Security Monitoring and Compliance Management: Two Sides of the Same Coin?

Anthony Gerkis, Accenture Security Technology Consulting
Kenton A. Hoover, Symantec Global Services
Agenda

1. Security and Compliance
2. Two Sides of the Same Coin
3. Services are Key
4. Summary and Closing
Security management and compliance scopes are complex and extensive

Executives are concerned that while they focus on compliance, new security threats may be lurking - how do you manage actual threats while focusing on compliance?

<table>
<thead>
<tr>
<th>Business</th>
<th>CRM services</th>
<th>SCM services</th>
<th>OMM services</th>
<th>R&amp;D services</th>
<th>BIS services</th>
<th>F&amp;A services</th>
<th>C&amp;C services</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Delivery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Mgt.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Mgt.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Mgt.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Mgt.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bus. App'n</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Structured</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unstructured</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connectivity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data centers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact centers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Traditional territory of IT security
Security and compliance management consume similar sets amounts of data

- System events
- Firewall and IDS traces
- Application events
- Account grants
- Physical access logs
- External threat intelligence
- Patch logs

“Before beginning a hunt, it is wise to ask someone what you are looking for before you begin looking for it.”
— Winnie the Pooh
Organizations are looking for ways to manage the complexity of security and find that security investment decisions are driven by compliance.

- Complex regulatory requirements
- Lack of control and automation
- Increasing complexity of threat landscape

Note: Multiple responses allowed.
Base: 966 U.S. sites in 2006; 2523 in 2005
Data: InformationWeek/Accenture Global Information Security survey of 2,193 Global business-technology and security professionals
The implications of non-compliance…

Inability to manage IT security just result in decreased IT availability and performance, while regulatory non-compliance can result in financial penalties. But security failures often expose compliance faults.

Visa fined 77 companies for a total of $4.7 million in 2006 for non-compliance with PCI standards.

Source: Gartner research

Failure to comply requires greater amounts of reserve capital

Basel II framework

Visa USA will link interchange rates to PCI starting 31 August 2007

Source: VISA Press Release

Ultimately, it lowers business agility by imposing new barriers to market entry, increasing operational expense and lowering margins
Firms want to leverage security and compliance investments

Use compliance as an agent of change and improvement

• Comprehensive approach with strategic planning
• Managing to acceptable level of risk
• Comprehensive views and regaining control of the IT infrastructure
• Competitive advantage: improved efficiencies and effectiveness

How does your organization measure the value of your security investments?

Lower FTE for security issues

Data: InformationWeek/ Accenture Global Information Security survey of 2,193 Global business-technology and security professionals

CIOs don’t measure compliance the same way
CIOs have the same concerns around both compliance and security

- What should we do when we find a problem?
- How do I know which events represent an actual problem?
- How can I tell how serious it is?
- How do I preserve my business agility?
- Which data is important to preserve? Am I storing it properly?
- What are the industry “best practices”?
- How do I measure the effectiveness of my efforts?
Typically, massive amounts of security data are collected but not used effectively.

BEFORE
Separate and highly manual auditing and logging processes, with most security information analyzed in isolation or not at all

AFTER
Efficient security monitoring and management across all IT environments, providing consolidated management views

Outsourcing vendor management reports

Separate and consolidated views
Security Monitoring Architecture

Infrastructure security solutions base on Symantec technology for compliance and security management enable automation and intelligent reporting.

- Global threat intelligence
- Monitoring
- Correlating
- Alerting
- Reporting
- Log management
- Forensic analysis
Two Sides of the Same Coin: Architecture Comparison

Compliance Transformation Architecture

- Solution Defined: Vision, Roadmap, Strategy, Integration Plan
- Monitoring Defined: System Prioritization, Policy Engine Rules, Log Collection
- Rules Defined: Compliance Requirements, Risk Definition, and Storage
- Action Defined: Strategy, Governance, Policy, and Remediation Processes
Two Sides of the Same Coin: Architecture Comparison

Security Management and Monitoring Architecture
The drivers and operational reality for security and compliance differ greatly...

- Top-down versus bottom up drivers
- Real-time response versus long-term governance
- Vulnerabilities as defects or policy violation versus lack of security controls
- Broad regulatory needs versus targeted incident remediation
- Incident management versus remediation roadmap
- Correlation versus policy management
- Audit ownership versus infrastructure ownership
… although the successful solution is the same!

