Using Continuous Monitoring Information Technology to Meet Regulatory Compliance

Presenter: Lily Shue

Director, Sunera Consulting, LLC

Outline

- **Current regulatory requirements in the US**
- **Challenges facing financial institutions or organizations maintaining customer information**
- **Tools and approaches use to meet the compliance challenges**

Current Regulatory Requirements in the US

- The Gramm-Leach-Bliley Act (GLBA) of 1999 requires financial institutions in the United States to create an information security program to:
  - Ensure the security and confidentiality of customer information
  - Protect against any anticipated threats or hazards to the security or integrity of such information
  - Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer

Current Regulatory Requirements in the US

- **Other Regulatory Requirements**
  - **Sarbanes Oxley (controls)**
  - **HIPAA (patients information)**
  - **FISMA (US Federal Information Security Management)**

What Organizations Must Do to Meet These Challenges?

- **Financial institutions and organizations must**
  - **Collect and archive cross-platform log data real time**
  - **Compress logs for efficient long-term storage**
  - **Simplify search and retrieval of specific logs for analysis and forensic investigations**
  - **Automatically identify important audit events and alerts appropriate individuals**
  - **Provide an easier and more affordable way to automate**
    - log & event management for compliance
    - file integrity monitoring for compliance

What Organizations Must Do to Meet These Challenges?

- **Financial institutions and organizations must**
  - **Maintain an ongoing information security monitoring and risk assessment program to comply with the regulatory requirements**
  - **Log data collections; review, archival, reporting and alerting of customer non-public-information (NPI)**
  - **Monitor file integrity**
    - Sarbanes Oxley
    - HIPAA
    - FISMA
    - Etc

What Organizations Must Do to Meet These Challenges?

- **Corporate and IT governance at financial institutions must now extend the continuous monitoring from applications/business processes to:**
  - **Monitoring and maintaining an inventory of NPI databases/files**
  - **Monitoring unauthorized access and providing alerts on a real-time basis**

What Organizations Must Do to Meet These Challenges?

- **Systems (in-house developed or acquired) must have:**
  - **Appropriate security controls**
  - **Controls to mitigate the risks posed by internal users disclosure or alteration of sensitive information in storage and transit**
  - **An inventory of all databases/files containing customer non-public-information (NPI)**
  - **Measures to:**
    - Monitor access to NPI
    - Monitor and control downloading of NPI outside the institution Implement malicious code prevention

Why So Difficult?

- **With the current information technologies capabilities, users can now create files and databases containing NPI to meet business requirements**

- **It would be next to impossible to manually monitor and maintain an inventory of databases/files containing NPI**

How Organizations Meet These Challenges?

- **Financial Institutions and organizations are implementing automated tools to:**
  - **Collect, aggregate and maintain all log data from all sources**
  - **Protect customer information by providing visibility across the entire IT infrastructure to detect, repair and remediate operational issues**
  - **Collect real-time alerts of violations related to:**
    - Compliance mandates – unauthorized creation and transferring of files with NPI
    - Security threat identification and suspected intrusion
    - Operational problems
    - Activities taken place inside database servers to ensure data security

How Organizations Are Meeting These Challenges?

- **Financial Institutions and organizations are implementing automated tools to:**
  - **Monitor change and configuration management of assets**
  - **Monitor security controls**
  - **Monitor updates and reporting**
  - **Monitor and detect changes or event activity associated with potential security attacks and intrusion s into customer information systems**

How Organizations Meet These Challenges?

- **Automated monitoring tools include:**
  - **In-house developed applications**
  - **Third party software vendor tools**

Summary

- **Corporate and IT governance at financial institutions must now extend their continuous monitoring program from applications/business processes to:**
  - **Monitoring and maintaining an inventory of NPI databases/files**
  - **Monitoring unauthorized access and providing alerts on a real-time basis**
  - **Securing all customer NPI**
- **IT must implement automated tools to meet the regulatory compliance requirements**
  - **In house developed tools**
  - **3rd party continuous monitoring tools/software**

Questions?

Thank You

SUNERA