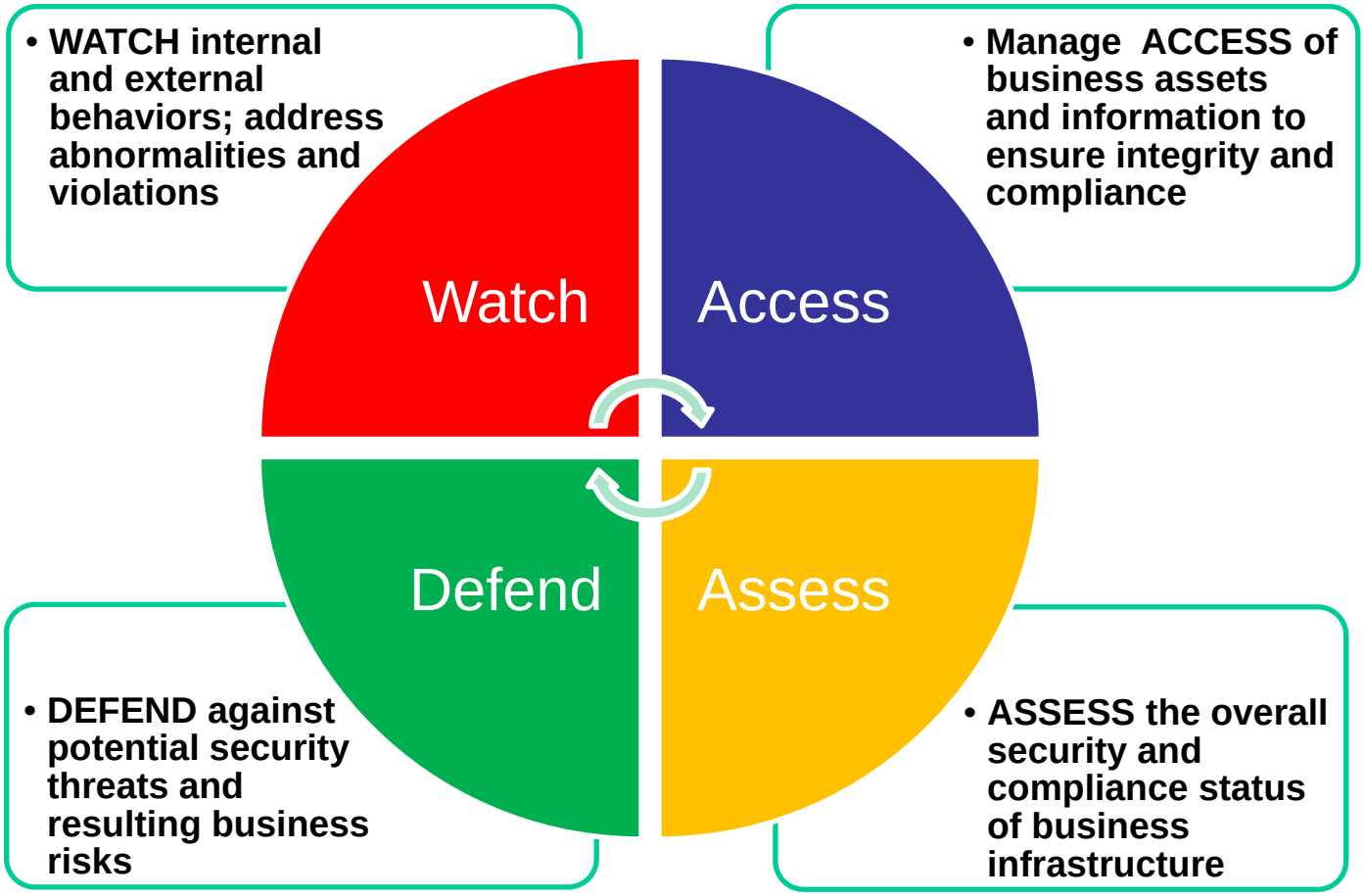
A Framework Should Include



Security Maturity Model



Four Elements of a Operational Security Strategy



Security as a Business Initiative
(focus on Information Security)

