

PCI, SOX, HIPAA, and et al.: How to integrate these mandates with present & future IT/IS initiatives. A philosophy of:

**Continuity of Compliance :
IT/IS Gets a Real Business Mission**

Presented by
James Danburg
Business Process Solutions Architect
May 2006



Timeline: Legislation, Events, Impact,
The Sky is Falling?

- PIPEDA, HIPAA, GLBA, SOX, already in play
- CA 1386 forces Disclosure, **allows exclusion**, for **encryption**.
- Commencing in February 2005, (and almost monthly) security breaches flood the Newswires, and continue today
- Demand created by public for more legislation
- Consumers increase vigilance
- Payment Card Industry (PCI) Members have huge increase in fraud costs (some sources state exponential increases)
- VISA announces in November 2005, an increase in “Anti-fraud spending” by \$200M over the next four years.
- Gartner and Forrester Studies both comment on CIO’s **fears of increased compliance cost**.

Mandates, Standards, et. al.



"[in 2006, Compliance] Technology spending will amount to \$8.8B...[and] Compliance costs will continue indefinitely." – AMR Research



North American and EU Initiatives

- Privacy Act 1985 (Canada)
- Personal Information Protection and Electronic Documents (**PIPEDA**) Act 2000 (Canada)
- Health Insurance Portability and Accountability Act (**HIPAA**) 1996 (US)
- Children's Online Privacy Protection Act 1998 (US)
- Gramm-Leach-Bliley Act (**GLBA**) 1999 (US)
- Sarbanes-Oxley Act 2002 (**SOX**) (US)
- Data Protection Directive 1998 (EU)
- Planned Directive on Corporate Governance (EU)
- Payment Card Industry (**PCI**) (Updates 2005)

BORDERWARE CONFIDENTIAL/PROPRIETARY INFORMATION
© Copyright 2006, BorderWare Technologies Inc. All Rights Reserved.



BUSINESS ISSUES: PRIVACY & COMPLIANCE

- Over 50% of organizations worry about the control they have over the content sent through email
- Most organizations have decided, either because of compliance regulations and/or privacy concerns to **protect critical information** including
 - Patient Health Information
 - Financial Transactions and Trade Information
 - Patent and Intellectual Property Business Plans
 - Strategic SEC Filing Information
 - Client - Attorney Privileged Materials
 - Other Confidential Material
- Failure can be costly - lost intellectual property, erosion of customer confidence, legal action, fines, penalties, jail terms

BORDERWARE CONFIDENTIAL/PROPRIETARY INFORMATION
© Copyright 2006. BorderWare Technologies Inc. All Rights Reserved.



Regulatory, Certifications, & Policy Matrix





PCI (Payment Card Industry) Merchant Mandate

- Members: VISA, MasterCard, Discover, American Express, Diners Club
- New standards issued in June of 2005, effective January 2006
- Four levels of Merchants (based on annual transactional volume)
1) 6M+ 2) 6M-150K 3) 150K-20K 4) Under 20K

Punitive Measures for Violations & Non-Compliance

- \$500K per incident for Security Breaches (Banks can pass Fines to Merchants)
- Automatic reclassification to highest level upon breach (also highest merchant charges).
- Privilege to process charges suspended (could be temporary or permanent)



PCI (Payment Card Industry) Merchant Mandate

Service provider levels defined:

- Service providers are organizations that process, store, or transmit Visa cardholder data on behalf of Visa members, merchants, or other service providers. Service provider levels are defined as:

Service Provider Level Description:

- 1) All VisaNet processors (member and Nonmember) and all payment gateways.*
- 2) Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually.
- 3) Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 Visa accounts/transactions annually.*Payment gateways are a category of agent or service provider that stores, processes, and/or transmits cardholder data as part of a payment transaction. Specifically, they enable payment transactions (e.g., authorization or settlement) between merchants and processors (VisaNet endpoints).