- Leveraging a core architecture
- Managing massive amounts of data and the complexity of security
- Success through people, processes and technologies
- Tools to enable decision making
- Automation and on-going monitoring
- Prioritization key to decision making
Comprehensive controls-driven security objectives leverages the same information and infrastructure provided by a more technically focused vulnerability management life cycle.

- Vulnerability management provides a subset of comprehensive controls for compliance
- Controls and infrastructure create a foundation of a security program
- Controls comprise technologies and configuration of IT infrastructure
It is recognized that a strong vulnerability management program and infrastructure that is properly mapped to compliance objectives, enables automation and compliance success.

- **Degree to which IT controls have been operationalized will be audited**
  - Vulnerability management processes and workflows can support audit and reporting for regulatory compliance
  - Organizations that already have a strong vulnerability management program can use policy, assessment, baseline and remediation functions to prove operational implementation of some major IT controls
- **Organizations that have mapped their controls to applicable security policies will have a more defensible posture in any audit discussion**
  - Ability to more fully automate controls auditing and compliance reporting driven by this mapping
  - Operationally implemented controls through a vulnerability management program will help demonstrate a strong security and compliance posture

Source: Gartner Research 2006
The size and complexity of the overall challenge can be amplified…

- Knowledge and skills gaps
- Technology and process gaps
- Size and complexity issues
- Lack of automation

Technology is only one part (and at most 25%) of any IT solution
...and services provide the framework to scale to address business needs.

- Enablers go far beyond technology
  - Strategy
  - Governance
  - Policy
  - Processes
- Baseline operational assessment
- Incident response capability
- Managing risk for compliance and incident response

The value of services is to maximize the effectiveness of whatever technology, process, management and remediation strategies have already been acquired or devised.
Three-quarters of typical compliance effort in enterprises focuses on IT…

The CIO’s Burden…

- ERP, CRM, SCM
- Financial Systems
- Online Sales
- Internet Security
- Telephones
- Messaging
- System Access
- Network Access
- Remote Access
- Data Protection
- Business Continuity

“Candidly, my biggest current threat is the army of auditors that are sapping my energy and diverting the attention of my people.”

– Fortune 100 CISO

Majority of compliance cost is IT related

- 76%
- 24%

Source: IDC
Enterprises face “compliance overload” because of highly manual, costly processes for managing and reporting on compliance requirements

**BEFORE**
Separate and highly manual management processes, and reporting for each compliance or industry standard

**AFTER**
Efficient compliance management program, with streamlined processes, automated tools, with consolidated reporting and dashboard views

Transform an often fragmented, complex compliance approach to a simple, consistent compliance program
Accenture and Symantec bring together a unique set of complementary capabilities and assets to provide security and compliance solutions.

### Customer Solutions

- Broad portfolio of security and storage products and solutions
- Fourth largest software company in the world
- Integration capabilities for products and solutions
- Operational skills
- Technical specialists
- Security expertise
- Global security intelligence network

- End-to-end offerings
- Ability to scale quickly
- Industry-leading business process outsourcing
- Best-in-class security expertise
- Integration with IT operations
- Reduced complexity and cost of operations

- Business consulting
- High performance business process transformation skills
- Security expertise
- Deep industry knowledge
- Global footprint and scalability
- Broad technology infrastructure and application expertise
- Ability to leverage lower-cost offshore resources
Conclusion

• Organizations need to reduce the cost of security monitoring and to manage the growth of compliance-related costs

• Combining security monitoring and compliance transformation leverages the automation from each to ensure best performance for both
  – Understand the needs and drivers of your client
  – Position security as an enabler of high performance
  – Assess and manage risk in terms of disruption and value to the business

• View both security and compliance as catalysts for business improvement and innovation
  – Converged benefits strengthen the value proposition of solutions

• Success is defined as less FTE spent on security-related issues
  – … while at the same time meeting compliance and security monitoring goals
Security and compliance programs enable business opportunities...

Should we focus on incrementally mastering the rules…

…or the new opportunities?

- New Markets
- Regulated Markets
- Mergers & Acquisitions

Symantec VISION 2007