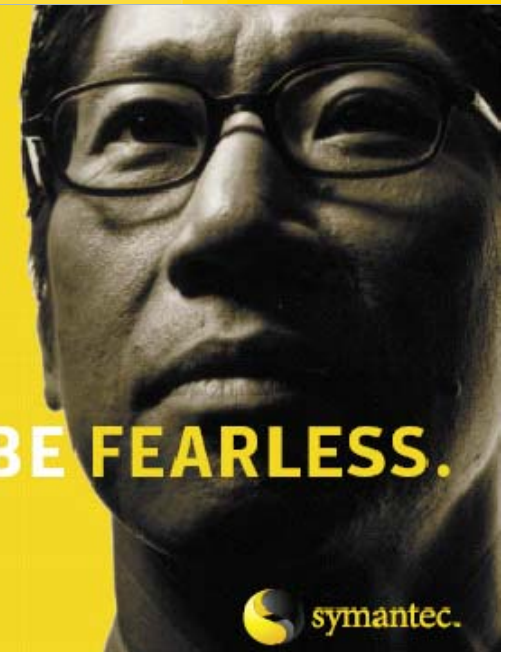
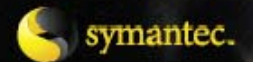




Overcoming the Barriers to Regulatory Compliance

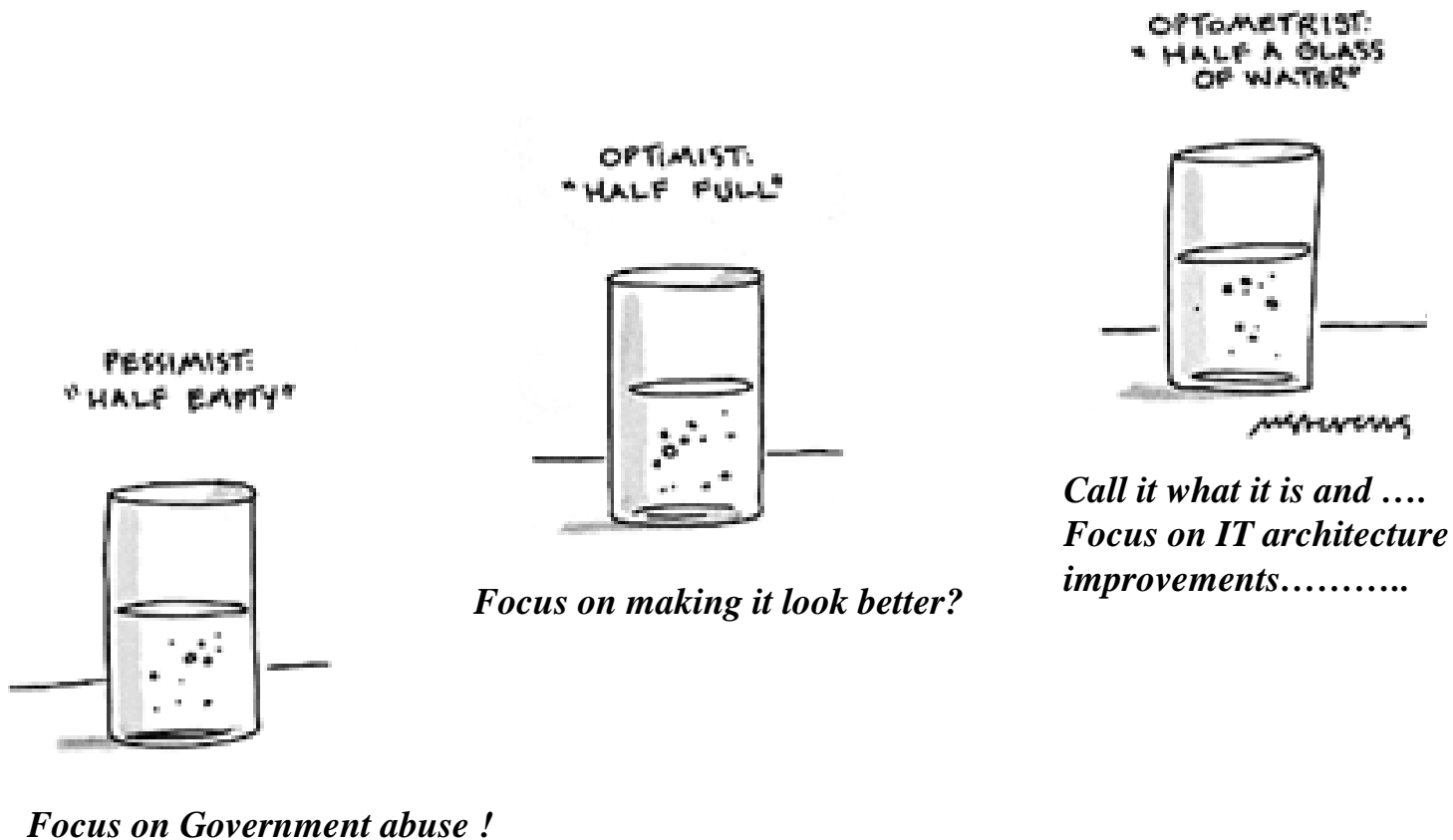
Don Kleinschnitz Jr.
Symantec Corp
VP Enterprise Administration Product Delivery
Don_kleinschnitz@symantec.com

* **BE FEARLESS.**





Paradigms for solving the problem?





Agenda



- ▶ Basic overview of regulations
- ▶ Implications for IT architecture
- ▶ Data protection through change control
- ▶ Data Retention with snapshots
- ▶ Summary

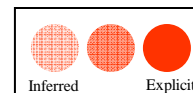


Many Regulations and Standards



Summary of requirements

Category	IT controls	SOX
Planning	IT Policy creation	●
	Control sensing, auditing and reporting	●
	Asset discovery & inventory	●
Security	Intrusion Detection & Protection	●
	Identity control	●
	Vulnerability assessment	●
Change Management	Provisioning	●
	Patch Remediation	●
Information Management	Disaster recovery	●
	Data Archive & Retention & Disposal	●



302: Executives certify accuracy of reports, disclose deficiencies and weaknesses in internal controls and corrective action

404: Design, implement, maintain and verify control structure. Auditors attest management assertions of control structure

409: communicate changes in financial state quickly, supported by information

802: Protection and retention of financial audit records for 5 years



Summary of requirements

Category	IT controls	SUM	SOX	HIPPA	FISMA
Planning and reporting	IT Policy creation	●	●	●	●
	Control sensing, auditing and reporting	●	●	●	●
	Asset discovery & inventory	●	●	●	●
Security	Intrusion Detection & Protection	●	●	●	●
	Identity control	●	●	●	●
	Vulnerability assessment	●	●	●	●
Change Management	Provisioning	●	●	●	●
	Patch Remediation	●	●	●	●
Information Management	Disaster recovery	●	●	●	●
	Data Archive & Retention & Disposal	●	●	●	●



Regulatory Compliance – Snapshot

WHO IT AFFECTS?

- ▶ All large & medium enterprises around the world have some level of regulation that impacts their business. It triggers:
 - ▶ Board of director interest
 - ▶ Penalties for non-compliance
 - ▶ Drive to improve corporate governance
 - ▶ Opportunity to streamline & open business processes
 - ▶ Challenges the current IT architecture

WHAT IS REQUIRED?

