



**NetApp**

Go further, faster

## New Regulations & Compliance Issues:

### How to Stay One Step Ahead

Blair Semple, CISSP-ISSEP  
Storage Security Evangelist  
NetApp



2008 IMI SECURITY SYMPOSIUM & EXPO

---

---

---

---

---

---

---

---



**NetApp**

## Agenda

- What's New in the Regulatory Landscape?
- Some Existing Regulations
- What Analysts Have to Say
- Best Practice Recommendations

© 2008 NetApp. All rights reserved.

---

---

---

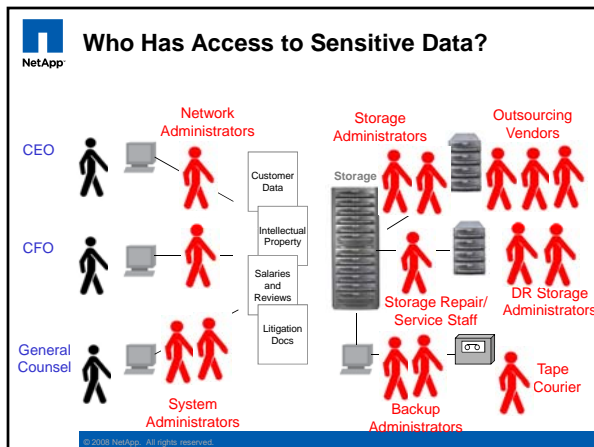
---

---

---

---

---



---

---

---

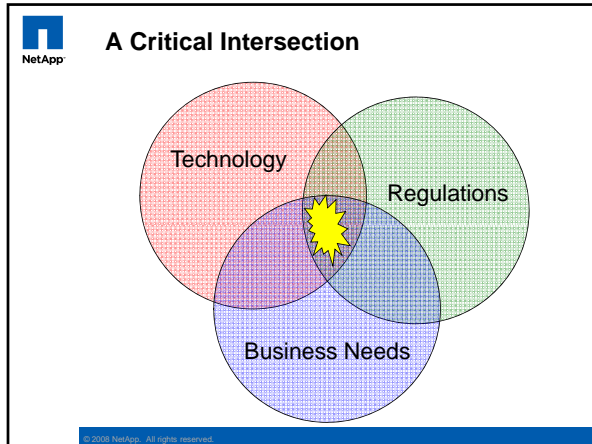
---

---

---

---

---



---

---

---

---

---

---

---

---

- 
- Some Recent Headlines**
- New Hampshire Considers Stricter Health Record Rules
  - We Are the Security Problem: Deloitte Report
  - Massachusetts Adopts Data Breach Law
  - UK – Privacy Commissioner Wants New Criminal Offence
  - Where Do Data Leaks Start? Check the IT Dept
  - Breach Disclosure Laws Shed Light on Inventory of Lost Records in 2007
  - New Study Recommends Reforms for Security Breach Notification Laws
- © 2008 NetApp. All rights reserved.

---

---

---

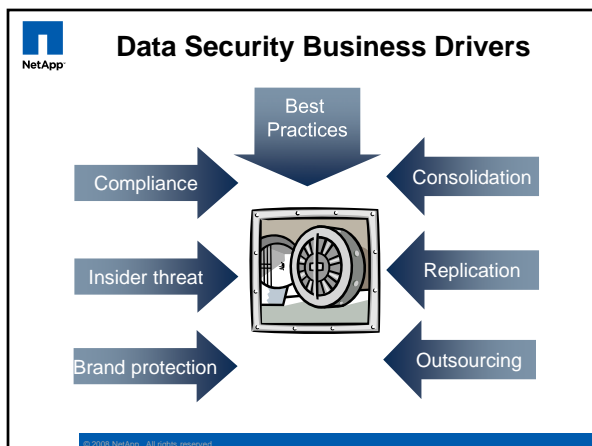
---

---

---

---

---



---

---

---

---

---

---

---

---



Go further, faster

# Privacy Regulations




---

---

---


---

---


---

---

---



## GLBA and SOX



**Gramm-Leach-Bliley Act (July 2001)**

- "... each financial institution has an ... obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." [15 U.S.C. § 6801(a)]
- Institutions must develop safeguards to protect against any anticipated threats or hazards and unauthorized access

**Sarbanes-Oxley Sec. 404**

- Enterprises must insure the integrity of their financial systems
- Examples:
  - Prevent rogue insiders from viewing or modifying financial records
  - Protect integrity and confidentiality of M&A documents, earnings releases, legal docs

© 2005 NetApp. All rights reserved.

---

---

---


---

---


---

---

---



## HIPAA - Healthcare & Pharmaceutical



**Sec. 164.306 Security Standards**

- "Covered entities must:
  - ensure the confidentiality, integrity and availability of all electronic protected health information they create, receive, maintain, or transmit
  - protect against any reasonably anticipated threats to the security or integrity of such information
  - protect against any reasonably anticipated uses or disclosures of such information that are not permitted
  - ensure compliance with these rules by their workforce (officers and employees)"

© 2005 NetApp. All rights reserved.