PCI-DSS (Data Security Standards)

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored data
- Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security



PCI (Payment Card Industry) Merchant Mandate

<u>Group</u>	<u>Level</u>	<u>Validation Actions (required unless noted)</u>
Merchant	1	On-Site Security Audit, Annual & Network Scan Quarterly
“	2&3	Self-Assessment Questionnaire, Annual & Network Scan Quarterly
“	4	Self-Assessment Questionnaire, Recommended annual & Network Scan Recommended Quarterly
Service Provider	1	On-site Security Audit, Annual & Network Scan Quarterly
“	2	On-Site Security Audit, Annual & Network Scan Quarterly
“	3	Self-Assessment Questionnaire, Annual & Network Scan Quarterly



PCI (Payment Card Industry) Merchant Mandate

- According to the *Wall Street Journal*:
- **“Only 17% of 231 large merchants have complied with card-industry guidelines that are designed to curb fraudulent activity and reduce the potential for criminals to hack into computer networks, according to data from Visa USA Inc.”**
- **“The rules, which cover transactions on cards branded with logos from Visa, MasterCard International Inc., American Express Co. and Discover Financial Services Co., require merchants to validate a series of security measures, such as the establishment of firewalls to protect databases.”**

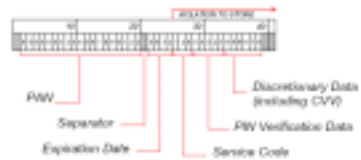


PCI (Payment Card Industry) Merchant Mandate

- **“Visa U.S.A. is considering imposing a fine on Bank of America Corp. in response to a recent data breach involving hundreds of thousands of compromised customer PINs. A source close to the investigation said Wednesday that criminals targeted debit card data stored by OfficeMax Inc. at about 30 of its 945 U.S. stores, mainly on the West Coast and in the Southeast. The source also said that Visa would fine Bank of America, though it was too early to say how large such a fine would be. The stolen account information has since been used to initiate transactions in at least three countries. In response, Citigroup Inc. blocked all PIN-based transactions initiated in Canada, the United Kingdom, and Russia.”**
- **And banks and credit unions sued BJ's Wholesale Club Inc. for a 2003 breach, demanding \$13 million in restitution for unauthorized charges involving 40,000 credit and debit cards.”**

SOLUTIONS FOR DATABASE COMPLIANCE

- DO NOT store the full contents of any track from the magnetic stripe
- DO NOT store the card-validation code (three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data))
- DO NOT store the PIN Verification Value (PVV)



PCI Safeguard Track Data: Requirement 3



PAYMENT CARD INDUSTRY ACCELERATOR

- **Protect Stored Data (Req. 3 & Req. 6)**
 - Centralizes aggregation and management of source program access
 - Provides unprecedented visibility on database activities Alerts if violation detected
 - Streamlines database security enforcement and regulatory compliance
- **Track and Monitor Access (Req. 10)**
 - No performance impact on database environment
 - Find out who is accessing cardholder information from where
 - Enables separation of duties
 - Continuous monitoring
- **Regularly Test and Validate (Req. 11)**
 - Independent of database server choice or specific database expertise
 - See who is attempting to access cardholder data
- **Streamline PCISAP reviews**
 - Automatically schedule reports and documentation
 - Send information to staff for review and signature





Common IT/IS Initiatives & Potential Collisions with the “Mandates”

- System Interoperability (SOA)

- Needed by many enterprises to connect disparate systems (often the result of M&A's) to achieve operational goals.
- Intra-nets and Portals are often involved as well (Partners and Clients can have access).

Collision Potential:

- 1) Examples exist where the operational goals are met, but also expose privacy data (as defined by the mandates) due to excessive access.
- 2) True Need-to-Know (NtK) Policies need to be defined & enforced



Common IT/IS Initiatives & Potential Collisions with the “Mandates”

- Mobile Enablement of Applications

- One of the largest and most pervasive desires in the enterprise today
- Applications go far beyond e-mail
- Include ERP, Financials, POS transaction information, EMR (patient information), many types of telematics applications

Collision Potential:

- 1) All of the above applications have Mandate defined privacy data potential.
- 2) Threats: Session Persistence, is a key vulnerability. It is variable from application to application.