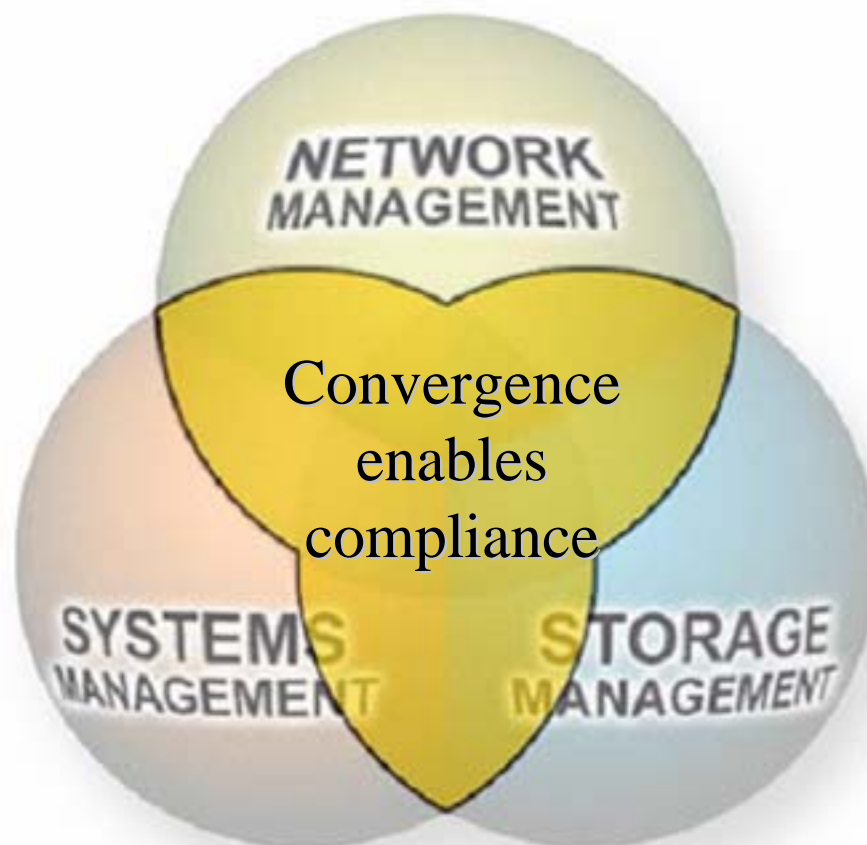
- ▶ Regulatory Compliances are directives from various government agencies to implement IT architectures that insure “due care is taken to protect the:
 - Confidentiality
 - Integrity
 - Privacyof information that impacts stakeholders:
 - Rights
 - Privileges
 - Safety

WHAT IT IMPLIES?

- ▶ **A more holistic and automated IT architecture converging Security, Systems and Storage disciplines**
- ▶ **An “infrastructure” with auditing capabilities**
- ▶ **Insurance that specific data is saved, archived and recoverable**

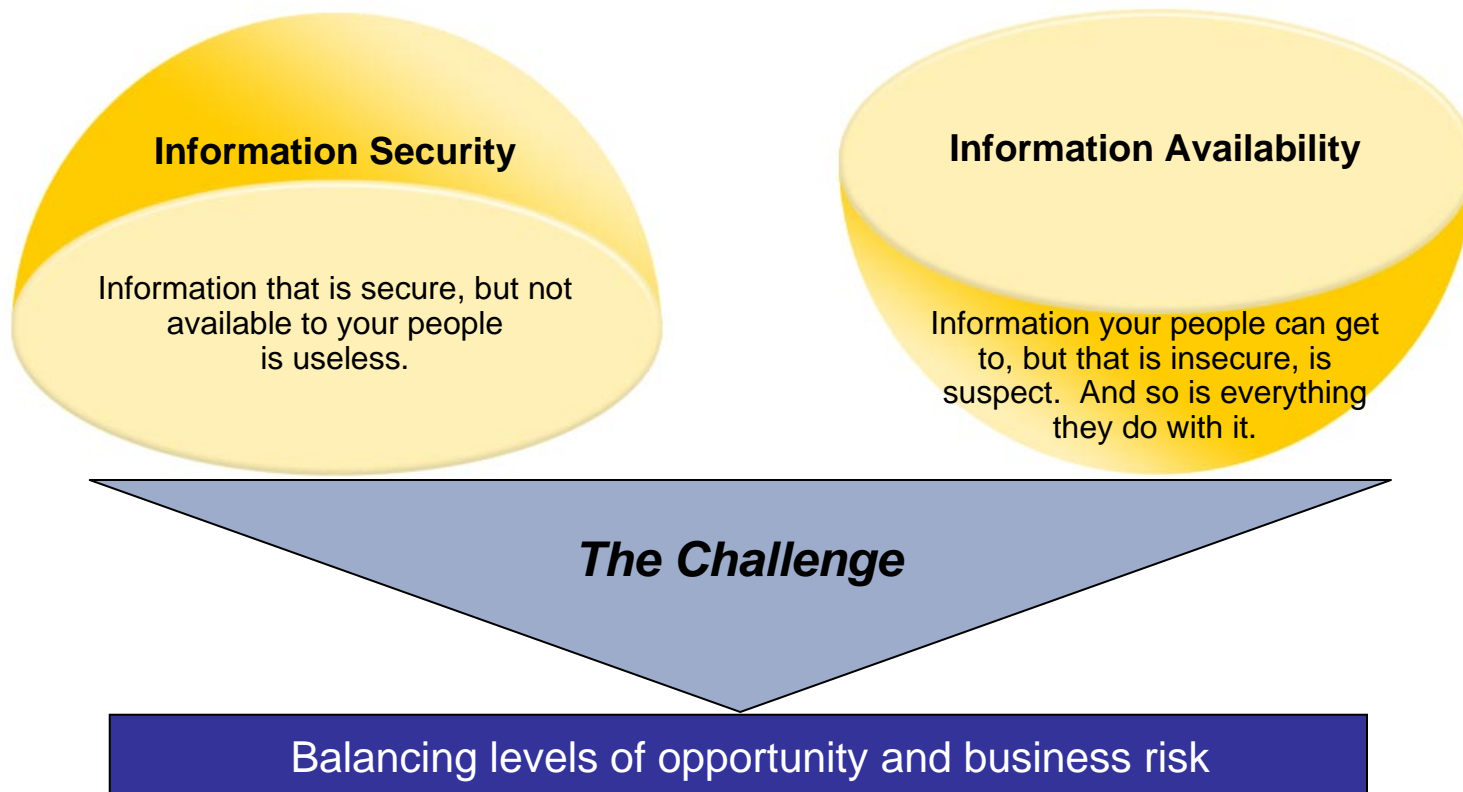


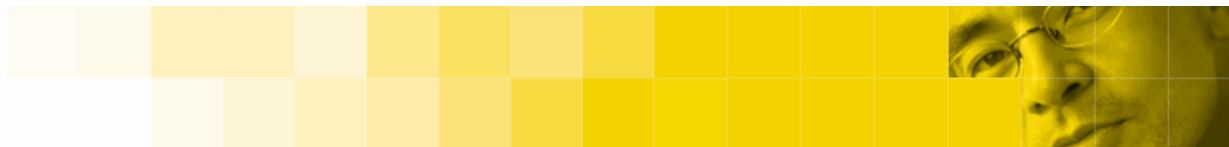
Convergence of Security and Operations is Essential





