Information Security and Operational Risk: Practical Solutions for Financial Services

June 12, 2003

Eddie Schwartz
EVP / GM Global Integrity™ Services
Predictive Systems, Inc.

Smart, Secure Infrastructure
Main Questions

• Are there any extractable operational models for effective security and privacy risk management?
• Is there any “compliance framework in a box” that can be bought off the shelf and customized to a financial services organization?
General Response

- There is no off-the-shelf framework
- Governance is still an amorphous issue within many organizations – it seems to be all over the place
- There are inherent legal and operational complexities within stakeholder networks for security and privacy management - that’s a key lesson from GLBA / HIPAA implementations
Architectural End-State Vision

Security and Privacy Management Program

Information Policy

Governance

Process

Technology

Compliance

Appropriate Actions

Measurable Results

Regulatory Compliance
What is a Security and Privacy Architecture?

• A set of guiding principles and an end-state vision that mesh with appropriate operational objectives set by the business
• An effective, well-supported and well-communicated governance structure
• An end-to-end management of process and technology areas affecting compliance
• A means to adopt a systems view toward technology solutions and measure compliance
Which Factors Shape What’s “Appropriate”?

- Legal/regulatory boundaries
- Business requirements (how the business model is designed to use customer data)
- Financial vectors
- Customer expectations
- Limits/capabilities of IT architecture
- Limits/capabilities of policy & process (management) controls, & security controls
- Risk management & compliance capabilities/maturity of organization
Benefits of a Security and Privacy Architecture

• Consistent alignment between I/T and business objectives regarding security and privacy
• Clear definition of control objectives and accountability for project teams
• Increase the level of security and privacy designed into systems, reducing cost
• Reduce risk: operational, regulatory, litigation, brand, etc.
• Information risk management becomes a repeatable and consistent process throughout the organization
## Security/Privacy Architecture

### Overall Schema Objectives

- **Ensure continuity of security/privacy management across business environments over time**

### Compliance Assurance

- Align technology support for business processes and security/privacy controls

### Risk Management

- Identify people across the enterprise accountable for security and privacy management
- Define policies articulating strategies and objectives across the enterprise

### Governance

- Aligned security and privacy organization and policies with business objectives

### Processes

- Align technology support for business processes and security/privacy controls

### Technologies

- Ensure continuity of security/privacy management across business environments over time

<table>
<thead>
<tr>
<th>Structural Elements</th>
<th>Functional Elements</th>
<th>Key Management Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Management</td>
<td>Governance</td>
<td>• Identify people across the enterprise accountable for security and privacy management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Define policies articulating strategies and objectives across the enterprise</td>
</tr>
<tr>
<td>Operational Management</td>
<td>Processes</td>
<td>• Align security and privacy organization and policies with business objectives</td>
</tr>
<tr>
<td></td>
<td>Technologies</td>
<td>• Align technology support for business processes and security/privacy controls</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Compliance Assurance</td>
<td>• Ensure continuity of security/privacy management across business environments over time</td>
</tr>
</tbody>
</table>
# Security/Privacy Architecture Management Processes

<table>
<thead>
<tr>
<th><strong>Structural Elements</strong></th>
<th><strong>Functional Elements</strong></th>
<th><strong>Key Management Processes</strong></th>
</tr>
</thead>
</table>
| Administrative Management | Governance             | • Organizational Design / Roles  
|                         |                         | • Policy Development          |
| Operational Management  | Processes               | • Standards/Guidelines Deployment  
|                         |                         | • Risk Assessment (policy-level) |
| Risk Management         | Compliance Assurance    | • Security                    
|                         |                         | • Information Management      |
|                         |                         | • Assess & Deploy Privacy Support Technologies (PETs) |
|                         |                         | • Risk Assessment (technology-level) |

**Key Management Processes:**
- Training
- Due Diligence / 3rd Party Assurance
- Documenting Policies & Processes
- Monitoring & Verification
## Security/Privacy Architecture

### Governance

<table>
<thead>
<tr>
<th>Structural Elements</th>
<th>Functional Elements</th>
<th>Key Implementation Tasks and Controls</th>
</tr>
</thead>
</table>
| Administrative Management | Governance: • Organization • Roles • Policy Development | • Develop CISO / CPO role & functions, define responsibilities and accountabilities, reporting channels  
• Enterprise stakeholder task force to set objectives, define policies and manage macro-level decisions  
• Operational working groups to manage program execution; identify line of business and functional information risk managers  
• Enterprise polices defining overall objectives and strategies  
• External policies to benchmark privacy objectives for consumers, regulators |
Characteristics of Successful Governance Structures