---

---

---

---

---

---

---

---



Go further, faster

## Disclosure Regulations




---

---

---


---

---

---

---

---



### CA SB1386 (2003) / AB 1950 (2005)

**1386** - "Any agency that owns or licenses computerized data that includes personal information shall disclose any breach ... in the security of the data to any resident of California whose **unencrypted personal information** was, or is reasonably believed to have been, acquired by an unauthorized person."

**1950** - Requires organizations to also maintain "reasonable security procedures and practices", extended the responsibility to organizations outside of the State if information on Californian residents is collected.

2003	Texas	Maine	Colorado
California	North Carolina	Ohio	Arizona
2005	New York	Montana	2007
Arkansas	2006	Rhode Island	Hawaii
Georgia	Connecticut	Wisconsin	Kansas
North Dakota	Illinois	Oklahoma	New Hampshire
Delaware	Louisiana	Pennsylvania	Utah
Florida	Minnesota	Idaho	Vermont
Tennessee	Nevada	Indiana	2008
Washington	New Jersey	Nebraska	Massachusetts

© 2008 NetApp. All rights reserved.

---

---

---


---

---

---

---

---



### International Momentum for Disclosure Law

- Advocacy Group Urges Ottawa to Draft Data Breach Notification Law
  - "Responding to an [Industry Canada request](#) for public consultation on data security laws, the University of Ottawa's Canadian Internet Policy and Public Interest Clinic (CIPPIC) this week recommended that mandatory reporting of data breaches to a public registry is the most effective way to persuade corporations to shore up their potential security risks"

© 2008 NetApp. All rights reserved.

---

---

---

---

---

---

---

---



**Industry Regulations** Go further, faster

**Payment Card Industry Data Security Standard - (PCI DSS)**




---

---

---


---

---

---

---

---



**Why Have Industry Regulation**

- Credit card fraud (25%) was the most common form of reported identity theft in 2006.  
*<http://www.consumer.gov>*
- More than \$48 billion lost by financial institutions & businesses in 2003 due to identity theft.  
*<http://www.ftc.gov>*
- "\$5 billion lost by individuals, it can be said that credit card E-commerce fraud is also on the rise, reaching \$3 billion in 2006 with an increment of 7% over 2005."  
*PCI DSS Made Easy Whitepaper – GFI Software*

© 2006 NetApp. All rights reserved.

---

---

---


---


---

---

---

---



**Some PCI Details** 

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Protect Cardholder Data

- **Requirement 3:** Protect stored cardholder data
- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks

Implement Strong Access Control Measures

- **Requirement 7:** Restrict access to cardholder data by business need-to-know
- **Requirement 8:** Assign a unique ID to each person with computer access
- **Requirement 9:** Restrict physical access to cardholder data

© 2006 NetApp. All rights reserved.

---

---

---


---

---

---

---

---

 **Penalties for non-Compliance**

- Compliance is a simple PASS/FAIL decision. A single failure results in overall failure
- Penalties for noncompliance range from fines of up to \$500,000 to increased auditing requirements or even losing the ability to process credit card transactions.
- Level 1 businesses -- those that process more than six million credit card transactions per year -- are subject to an annual on-site audit and quarterly network scans performed by an approved vendor.
- Level 2 or 3 companies that process 20,000 to 6 million credit card transactions a year must fill out an annual self-assessment questionnaire and must also have an approved vendor conduct quarterly network scans.

© 2008 NetApp. All rights reserved.

---

---

---

---

---

---

---

---

---

---

---

---

 **Go further, faster**

**Some Analyst Perspectives on Compliance**




---

---

---

---

---

---

---


---

---

---


---

---

 **Potential Cost of Privacy Breach**

- Gartner study quantifying costs of privacy breaches
  - Cost estimate for a 100,000 record breach:
    - \$90 per customer account
    - Notification costs, credit reporting, legal...
    - Estimate does not include fines or brand damage
  - Cost of encryption to prevent:
    - \$6 per customer account (annual maintenance \$1)

*"Most data theft attacks would have failed if the stored information was encrypted, and the encryption keys were sufficiently protected"*



© 2008 NetApp. All rights reserved.

---

---

---

---

---

---

---


---

---

---

---

---



### Forrester Research – Up to \$305 per Record

Category	Description	A:	B:	C:
Discovery, notification, and response	Outside legal counsel, mail notification, calls, call center, and discounted product offers	\$50	\$50	\$50
Lost employee productivity	Employees diverted from other tasks	\$20	\$25	\$30
Opportunity cost	Customer churn and difficulty in getting new customers	\$20	\$50	\$100
Regulatory fines	FTC, PCI, SOX	\$0	\$25	\$60
Restitution	Civil courts may ask to put this money aside in case breaches are discovered.	\$0	\$0	\$30

Company A: Low-profile breach in a non-regulated industry  
 Company B: Low-profile breach in a regulated industry  
 Company C: High-profile breach in a highly regulated industry

© 2005 NetApp. All rights reserved. Source: Forrester Research, Inc.