Information Integrity



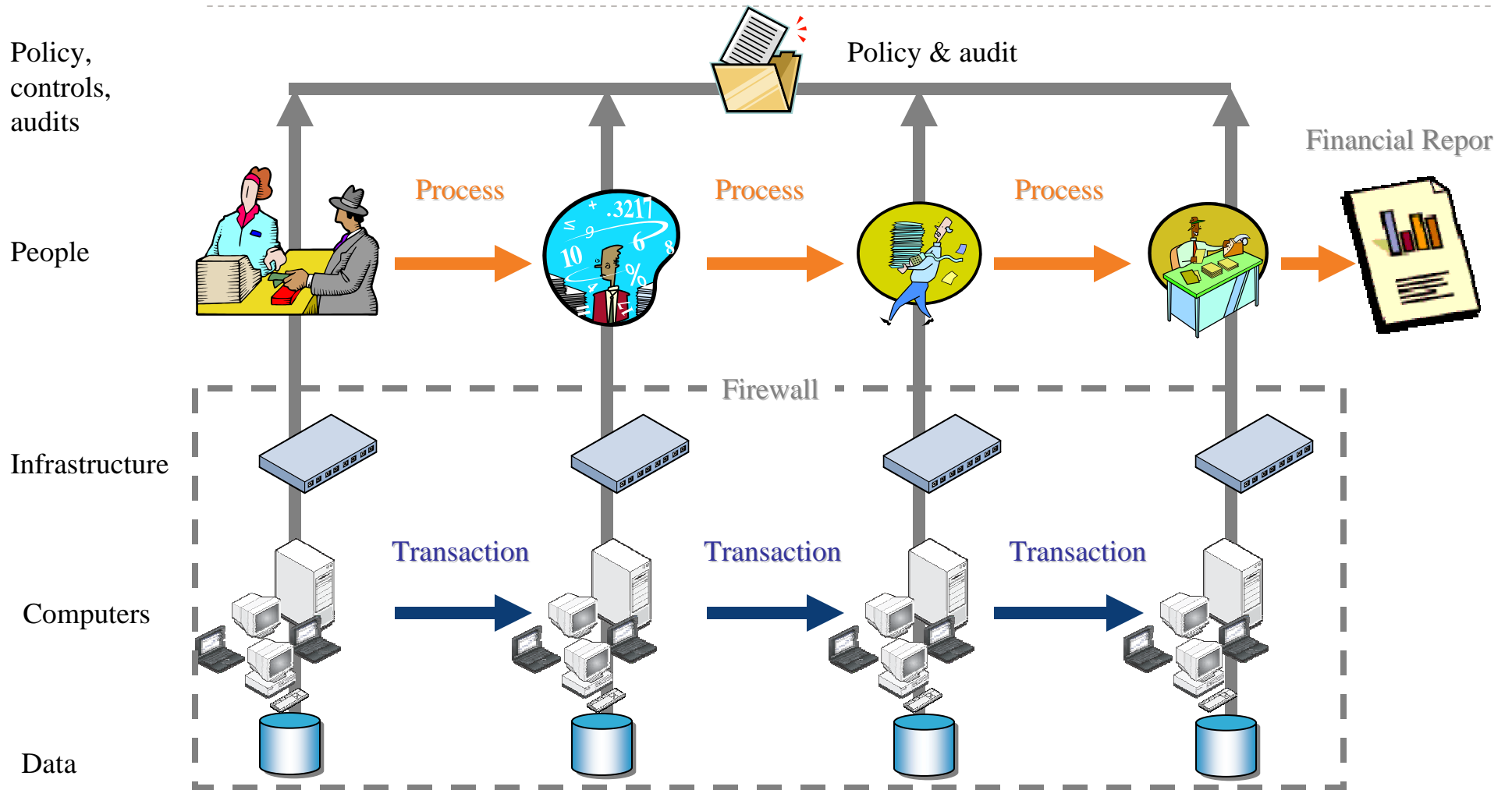


Regulatory Compliance

We must create and sustain IT policy by automating and monitoring IT controls!

- ▶ *Understand* – The latest vulnerabilities, threats, risks, exposures and mitigating factors that could impact the compliance to IT policy
- ▶ *Control* – A proactive management system that monitors and demonstrates a continuous state of compliance with IT policy
- ▶ *Act* – Establish, monitor and test existing security and availability controls mapping the current state to the policy state, remediate control gaps as required

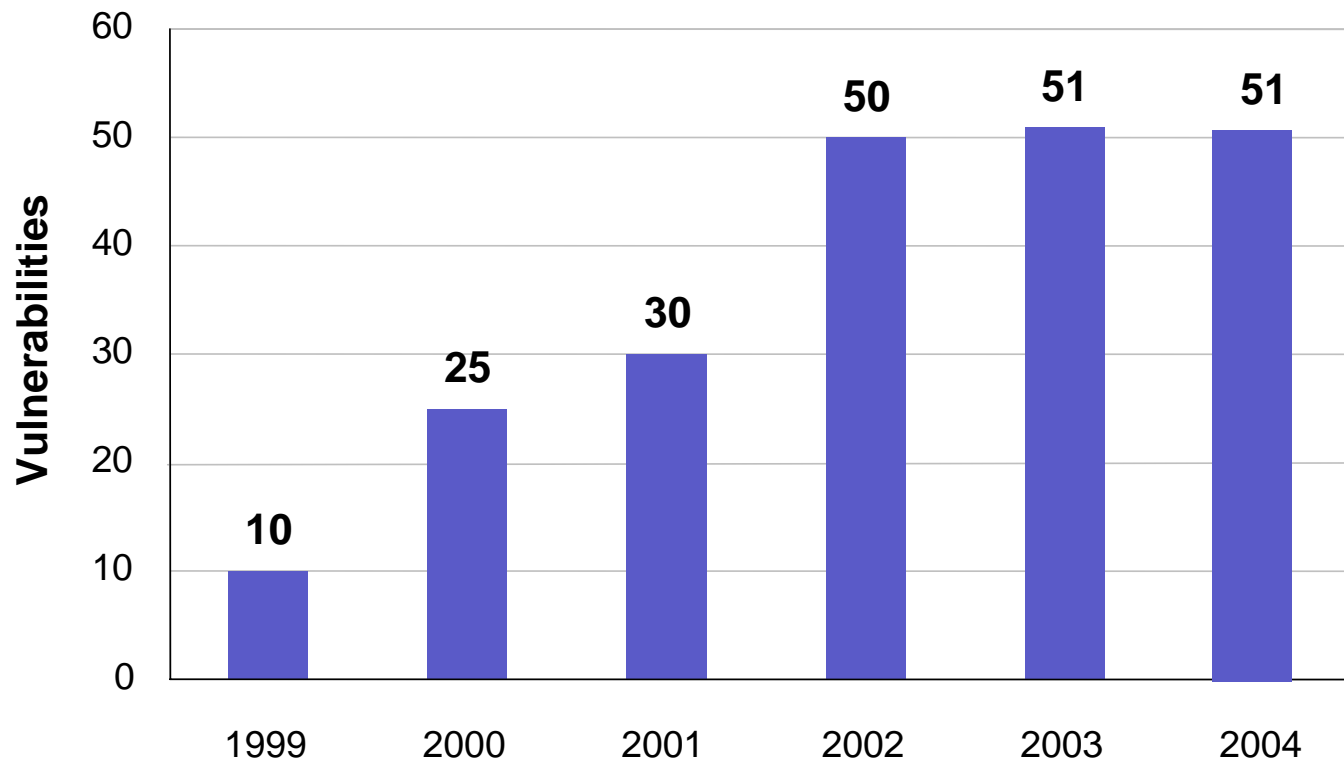
Compliance will drive the merger of Policy, People, Process & Technology



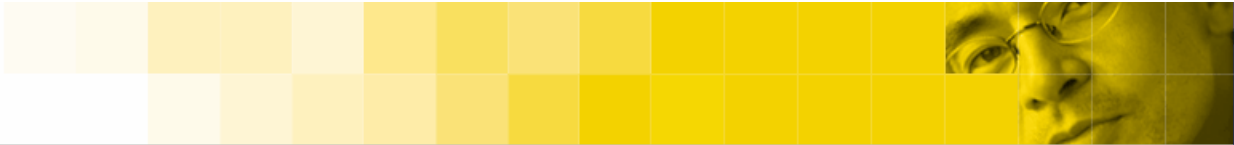


Un-patched software puts Data at risk!