Common IT/IS Initiatives & Potential Collisions with the “Mandates”

- **VOIP (Voice Over IP)**
- One of the largest technology initiatives in enterprise space
- Great deal of capital investment in this infrastructure upgrade
- Benefits are increasing, and will increase enterprise infrastructure flexibility and capability.

Collision Potential:

- **SIP (Session Initiation Protocol) is the now de-facto standard. SIP is just becoming a complete Protocol with appropriate security standards**
- **This initiative has the potential for Mandate defined privacy data violations, due to the use of text messaging via VOIP not necessarily voice calls (very difficult to intercept)**
- **Converged Messaging attacks can strike via VOIP**



Common IT/IS Initiatives & Potential Collisions with the “Mandates”

- **Open Source Trends**
- The use of open source software is pervasive. Eighty to ninety percent of Fortune 1000 companies use open source software. (Business Week, Feb 2006)
It is safe to assume that Open Source adoption will continue to grow.
- **Why Open Source use is becoming more pervasive**
 - Lower Cost of Operation
 - Reliability and Performance
 - Ease of Deployment
 - Freedom From Platform Lock –In
 - Security**



WHAT ARE THE RISKS?

Commingling of Open Source software and proprietary or third party software can trigger:

- License compliance issues (Attribution or Downstream Disclosure of modified code)
- Intellectual Property Issues (Ownership of code uncertainties due to Downstream Disclosure license requirements)
- Employment Issues due to the unauthorized use of open source by employees and noncompliance of license requirements can cause **SOX compliance** issues due to lack of controls for the use of open source and other issues
- **Mergers & Acquisitions issues due to the commingling of open source and Intellectual Property Assets.**
- The acquisition of open source software bypasses the normal procurement process
- Most organizations do not have a strategy for the use of open source
- Most organizations do not have a strategy for the use of open source by onshore and offshore outsourcing agent



HOW OPEN SOURCE RISKS CAN BE CATEGORIZED

- **Open Source risks can be broadly separated into three categories:**
 - (a) **Acquisition risks;**
Acquisition risks relate to the risks that are involved in the acquisition of software from a third party.
 - (b) **Supply risks;**
Supply risks relate to the risks involved in the supply of software whether your own or someone else's, to a third part
 - (c) **Commingling risks.**
Commingling risks are risks that involve an element of both of these aspects – for example, the acquisition of some software (open source) for the purpose of modification and on supply of the software as modified.



HOW OPEN SOURCE RISKS CAN BE ADDRESSED

- (1) **Developing a Strategy** for the use of Open Source that meets the business and technical needs of the organization and mitigates the risks associated with the use of open source software. Proactive measures include the adoption of policies to be followed when acquiring open source software.
- (2) **Performing a source Code Audit** to determine current and past use of open source.
- (3) **Executing a Source Code remediation program** to address license compliance issues and problems raised by patents and copyrights of others, covering open source code as a result of code scanning and analysis.
- (4) **Implementing Best Practices** to addresses the internal and external use of Open Source software in your client's organization.
- (5) **Creating an Open Source Review Board** to provide policy, process and procedure to ensure future compliance and mitigate risk.



Continuity of Compliance

- How to integrate these Mandates & Initiatives?
- Oh great, now I have more to do
- The “Corners” don’t understand the real impact on IT/IS
- How do I get the additional budget approvals

- **Major disconnects between IT/IS & CxO’s:**
- **Communications: one speaks “Greek” the other “Italian”**
- **CxO’s see IT/IS as “always having their hands out” (real reason for ROI)**
- **IT/IS often not proactively involved in Business Planning (both parties are liable here)**



Continuity of Compliance Mandates are your friends!

- Frameworks already defined
- Utilize Best practices
- Compliance Remediate Risk (obviously)
- Gives IT/IS a Business Mission that ties to other Business Process Departments: i.e. Finance, Legal, (Corporate Governance).
- In Fact some CEO's see SOX compliancy tools as an aid to IT/IS Governance
- Use Enterprise Appropriate Mandates as "Templates"
- As Initiatives evolve:
 - Perform Workflow Analysis (WFA)
 - Flowchart & then "Compare" with Mandates for "Red Flags"



Continuity of Compliance IT/IS Become the Watchdog's!