---

---

---

---

---

---

---


---

---

---

---

---



### Forrester Research – Continued

Category	Description	A:	B:	C:
Additional security and audit requirements	The security and audit requirements levied as a result of a breach	\$0	\$5	\$10
Other liabilities	Credit card replacement costs. Civil penalties if specific fraud can be traced to the breach.	\$0	\$0	\$25
<b>Total cost per record</b>		<b>\$90</b>	<b>\$155</b>	<b>\$305</b>

Company A: Low-profile breach in a non-regulated industry  
 Company B: Low-profile breach in a regulated industry  
 Company C: High-profile breach in a highly regulated industry

© 2005 NetApp. All rights reserved. Source: Forrester Research, Inc.

---

---

---

---

---

---

---


---

---


---

---


---



### An Ounce of Prevention



- **Forrester Research:**
  - **\$90-305 per record**
  - Legal fees, call center costs, lost employee productivity, regulatory fines, loss of investor confidence and customer losses
- **Ponemon Research:**
  - **\$182 per compromised record**
- **Gartner:**
  - Cost estimate for a 100,000 record breach: **\$90 per customer account**
  - Cost of encryption to prevent: **\$6 per customer account**



© 2005 NetApp. All rights reserved.

---

---

---

---

---

---

---

---

---

---

---

---



Go further, faster

## Best Practice Considerations for Compliance




---

---

---


---

---

---

---

---



### SNIA– SSIF Best Current Practices

#### 2.1.5 GEN 05 – Address Data Security Compliance

- **Accountability:** Unique IDs, restrict privileges, logging
- **Traceability:** Detailed logs, unique ID, treat logs as evidence
- **Risk Management:** Classify data, assess risks/threats, analyze probability/impact, risk treatment (avoid, transfer, reduce accept), test & review
- **Detect, Monitor and Evaluate**
- **Information Retention and Sanitization:** Retention policy, Destruction policy
- **Privacy:** Access Controls, Confidentiality (encryption)

*SNIA Storage Security – Best Current Practices (BCPs) Version 2.0*

© 2005 NetApp. All rights reserved.

---

---

---


---

---

---

---

---




### Steps To Managing Information Risk

**Evaluate Threats**

- ▶ External
- ▶ Internal

**Assess Exposure**

- ▶ Potential damage from data security/privacy breach



**Enforce using Technology**

- ▶ Encryption based storage security
- ▶ Strong Access Controls
- ▶ Audit Logging

**Review People/ Processes**

- ▶ Classification, Role Separation, Authentication, Quorum requirements, Need to know, Auditing

© 2005 NetApp. All rights reserved.

---

---

---

---

---

---

---

---



**Encryption as a Possible Step to Compliance**




---

---

---


---

---


---

---


---




**Host / Application**



**Network**



**Storage**



Arrows indicate data flow between Host/Application, Network, and Storage.

<p><b>Pros:</b></p> <ul style="list-style-type: none"> <li>•Granular options</li> <li>•Encrypted at host</li> <li>•Lower cost (SW)</li> </ul> <p><b>Cons:</b></p> <ul style="list-style-type: none"> <li>•CPU intensive, slow</li> <li>•Weak Key Mgt</li> <li>•Keys exposed in OS</li> <li>•Complex to implement/manage</li> <li>•Poor coverage for diverse environments</li> </ul>	<p><b>Pros:</b></p> <ul style="list-style-type: none"> <li>•Transparent to host, storage, and apps</li> <li>•Wire-speed encryption and compression</li> <li>•Strong logging and Access Control</li> <li>•HW-based - provides strong security</li> </ul> <p><b>Cons:</b></p> <ul style="list-style-type: none"> <li>•May require additional device</li> </ul>	<p><b>Pros:</b></p> <ul style="list-style-type: none"> <li>•Transparent to host</li> <li>•Bundled with HW</li> </ul> <p><b>Cons:</b></p> <ul style="list-style-type: none"> <li>•Immature key mgmt</li> <li>•No support for diverse environments</li> <li>•Lock-in to one vendor</li> <li>•“Forklift upgrade”</li> <li>•Not backwards compatible in many cases</li> </ul>
---	--	---

---

---

---


---

---

---

---

---



- ~~Performance degradation~~
- ~~Key management complexity & security~~
- ~~High availability issues~~
- ~~Application changes and downtime~~
- ~~Database changes required~~
- ~~Increased tape media usage~~
- ~~Changes to desktops, servers, workflow~~

A proper solution must address all of these concerns.

---

---

---

---

---

---

---

---