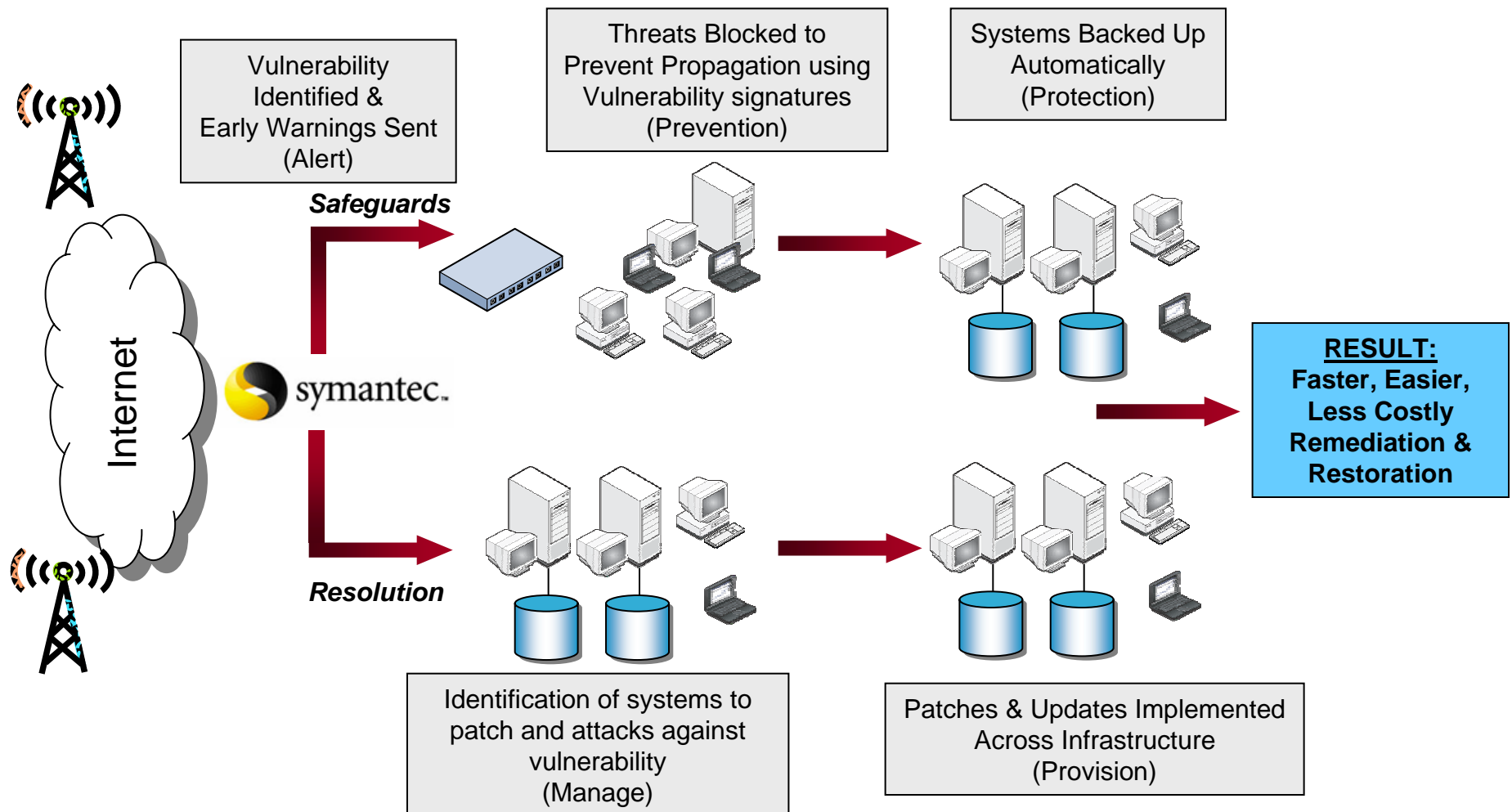
- ▶ Average time for a vulnerability exploit to appear = 6 days
- ▶ Average number of new vulnerabilities discovered every week



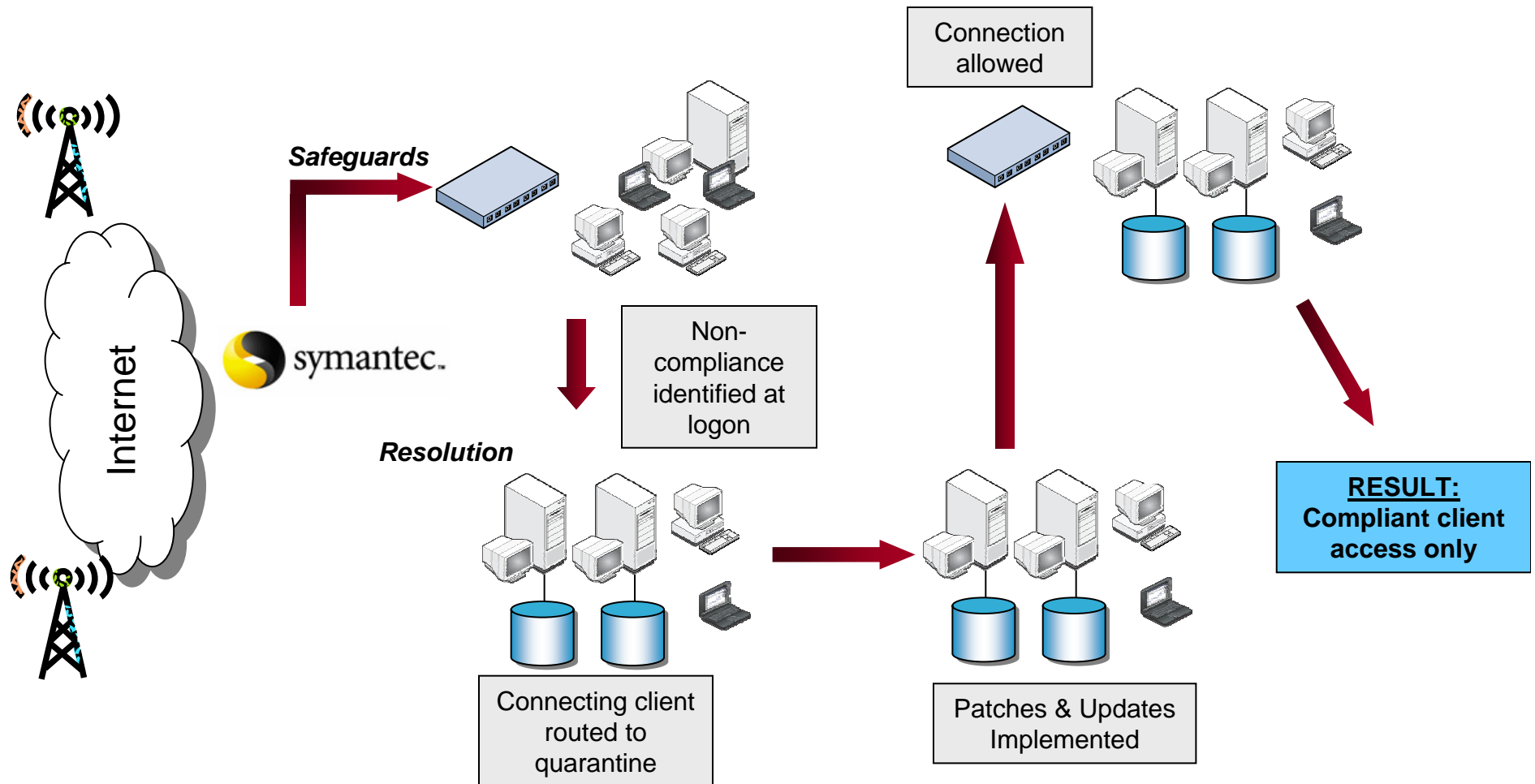
Source: March 2005 Internet Security Threat Report, Symantec Corporation

