Logging and Auditing in a Healthcare Environment

Mac McMillan

CEO CynergisTek, Inc.

OCR/NIST HIPAA Security Rule Conference

Safeguarding Health Information: Building Confidence Through HIPAA Security

May 11, 2010

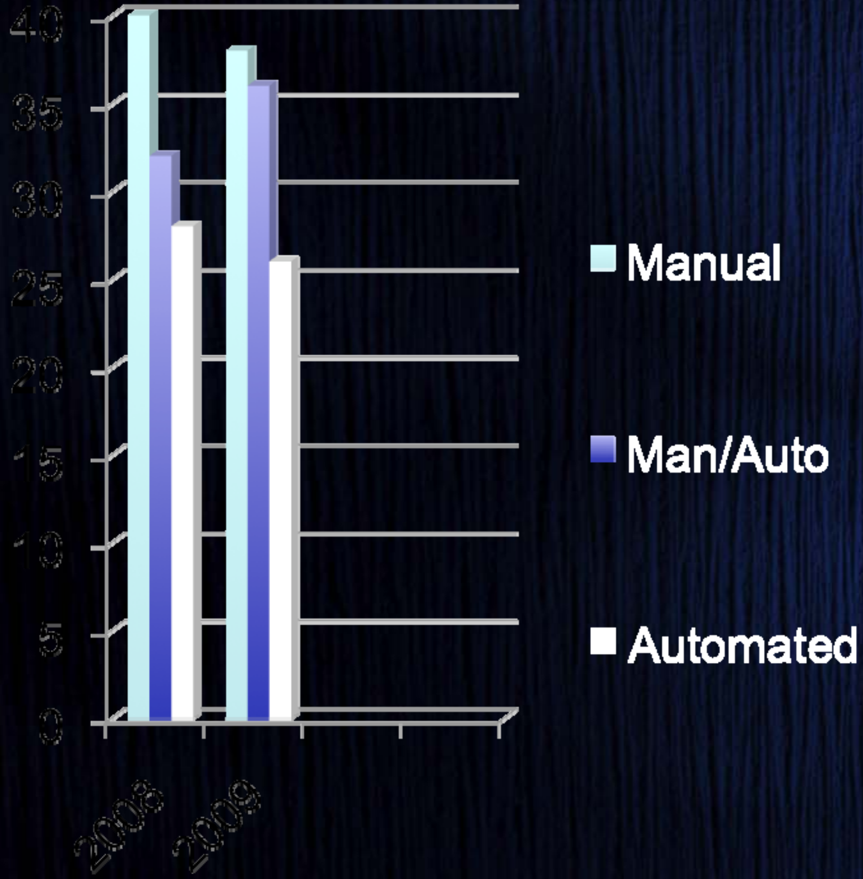
Introduction

- HIMSS Privacy & Security Steering Committee
- Former Chair, HIMSS Information Security Working Group
- National Practice Director, CTG Healthcare Solutions
- Director of Security, SAIC Intelligence Solutions Group
- Director of Security, Defense Threat Reduction Agency, DoD
- Director of Security, On-Site inspection Agency, DoD
- DoD Critical Infrastructure Protection Committee
- Information Security in Healthcare: Managing Risk

Logging & Audit in Healthcare

- Current Trends
- Logging & Audit Requirements
- Privacy vs. Security
- Correlation
- Challenges & Barriers
- Observations

Logging & Audit Trends



- 2008 – only 60% using automated or partially automated means to collect/review log data
- 2009 – only 64% using automated or partially automated means to collect/review log data

HIMSS Annual Survey – Log Sources

• Firewall Logs	83%
• Application Logs	72%
• Servers	70%
• Intrusion Detection	60%
• Network Devices	61%
• Additional Storage Devices	15%
• Don’t Collect	6%

Growth in Log Data

- According to SANS survey there is a 15/20% growth in log data being collected each year, primarily due to:
  - Increased log sources
  - New regulations
  - Inclusion of application logs

Frequent Themes Expressed

- Frustration with primarily reactive processes
- Frustration with time consuming manual processes
- Lack of confidence in manual searches
- Desire to mitigate potential public embarrassment
- Gaps in current SIEM/Log Management solutions to address clinical applications
- Lack of log/audit functionality in systems

Proliferation of Regulations with Log/Audit Requirements

- HIPAA/HITECH
- FTC Red Flag Rules
- 21 CFR Part 11
- 42 CFR part 2
- SOX
- GINA
- FISMA
- Payment Card Industry/Data Security Standard
- State Laws

HIPAA/HITECH requirements driving logging and audit

- Risk Management
- Information System Activity Reviews
- Audit Controls
- Accounting of Disclosure

- Meaningful Use
- EHR Certification
- Breach Notification
- Accounting of Disclosures

Some Other Requirements

- Data retention policies
- Account management reviews
- Process audits
- Controls audits
- Third Party security audits
- User education/awareness

Collection & Uses of Log Data

- Detect/prevent unauthorized access and insider abuse
- Meet regulatory requirements
- Forensic analysis and correlation
- Ensure regulatory compliance
- Tracking suspicious behavior
- IT Troubleshooting & network operations

Breach Data/Enforcement Demonstrate Need

- Number of organizations reporting breaches increased 6% over last year
- 80+ breaches of 500 records or more to OCR in 2010, countless smaller ones
- Malicious intent is still “less likely” to be cause
  - – Unauthorized access by User
  - – Wrongful access of paper based records
  - – Physical loss/theft of device

Disjointed Efforts

- Privacy and Compliance organizations have focused on application monitoring
- Technical and Security organizations have focused on monitoring events affecting security of the IT infrastructure
- This approach is inefficient and adds to the risk of exploitation

Privacy vs. Security Auditing

- Privacy violations
- Internal Threats
- EHR/Clinical applications
- Application log managers

- Network/system security
- Internal/external Threats
- IT Infrastructure
- Network log managers/SIEM

Using Other Technologies to Audit

- Data Loss Prevention
- Email Encryption
- Vulnerability Scanners
- Policy Management Scanners
- Configuration Managers

How Correlation Enables Proactive Audit and Monitoring

- Increases efficiency in investigative processes
- Multiple reports increases confidence
- Assists in identifying false alarms
- Missing data is not as limiting
- More thorough understanding of incidents
- Reduces number of false alerts

Correlation Does Matters

- Confirmation of multiple pieces of information
- Statistical correlation
- Historical correlation
- Pattern or rule-based correlation

Challenges/Barriers

- Volume of systems/data
- Lack of Integration
- Identity Management
- Lack of Access
- Health Information Exchanges

- Lack of functionality
- Lack of definition
- Lack of data elements
- Lack of correlation
- Lack of data mapping

Healthcare Logging & Audit Needs

- Behavior based modeling for privacy enforcement
- Proactive alerting of potential issues
- Accurate search and investigative functionality
- Correlation across critical applications and systems of log events
- Early detection of security/privacy breaches
- Automated reporting/alerting for prompt action

Opportunities for Improvement

- Federal guidance on logging and audit requirements
- Vendor inclusion of audit functionality and necessary data in clinical applications
- Inclusion of logging/audit functionality in EHR certification criteria
- Continued development of log management and SIEM product improvements and integration
- Address identity management shortfalls

Questions

References

- 2010 HIMSS Analytics Report: Security of Patient Data – Kroll Fraud Solutions
- 2008/2009 HIMSS Security Survey – Booz Allen Hamilton/Symantec
- SANS Sixth Annual Log Management Survey Report