What needs to be secured

Security Horror Stories

Security Best Practices

Employee Trust

•Construction Company

•Senior IT person also in charge of security
•Used cost issue to convince upper management to let him store data at his home rather than pay for external off-site storage
•Conflict arose between the Employee and Employer
•Employee sent email's to clients of the construction company indicating he had personal information
•Took 6 months to shut down the rogue employee after the employee used the internet to threatened people at which time the FBI became involved
•Construction company was fundamentally out of business

http://www.cio.com/article/454614/IT_Security_Pros_Share_Horror_Stories

Process Vulnerability

•Security administrator asked to shut off web security monitoring system as it was interfering with marketing's ability to access the corporate web site for creation and editing.
•Director said 'switch off' not….. find a work around…find a fix….just 'switch it off'
•Users quickly found that out that all web controls were no longer active
•A report surfaced that a user had used a desktop to access porn
•Due to the use of generic accounts tracking activity to a user was not possible
•Took 3 months, CCTV, internal and external police to finally catch the culprit
•To make matters worse the company dropped any further work on a security framework and made the security positions obsolete

itnews
FOR AUSTRALIAN BUSINESS

KASPERSKY lab

News | Technology | Business | Forums

Reviews | Galleries | Events | Net Seminars | Whitepapers | Downloads | Newsl

Home > News > Technology > Security > Security experts beaten at their own game

SECURITY

Security experts beaten at their own ga

By Tom Sanders
Feb 9, 2007 1:36 PM
Tags: security | experts | beaten | own | game

RSA Conference delegates leave themselves wide open to attack.

More than half of the computers used by security experts attending the RSA Conference in San Francisco this week lack the proper protection and may have been compromised, according to wireless security firm AirDefense.

The company scanned all wireless traffic on the first day of the conference and found a total of 623 Wi-Fi enabled notebooks and mobile phones.

Some 56 per cent of these devices were configured automatically to log-on to networks with common names such as 'Linksys' or 'T-Mobile', a feature known as an open access wireless account.

Attackers could exploit the feature through a so-called man-in-the-middle

- RSA conference 2007
- Over half the computers lacked proper protection
  - Many configured to automatically log on to WiFI networks like ‘Linksys’ ‘T-Mobile’
- Five rogue networks mimicked common hotspot names
  - These could easily insert man in the middle routines and capture data
- The RSA conference had a SAFE WIFI network but it was toooooo complex to use and the help desk line was long and slow

2009 Litigation Highlights

Starwood v. Hilton (2009) - Complaint alleging that 2 former Starwood execs looted >100k Starwood computer files.

U.S. v. Chung (2009) – Boeing employee convicted at trial for passing trade secrets to Chinese government for 30 years. Co-defendant convicted and jailed for 24 years; Chung, 74 years old, received 15 years in prison.

-US v. Zhu (2009) – Indictment alleging Chinese national employed as engineer at US environmental company stole software from his employer and sold modified version to Chinese government.

US v. Lee (2009) – Former technical director of paint and coating company quit 2 weeks after return from business trip to China; discovered downloaded trade secrets, deleted files, one way ticket from Chicago to Shanghai.

Vistakon v. Bausch & Lomb (2009) – Subsidiary of J&J alleges that B&L misappropriated trade secrets in an effort to recruit sales force to bring new contact lens product to market quickly.

Security as a Business Initiative
(focus on Information Security)

What needs to be secured

Security Horror Stories

Security Best Practices

Why Security Metrics are Important

- To show ongoing improvement;
- To show compliance (with Standards, contracts, SLAs, OLAs, etc);
- To justify any future expenditure (new security software, training, people, etc);
- ISO 27001 certification requires it. Other Management Systems also require it – ISO 9001, ISO 20000;
- To identify where implemented controls are not effective in meeting their objectives;
- To provide confidence to senior management and stakeholders that implemented controls are effective.