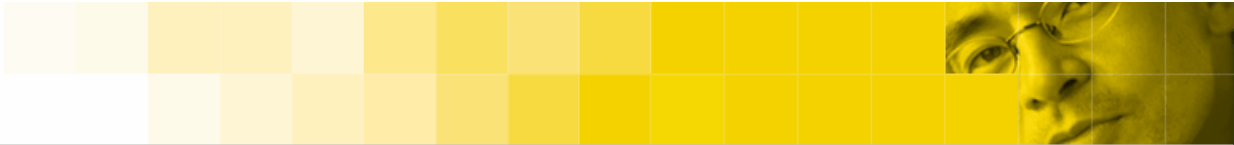


Insuring compliance through “protected remediation”

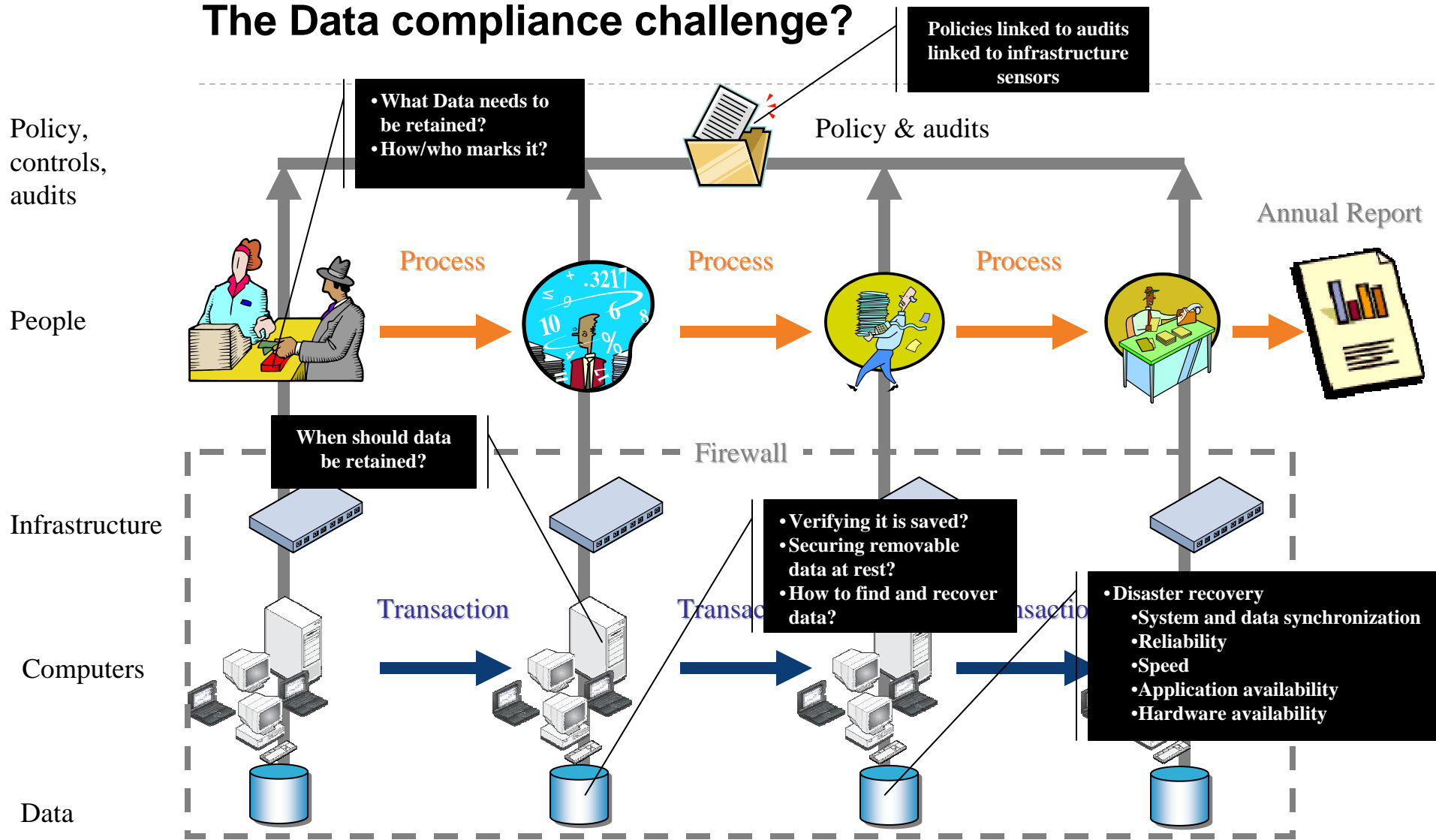


Endpoints put data at risk! Insuring compliance at the “endpoint”

