New Regulations and Compliance Issues

How to Stay One Step Ahead
Agenda

- What’s New in the Regulatory Landscape
- Some Existing Regulations
- What Analysts Have to Say
- Best-Practice Recommendations
A Critical Intersection

Technology

Regulations

Business Needs
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
Data Security Business Drivers

Best Practices

Compliance

Insider threat

Brand protection

Consolidation

Replication

Outsourcing

© 2011 NetApp, Inc. All rights reserved.
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 documents
“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)”
Disclosure Regulations

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,” extending the responsibility to organizations outside of the State if information on Californian residents is collected.

<table>
<thead>
<tr>
<th>2003</th>
<th>Texas</th>
<th>Maine</th>
<th>Colorado</th>
</tr>
</thead>
<tbody>
<tr>
<td>California</td>
<td>North Carolina</td>
<td>Ohio</td>
<td>Arizona</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>Rhode Island</td>
<td>Hawaii</td>
<td></td>
</tr>
<tr>
<td>Arkansas</td>
<td>Connecticut</td>
<td>Wisconsin</td>
<td>Kansas</td>
</tr>
<tr>
<td>Georgia</td>
<td>Illinois</td>
<td>Oklahoma</td>
<td>New Hampshire</td>
</tr>
<tr>
<td>North Dakota</td>
<td>Louisiana</td>
<td>Pennsylvania</td>
<td>Utah</td>
</tr>
<tr>
<td>Delaware</td>
<td>Minnesota</td>
<td>Idaho</td>
<td>Vermont</td>
</tr>
<tr>
<td>Florida</td>
<td>Nevada</td>
<td>Indiana</td>
<td></td>
</tr>
<tr>
<td>Tennessee</td>
<td>New Jersey</td>
<td>Nebraska</td>
<td>Massachusetts</td>
</tr>
<tr>
<td>Washington</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 (CIPPIIC) 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”
Industry Regulations

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.
  

- More than $48 billion was lost by financial institutions and businesses in 2003 due to identity theft.
  
  [http://www.ftc.gov](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” White Paper—GFI Software
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
Penalties for Noncompliance

- 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.
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.”
Gartner: Pitfalls of Column-/App-Level Encryption

- Database encryption is difficult, especially on existing systems
- App-level encryption may not address all requirements of PCI
  - Significant performance impact when encrypting indexed fields
  - The cost of application changes (if even possible) to handle encrypted results or error messages
  - Failure to meet “separation of duties” requirements
  - Range searches and reporting require decryption of all records to execute, dramatically damaging performance

“Field encryption in databases may be a two- to three-year project, but combining database activity monitoring with media encryption offers many of the security benefits, without the pitfalls.” - Rich Mogull, Gartner, July 2006
## Forrester Research—Up to $305 per Record

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>A:</th>
<th>B:</th>
<th>C:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional security and</td>
<td>The security and audit requirements levied as a result of a breach</td>
<td>$0</td>
<td>$5</td>
<td>$10</td>
</tr>
<tr>
<td>audit requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other liabilities</td>
<td>Credit-card replacement costs; civil penalties if specific fraud can be</td>
<td>$0</td>
<td>$0</td>
<td>$25</td>
</tr>
<tr>
<td></td>
<td>traced to the breach</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total cost per record</td>
<td></td>
<td>$90</td>
<td>$155</td>
<td>$305</td>
</tr>
</tbody>
</table>

Company A: Low-profile breach in a nonregulated industry

Company B: Low-profile breach in a regulated industry

Company C: High-profile breach in a highly regulated industry

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
Best-Practice Considerations for Compliance
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 and review
- Detect, Monitor, and Evaluate
- Information Retention and Sanitization: Retention policy, destruction policy
- Privacy: Access controls, confidentiality (encryption)
Data-Security Framework

Application Security
- dB App Users
- dB Application Server
- dBA
- App Developer
- Discovery / Search
- Index Database
- Data Set
- Secure Storage
- Backup Security

File/NAS Security
- AD Admin
- Directory Server
- Clients
- Audit

Security Policy Management
- Security Officer
- Key/Security Policy Manager

© 2011 NetApp, Inc. All rights reserved.
Encryption—the Foundation for Compliance, but…

- Important considerations
  - Auditability
  - Interoperability
  - Multisite access and recovery
  - Protection of encryption keys
  - Management of copies
  - Performance
  - Secure disposal

*Key management and related policy management are the key to encryption*
Key Management Goals

- Backup/Restore Key Material
- Archival and Retention of Key Material
- Distribution of Key Material
- Expiration, Deletion, Destruction of Key Material
- Audit of Key’s Lifecycle
- Reporting Events and Alerts

Source: SNIA Tutorial – “An Introduction to Key Management for Secure Storage”
Steps to Managing Information Risk

**Evaluate Threats**
- External

**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
Summary

- Regulatory environment continues to expand
- Compliance strategies need to include multiple facets: technology, process, training, auditing, etc.
- Encryption is a foundation for achieving compliance
- Key management is critical to effective use of encryption technologies
- Index and catalog technologies combined with encryption lead to compliance
Thank you