Benefits of Measuring Security

•Actually eases process of monitoring the effectiveness of the ISMS (e.g. less labor intensive, for example, if using tools, and provides a means of self checking);
•Proactive tools to measure / prevent problems arising at a later date (e.g. network bottlenecks, disk clutter, development of poor human practices);
•Reduction of incidents, etc;
•Motivates staff when senior management set targets;
•Tangible evidence to auditors, and assurance to senior management that you are in control – i.e. Corporate Information Assurance (Corporate Governance), and top down approach to Information Assurance.

What should be measured?

1.Management Controls: Security Policy, IT Policies, Security Procedures, Business Continuity Plans, Security Improvement Plans, Business Objectives, Management Reviews

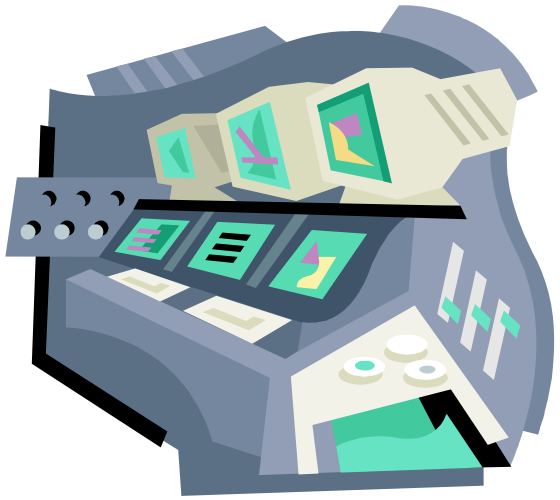
2.Business Processes: Risk Assessment & Risk Treatment Management Process, Human Resource Process, SOA selection process, Media Handling Process

3.Operational Controls: Operational Procedures, Change Control, Problem Management, Capacity Management, Release Management, Back up, Secure Disposal, Equipment off site

4.Technical Controls: Patch Management, Anti-Virus Controls, IDS, Firewall, Content Filtering