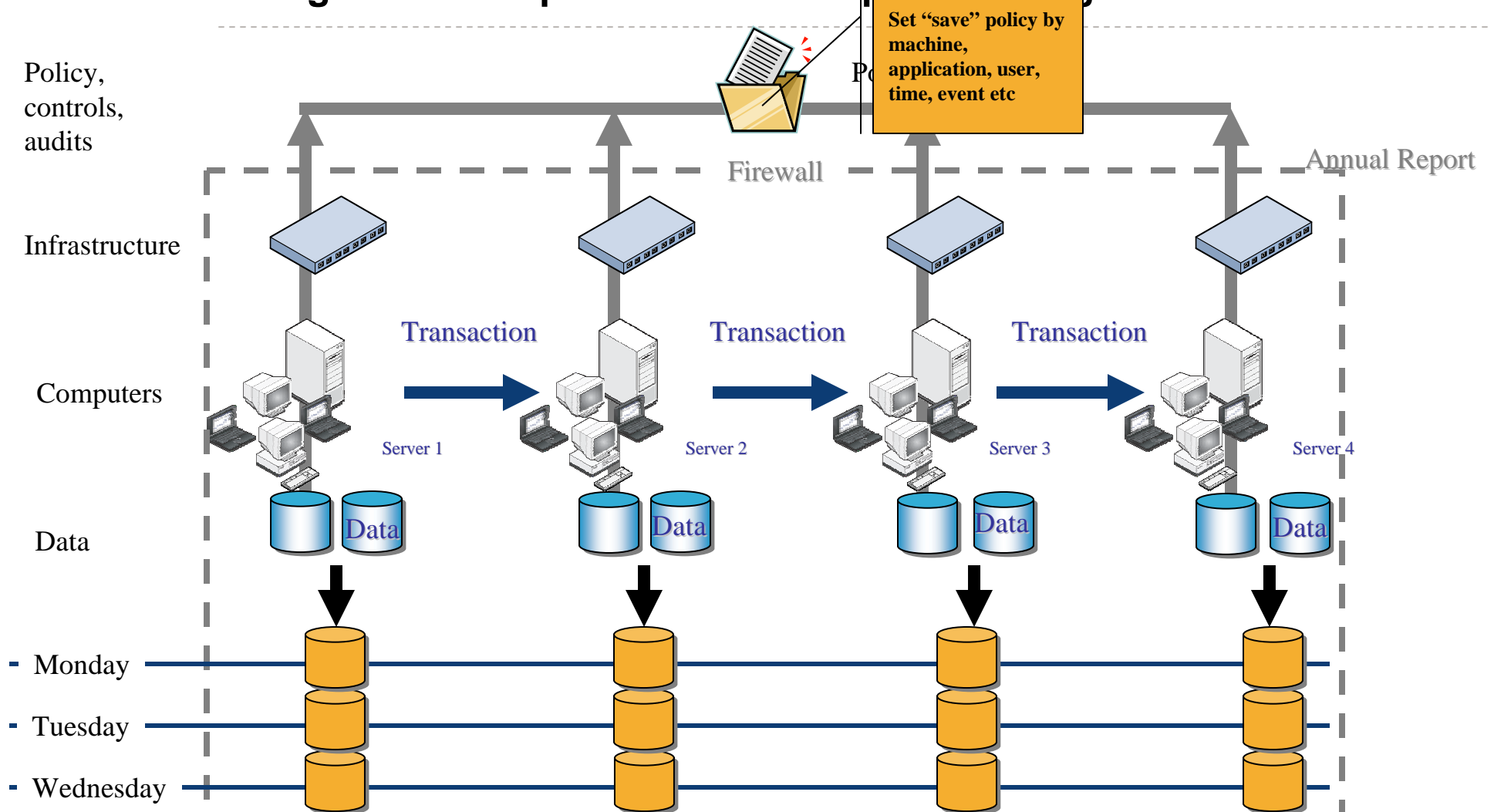




The Data compliance challenge?



An approach to data retention Using Saved Snapshots ie: keep everything?



Example Policy: save scenarios based on events and conditions

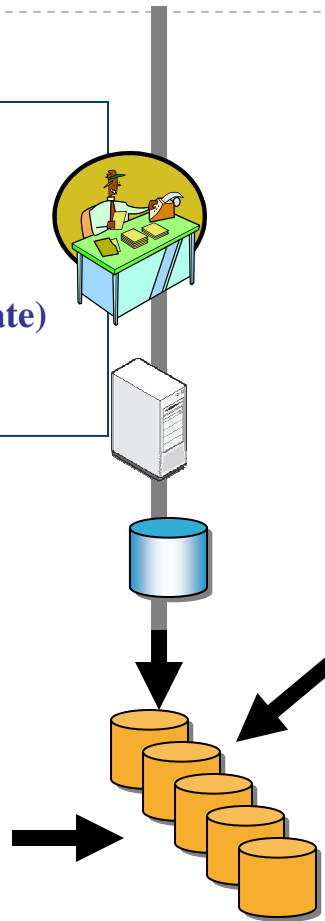
Snapshot_policy:

```

John_Doe = logged on;
File = (annual_report.xls = changed);
File = (annual_report.xls = closed);
Save_Volume (name = Annual Report Activity (date)
.v21, Volume = Data, schedule = ++backup_que);
End Snapshot Policy:
    
```

Volume Save Actions can be based on one or all of:

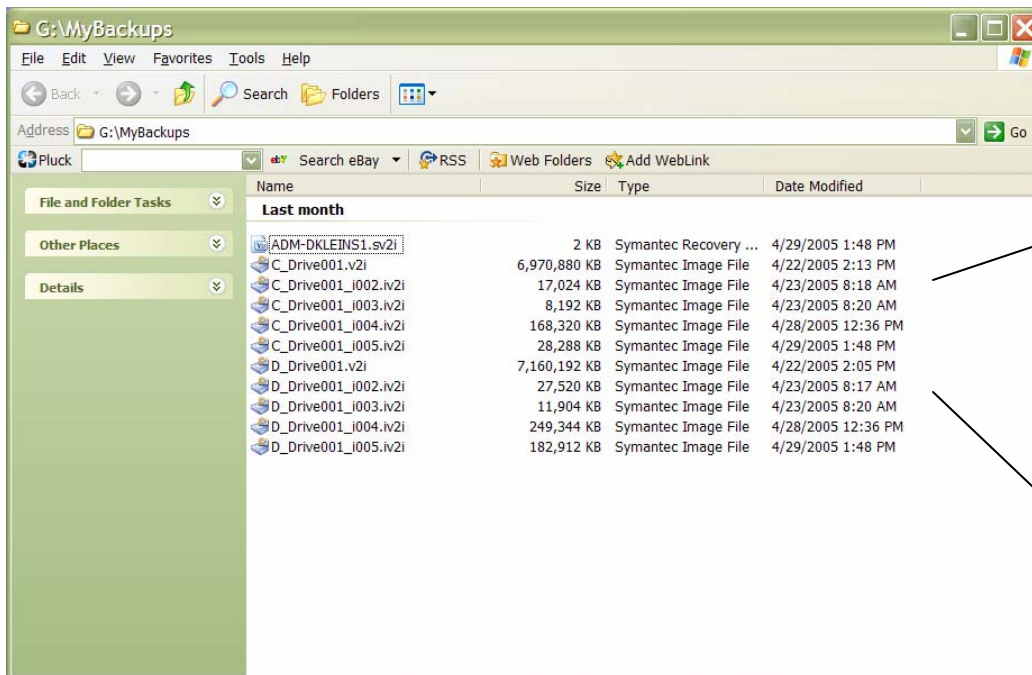
- User logon
- Application activity
- File system activity
- Installation actions
- Threat levels
- Specific file mark
- etc



Regulatory enablement features:

- Verified as saved and clean
- Create audit trail of “saves”
- Return the machine to specific “point in time”
- Audit the contents of offline snapshot
- Convert to virtual environment and restore

Cost of saving everything once a day for a year?