- By using Mandates as templates, additional communication between "The Corners" and IT/IS can be utilized using flowcharts and WFA's.
- This facilitates clear communication between departments
- IT/IS's New Mission is to Watchdog the "Mandates" (with input from appropriate departments) from a technical perspective.
- This functionally attaches IT/IS into the "Mandate" budget, rather than an additional or even separate budget item. Integration into the Business Mission is the goal.
- Some compliance tools can be used to benefit this process as well

BUSINESS CHALLENGES: PRIVACY & COMPLIANCE

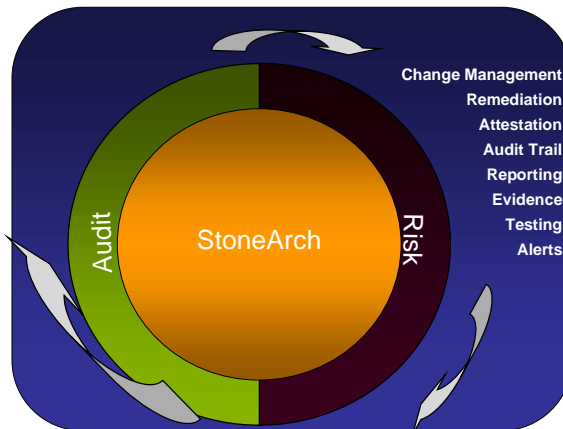
Example: E-mail

- Lack of centralized management and control of infrastructure
- Disparate systems, limited interoperability
- End-user driven and prone to error
- Different interpretations of regulatory requirements (Finance vs. IT)
- Difficult to audit and track

BORDERWARE CONFIDENTIAL/PROPRIETARY INFORMATION
© Copyright 2006. BorderWare Technologies Inc. All Rights Reserved.



SUSTAINING COMPLIANCE



Transparent Repeatability





WHAT BUSINESSES NEED

- Complete control over the types of content that enter and leave the network
- The ability to encrypt emails for greater security
- Easily address compliancy regulations
- Universal – regardless of capabilities or location of users
- Does not sacrifice usability for the sake of privacy and compliance
- Centrally managed for company-wide visibility, auditing and reporting

BORDERWARE CONFIDENTIAL/PROPRIETARY INFORMATION
© Copyright 2006. BorderWare Technologies Inc. All Rights Reserved.



REPORTING/NOTIFICATION

- Traffic and compliance reports are critical
 - Reports must be flexible to provide multiple views including
 - Overall traffic
 - Policy-specific activity
 - Traffic
 - Most active senders and receivers
 - Ranking of most common words and phrases
- All identified violations must also be easy to track and audit

Mail Filter (acted upon)	Hour	Day	Week	Month
Compliance Violation	430	430	430	430
Clean or not Scanned	115	127	127	127
Total Messages	545	557	557	557
Percent Blocked	79	77	77	77

BORDERWARE CONFIDENTIAL/PROPRIETARY INFORMATION
© Copyright 2006. BorderWare Technologies Inc. All Rights Reserved.





PRIVACY AND COMPLIANCE IS POSSIBLE!

- **You can have:**

- Control over the content that **enters and leaves** the network
- **Enforce** corporate and regulatory compliance requirements
- Deliver messages based on **policies including encryption**
- Granular content and policy enforcement **without sacrificing usability**
- Monitor **company-wide** activity
- Provide detailed reports to **proactively identify issues** and demonstrate compliance

BORDERWARE CONFIDENTIAL/PROPRIETARY INFORMATION
© Copyright 2006. BorderWare Technologies Inc. All Rights Reserved.



James Danburg
Business Process Solutions Architect
952-898-4963 E-mail: swedes3@earthlink.net

Thanks to the following organizations for their contributions:

Guardium

BorderWare

StoneArch Software

TOSTA

(The Open Source Technology Alliance)