• Accountability
  – Organizational design, roles, ownership, competency

• Transparency
  – Reliability, durability and ease of use of supporting information

• Disclosure
  – Timely and complete communications, clear standards/plans

• Independence
  – Continuous improvement, 3rd party review and measurement
Governance Sample Questions

- What is the overarching process for governing the use of information?
- Who owns the customer records?
- Who responds to security and privacy inquiries from customers and regulators?
- Who has the authority to make decisions with respect to the use of the data?
- What is the accountability and reporting model?
## Security/Privacy Architecture

### Processes

<table>
<thead>
<tr>
<th>Structural Elements</th>
<th>Functional Elements</th>
<th>Key Implementation Tasks and Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operational Management</strong></td>
<td><strong>Processes</strong></td>
<td>• Internal policies to benchmark information risk objectives and strategies for management across lines of business and business functions</td>
</tr>
<tr>
<td></td>
<td>• Policy, Standards Deployment</td>
<td>• Development of granular business rules for information use</td>
</tr>
<tr>
<td></td>
<td>• Risk Assessment</td>
<td>• Identify target audience and mechanisms for ensuring and tracking external policy delivery</td>
</tr>
<tr>
<td></td>
<td>• Change Management</td>
<td>• Define control objectives for internal policies &amp; business rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Identify target audiences for internal policy customization and deployment (customer service, distribution channels, affiliates, vendors and other third parties)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Identify responsibilities and accountabilities at operational levels (e.g., distribution/sales &amp; marketing, customer service, data processing)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Implementation plans and tracking</td>
</tr>
</tbody>
</table>
Process
Sample Questions

- What processes are followed in the lifecycle of information?
- Who touches the information?
- Who has access to the information?
- How is information labeled?
- How do CSRs handle the data?
- Are there any rules in place for the secure handling of the data?
Security/Privacy Architecture Technology

<table>
<thead>
<tr>
<th>Structural Elements</th>
<th>Functional Elements</th>
<th>Key Implementation Tasks and Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operational Management</strong></td>
<td><strong>Technologies</strong></td>
<td>• External regulatory environment review to focus baseline risk assessments and gap analyses</td>
</tr>
<tr>
<td>• Align technology support for business processes and security/privacy controls</td>
<td>• Information Management</td>
<td>• Internal technology assessment - security architecture and controls</td>
</tr>
<tr>
<td></td>
<td>• Integration</td>
<td>• Map data flows to identify risk areas and regulatory control points (e.g., customer service, distribution channels/customer acquisition, data sources, affiliates, vendors and other third parties)</td>
</tr>
<tr>
<td></td>
<td>• Security</td>
<td>• Internal technology assessment - information management controls for tracking and ensuring implementation of customer preferences</td>
</tr>
<tr>
<td></td>
<td>• Privacy Support Technologies (PETs)</td>
<td>• External technology assessment - additional security enhancements and appropriateness of privacy enhancing/supporting technologies</td>
</tr>
<tr>
<td></td>
<td>• Risk Assessment</td>
<td>• Develop employee awareness and meet regulatory obligations for training</td>
</tr>
</tbody>
</table>
Technology
Sample Questions

• How is the data organized, labeled, and stored?
• What paths does the data take when getting from point A to point B and how are these paths protected?
• Who is responsible for the management of these information systems?
• Is there positive control over the data at all time? How is access control managed?
• What specific security mechanisms surround the use of the data?
## Security/Privacy Architecture

### Compliance

<table>
<thead>
<tr>
<th>Structural Elements</th>
<th>Functional Elements</th>
<th>Key Implementation Tasks and Controls</th>
</tr>
</thead>
</table>
| Risk Management     | Compliance Assurance| • Develop employee awareness and meet regulatory obligations for training  
                      |                     | • Test security and privacy controls  
                      |                     | • Privacy Impact/Technology Risk Assessments to verify compliance, create documentation archives, perform due diligence  
                      |                     | • Due Diligence- ongoing vendor review new business initiatives impacting information resources, vendor assessment, review of potential partners, adoption of new information technologies  
                      |                     | • Compliant resolution processes  
                      |                     | • Feedback and revision mechanisms- including revision of privacy objectives and strategies, assurance of complaint resolution and customer inquiries  
                      |                     | • Verification of compliance |