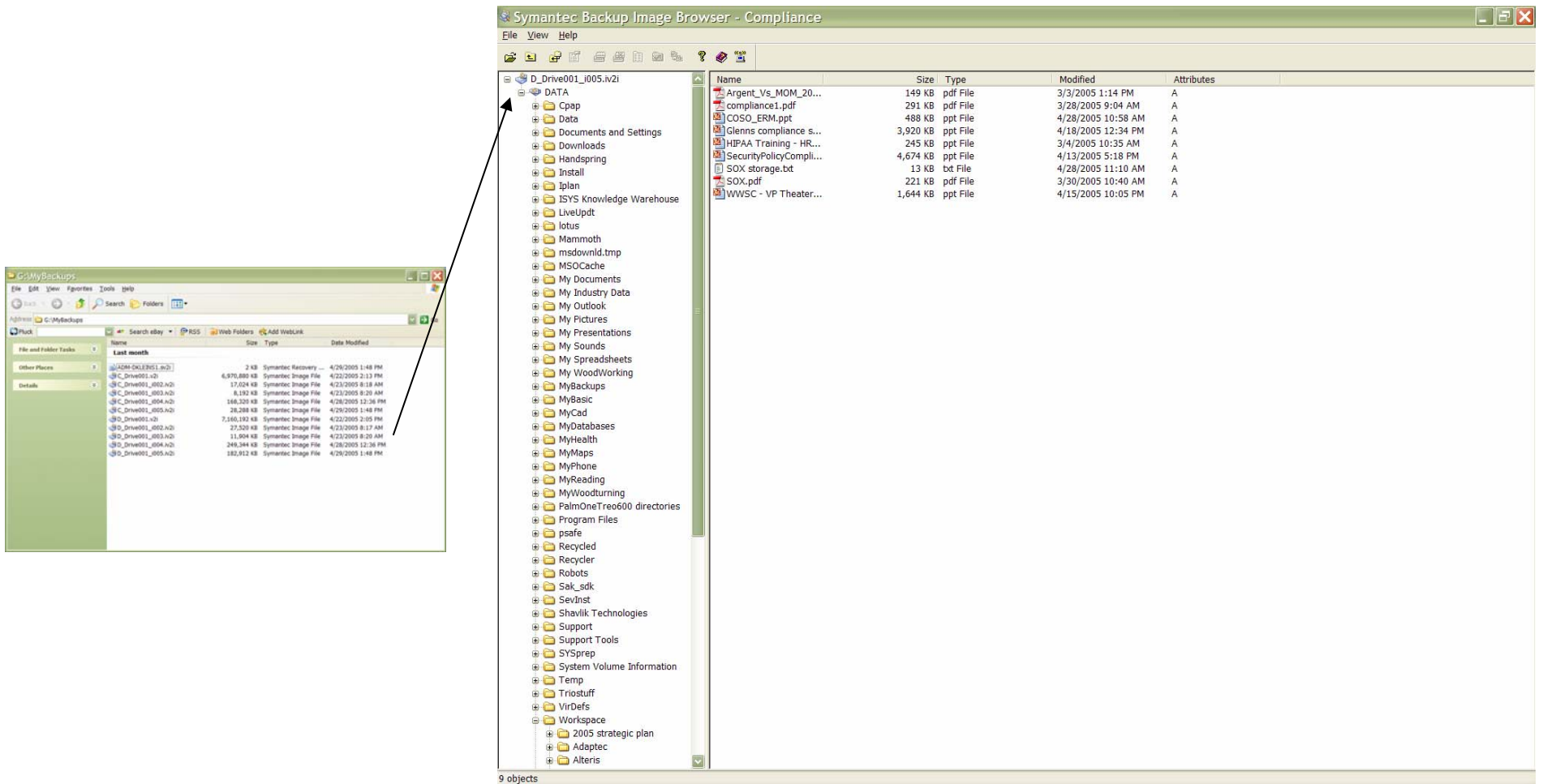


Snapshots saved on USB drive

C DRIVE		
Date	Size (KB)	Type
22-Apr	6,970,880	Base
23-Apr	17,024	Incremental
23-Apr	8,192	Incremental
28-Apr	168,320	Incremental
29-Apr	28,288	Incremental
Days	6	
Base	6,970,880	
Total Incrementals	221,824	
Delta/day	36,971	
365 days of storage	20,465,173	
Yearly Cost at \$2.68GB	\$ 54.85	

D DRIVE		
Date	Size (KB)	Type
22-Apr	7,160,192	Base
23-Apr	27,520	Incremental
23-Apr	11,904	Incremental
28-Apr	249,344	Incremental
29-Apr	182,912	Incremental
Days	6	
Base	7,160,192	
Total Incrementals	471,680	
Delta/day	78,613	
365 days of storage	35,854,059	
Yearly Cost at \$2.68GB	\$ 96.09	
Yearly Cost for entire machine	\$ 150.94	

Browsing a disconnected Saved Snapshot

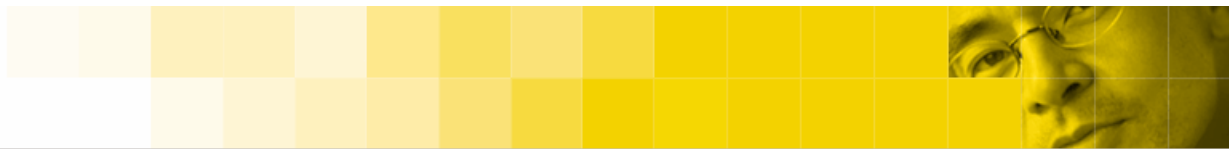


The main window, titled "Symantec Backup Image Browser - Compliance", displays a file explorer view of a disconnected saved snapshot. The left pane shows a tree view of folders, with "D:_Drive001_i005.iv2" selected. The right pane shows a list of files with columns for Name, Size, Type, Modified, and Attributes.

Name	Size	Type	Modified	Attributes
Argent_Vs_MOM_20...	149 KB	pdf File	3/3/2005 1:14 PM	A
compliance1.pdf	291 KB	pdf File	3/28/2005 9:04 AM	A
COSO_ERM.ppt	488 KB	ppt File	4/28/2005 10:58 AM	A
glenns compliance s...	3,920 KB	ppt File	4/18/2005 12:34 PM	A
HIPAA Training - HR...	245 KB	ppt File	3/4/2005 10:35 AM	A
SecurityPolicyCompli...	4,674 KB	ppt File	4/13/2005 5:18 PM	A
SOX storage.bt	13 KB	txt File	4/28/2005 11:10 AM	A
SOX.pdf	221 KB	pdf File	3/30/2005 10:40 AM	A
WWSC - VP Theater...	1,644 KB	ppt File	4/15/2005 10:05 PM	A

The inset window, titled "G:\MyBackups", shows a list of backup files with columns for Name, Size, Type, and Date Modified. An arrow points from the "G:\MyBackups" window to the "D:_Drive001_i005.iv2" folder in the main window.

Name	Size	Type	Date Modified
ADMIN-0413101.iv2	2 KB	Symantec Recovery ...	4/29/2005 1:48 PM
C:_Drive001.iv2	6,976,880 KB	Symantec Image File	4/22/2005 2:13 PM
C:_Drive001_002.iv2	17,024 KB	Symantec Image File	4/23/2005 8:18 AM
C:_Drive001_003.iv2	6,192 KB	Symantec Image File	4/23/2005 8:20 AM
C:_Drive001_004.iv2	166,320 KB	Symantec Image File	4/28/2005 12:36 PM
C:_Drive001_005.iv2	28,208 KB	Symantec Image File	4/29/2005 1:48 PM
C:_Drive001.iv2	2,160,192 KB	Symantec Image File	4/22/2005 2:05 PM
C:_Drive001_002.iv2	27,520 KB	Symantec Image File	4/23/2005 8:17 AM
C:_Drive001_003.iv2	11,904 KB	Symantec Image File	4/23/2005 8:20 AM
C:_Drive001_004.iv2	246,344 KB	Symantec Image File	4/28/2005 12:36 PM
C:_Drive001_005.iv2	182,912 KB	Symantec Image File	4/29/2005 1:48 PM



Saved Snapshots are Compliant!