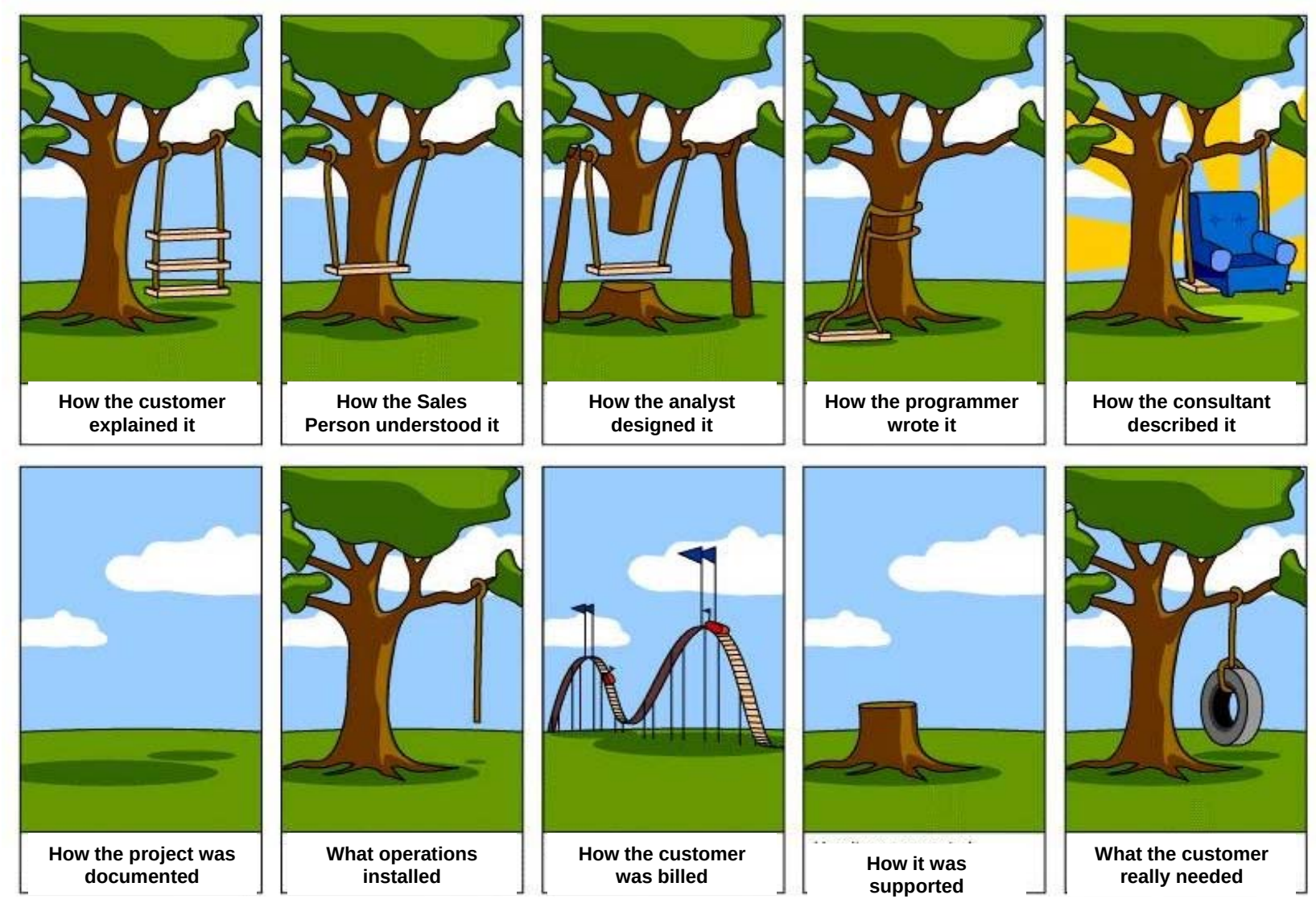
What controls should be used?

•Confirm relevance of controls through risk assessment;
•Define objectives, ensuring they map back to the business;
•Use existing Indicators wherever possible, e.g. in ITIL terms, KPIs:
•Within the ISMS audit framework, identify controls which can be continuously monitored, using chosen technique;
•Before using any tools, confirm the objectives with senior managers as well as staff. Corroborate with third parties, or through SLAs/OLAs where internal third parties are concerned e.g. ISO15000 (ITIL);



Processes to be used

- Establish a baseline, against which all future measurements can be contrasted/compared
- Provide periodic reports to appropriate management forum/ISMS owners (show graphs, pictures paint a thousand words)
- Identify Review Input – agreed recommendations, corrective actions, etc
- Implement improvements within your Integrated Management Systems (IMS) e.g. merged ISO's 9001, 14000, 27001, 20000
- Establish/agree new baseline, review the output, apply the PDCA approach (Plan – Do – Check – Act)



QUESTIONS?

laurak@aesclever.com
www.aesclever.com
650-617-2400

Our other presentations:

Monday, 3:00 am - 4:00 am: Introduction to TCP/IP
Tuesday, 11:00 am – 12:00 pm: What every network manager needs to know about security
Tuesday 1:30 pm – 2:30 pm: Diagnosing Mainframe Network Problems with Packet Trace
Wednesday 11:00 am – 12:00 pm: Cloud Computing Environment
Wednesday 1:30 pm – 2:30 pm: Hot Topics in Networking and Security
Wednesday 4:30 pm – 5:30 pm: Wireless Security Challenges
Thursday 11:00 am – 12:00 pm: Virtualization – The Evolution of the Data Center