- Ensure continuity of information risk management across business environments over time
- Measure and report
Compliance Sample Questions

• Is there an information risk management compliance strategy?
• What are the elements of the compliance program? Security? Privacy?
• What is the role of the auditor?
• Does the compliance program have teeth?
• What are the characteristics of the reporting?
Working with Stakeholders
-- Get Everyone Involved

- Business Unit Risk Managers (Data Owners)
- Privacy Officer
- Information Security Officer
- Product and Operational Leads
- Information Technology Managers
- General Counsel
- Government Affairs
- Compliance Office
- Internal Audit
- Human Resources
- Marketing
- Business Partners
- External Auditor
- CEO/Board
Bottom Line Regarding the Regs and Risk Mgmt

- The statutes are all somewhat intentionally vague (that’s a good thing!) -- basically, you have to have a real security program in place
- You need to meet a demonstrable “standard of due care” and tests of reasonableness for your sector / organizational size / criticality
- If you don’t already have CEO-level support for security and privacy programs, add this fuel to the fire
Understand the Doctrine Inside & Outside the Sector

• Guidelines:
  – GLB Section 501(b) and FTC Advisory Committee on Online Access and Security
  – HIPAA/HHS Requirements
  – International Requirements (e.g., EU Data Protection Directive 95/46/EC)
  – FFIEC Guidelines (v.2), BASEL II
  – ISO 17799
  – ISF Standards of Good Practice, v2
  – FISMA
  – Many others…..
Summary

• It’s time to get serious about information risk management / governance
• Define and communicate the end-state vision
• Obtain CEO support
• Define roles and accountabilities up-front
• Don’t underestimate the work involved and the associated costs and time to complete
• Use formal approaches for gap analysis, risk assessment, planning, and operations
• Monitor, measure and report to the CEO
Questions?

egschwartz@computer.org
+1-917-533-6536
Additional Reference Material

Smart, Secure Infrastructure
Network Security Issues

• Use perimeter defenses
  – Firewalls
  – Intrusion Detection
  – Log file monitoring

• Protect the data paths carefully
  – Encryption
  – Device/Server Authentication
Database Security Issues

• Typically the most difficult security problem
• Areas of concern and focus:
  – Data Architecture
  – General and Administrative Access Controls
  – Role-based Access Control
  – Auditing
• Tools
  – Disassociation technologies
  – Database encryption
Other Tools in the Toolbox

• Identification, Authentication, Authorization
  – Two-factor, data segmentation, directory services, role-based access

• PKI/Encryption
  – Digital IDs, Digital signatures, VPNs

• Access Auditing
  – Notice, data integrity, Opt In/Opt Out

• Monitor Threats
  – Use an vulnerability alerting service
Architecture and Technology

- Policies and procedures build the foundation for technology use practices
- The technology does the end work of encrypting, storing, and transporting the data
- Don’t forget the legacy systems, be realistic about constraints
- *Integrate* the security and privacy technology, don’t bolt it on
Test and Train

• Education is essential!
• Deliver staff training on the issue:
  – Legal and ethical requirements – no one can opt-out!
  – Solicit feedback
  – Management involvement and clear sponsorship
• Don’t expect perfection
• Practices that are not reasonable will not be followed
• Get buy-in and get it in writing
• Watch and learn, hone as necessary
Compliance Monitoring

• Areas of monitoring should include:
  – Policy dissemination
  – Security and systems integrity
  – General compliance and control procedures
  – Business process -- disclosure and security/privacy risk management activities of affiliates and other related parties
  – Internet monitoring of all online sites
To-Do List for FSPs

• Audit prep and remediation (FFIEC Guidelines)
• Security implementation (federal, state; service provider/partner reviews)
• Ensuring data are controlled as represented-understanding data flows/relationships
• Governance - especially as FSPs develop; alignment of privacy and security strategies/objectives
• Due diligence- M&A, partnerships, new technologies, new business development, new information resources
• Multinational issues
• Compliance assessment/assurance/monitoring