- ▶ Reliable recovery disk based
- ▶ Tape compatible it's a file
- ▶ Easily archive-able ... it's a file
- ▶ Easy to replicate ... it's a file
- ▶ File extraction through browsing
- ▶ Includes strong DR capability
 - Data & application recovery
 - Recovery to new hardware (coming soon)
- ▶ Protected data at rest: encrypted and password protected
- ▶ Event driven
- ▶ Platform, infrastructure and storage independent
- ▶ Criteria driven (future)



Summary

- ▶ **Regulations are not prescriptive but infer:**
 - A more holistic and automated IT architecture
 - An “infrastructure” with auditing capabilities
 - Insurance that specific data is saved, archived and recoverable
- ▶ **Convergence is needed:**
 - Security
 - Systems
 - Storage
- ▶ **Data marking may evolve in two ways**
 - Data Marking
 - Saved & managed snapshots
 - Better indexing for retrieval
- ▶ **Technology Improvements**
 - Better definition and integration of infrastructure sensors
 - Built in infrastructure audit reporting
 - Better links between applications to infrastructure
 - Solutions to the data retention challenge



Questions



Geographic Applicability

US

- ▶ GLBA
- ▶ HIPAA
- ▶ FISMA
- ▶ NERC
- ▶ Visa CISP
- ▶ COSO
- ▶ COBIT
- ▶ California Senate Bill

European Union

- ▶ EU Data Protection Act
- ▶ EU Privacy Act

Australia

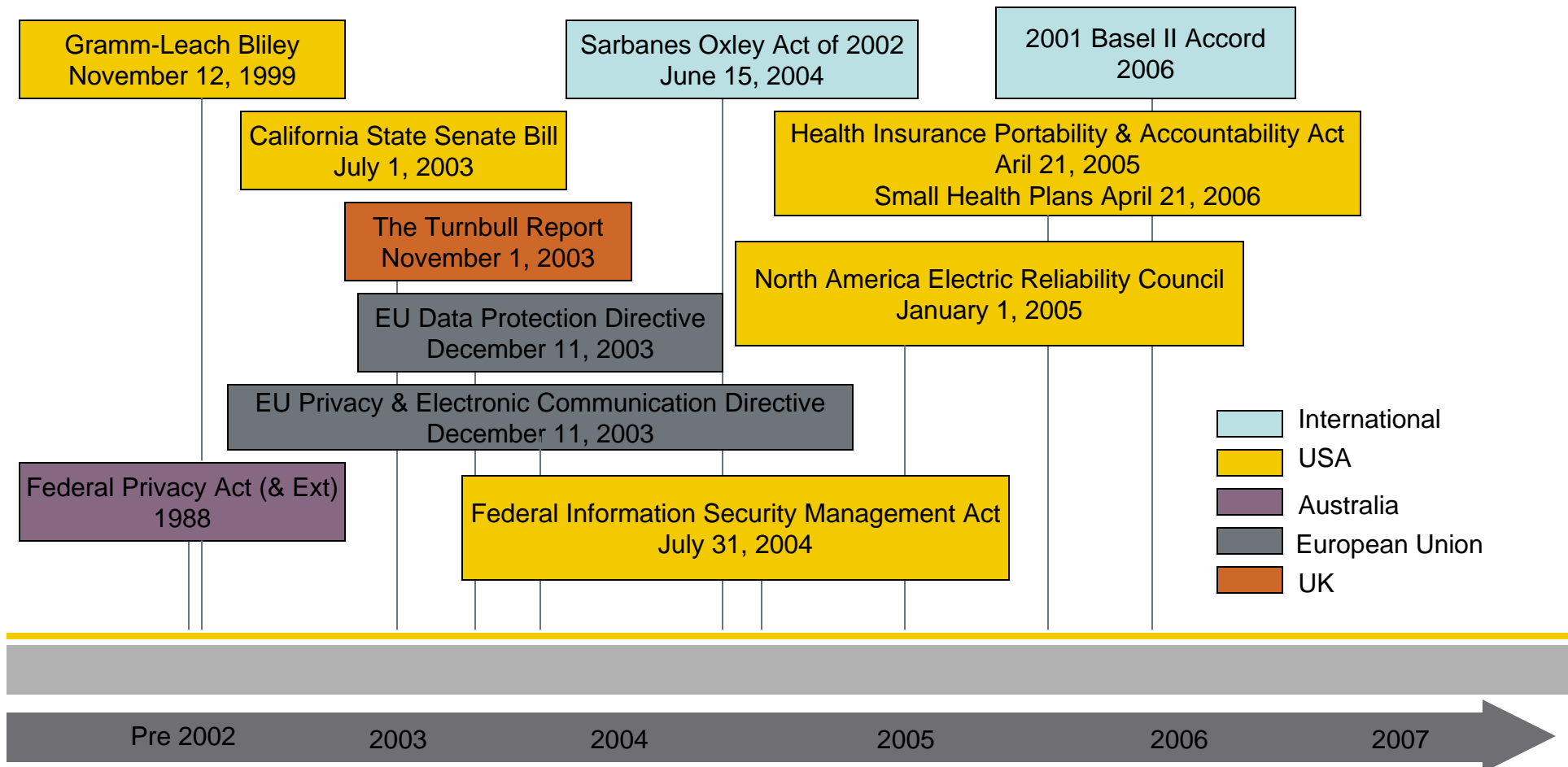
- ▶ Australian Federal Privacy Act
- ▶ PSM
- ▶ ACSI 33

Global Standards

- ▶ Basel II
- ▶ Information Security Forum

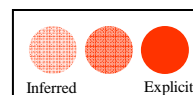


Timelines for Implementing Regulations



Summary of requirements

Category	IT controls	HIPPA
Planning & reporting	IT Policy creation	●
	Control sensing, auditing and reporting	●
	Asset discovery & inventory	●
Security	Intrusion Detection & Protection	●
	Identity control	●
	Vulnerability assessment	●
Change Management	Provisioning	●
	Patch Remediation	●
Information Management	Disaster recovery	●
	Data Archive & Retention & Disposal	●



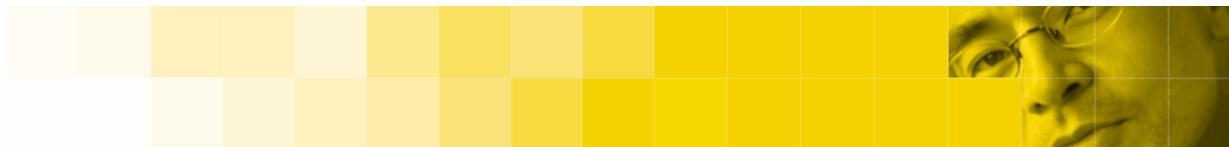
Security: Ensure the confidentiality, integrity and availability of electronic health information. Protect against threats or hazards to that information and against misuse or disclosure

Administration: Implement policies and procedures to prevent, detect, contain, and correct security violations and security incident response. Implement procedures for disaster recovery .

Physical Safeguards: Implement policies and procedures for handling hardware containing protected health information

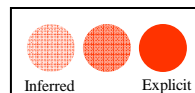
Technical Safeguards: Implement access control procedures, audit, integrity and transmission controls : that prevent unauthorized access

Policy, procedures and documentation: support of policies that meet the standards and it implementation



Summary of requirements

Category	IT controls	FISMA
Planning and reporting	IT Policy creation	●
	Control sensing, auditing and reporting	●
	Asset discovery & inventory	●
Security	Intrusion Detection & Protection	●
	Identity control	●
	Vulnerability assessment	●
Change Management	Provisioning	●
	Patch Remediation	●
Information Management	Disaster recovery	●
	Data Archive & Retention & Disposal	●



Information Security

Program:

Agency risk assessment

Security policies and procedures

Subordinate plans

Training

Annual testing and evaluation

Corrective action

Security incident reporting

Continuity of operations