Capturing the Synergy Between Information Security and Internal Audit/Compliance: Challenges, Benefits and Opportunities

NCHICA Presents the 12th AMC Security & Privacy Conference

Managing Security & Privacy in an Environment of Increased Risk & Threats

June 27-29, 2016 • The Friday Center, Chapel Hill, NC

June 28, 2016
Panel Members

Phyllis A. Patrick, MBA, FACHE, CHC, CISM

Alan Moorhead, CPA, CISA, CFE, CFSA
Alan Mitchell, CISSP, NSA, IAM, ITIL

Ed Taliaferro, CFA, CFE, CRMA
Patricia Skarulis, MA, LCHIME
Our Agenda

Changing roles, responsibilities and priorities: information security and internal auditing

Collaboration: building relationships for shared success

Scenarios and case studies
  - Hanger, Inc.
  - Memorial Sloan Kettering Cancer Center

Lessons learned: going forward
Learning Objectives for the Session

• Understand the different perspectives and skills of the Chief Audit Officer (CAO) and the Chief Information Security Officer (CISO) in protecting the organization’s information resources.

• Discuss how to develop and exploit the synergy between information security and internal audit in assessing risk and protecting information from a variety of risks.

• Describe what other organizations are doing and what lessons can be learned from case scenarios.
Questions for Session Participants

• How is the Internal Audit department involved in the Information Security Program?
• How is your program organized?
• Where does the Information Security program report?
• Is Internal Audit involved in ongoing risk assessment and management for the organization as a whole?
• Is risk assessment and management for information security separate from other risk areas?
• How is information security included in the annual audit planning process?
• Your Questions ???
Focus on the Information Security Officer

Responsibilities often combined with existing roles (CIO, IT Network Director, Privacy Officer, HIPAA Officer, etc.) – “doing double duty”

Security may be viewed as IT function – i.e., technical controls

Generally not designated senior management position

Program developments and metrics not reported to Board

Profile of CISO changing (larger organizations, independent networks)
Primary Responsibilities of CISO

Coordinate development, implementation and management of the information security program for the organization.

Coordinate development, implementation, and communication of policies, standards and procedures required for the organization’s information security program.

Work with the Privacy Officer (PO) to assure that privacy and security programs meet the organization’s needs and support other requirements (e.g., Health Information Exchange, etc.).

Identify information security goals, objectives and metrics consistent with the corporate strategic plan.

Ensure that organizational policies and practices support compliance with regulations.
Evolving Role of the CISO

Role and responsibilities are being re-evaluated in some organizations. CISO position is being elevated to senior leadership with enhanced responsibility for strategic planning and oversight of the entire security program.

Regular reports on status of programs to Board and senior leaders responsible for compliance, risk, and audit oversight is important.

Alignment with Compliance and Privacy Officers, Internal Audit, General Counsel, Risk Management, and others is key to gaining support and getting the job done.
Case Scenario: Hanger

Alan Moorhead, CPA, CISA, CFE, CFSA
Alan Mitchell, CISSP, NSA, IAM, ITIL
• James Edward Hanger, first amputee of Civil War
  • Patented prosthesis with functional knee
  • Established JE Hanger Corporation in 1861
  • Expanded company nationwide

• Hanger, Inc., nation’s largest O&P company
  • Over 800 patient care clinics
  • Largest O&P distribution network
  • Nationwide contracting division
150 Years of Progress & Empowerment
Patient Empowerment

Managing Security and Privacy in an Environment of Increased Risk and Threats
Public Acceptance
Technology

Managing Security and Privacy in an Environment of Increased Risk and Threats
Potential to Achieve

Activities of Daily Living
Technology Areas of Influence

- Documentation & patient management
- Design & fabrication
- Component performance
- Outcomes measurement
Component Performance

Managing Security and Privacy in an Environment of Increased Risk and Threats
Materials Technology
Cyber Security Threat Landscape and State of Healthcare

• For the first half of 2015, the healthcare industry had the highest number of data breaches with 187 (which accounts for 21% of total number of breaches).

• Healthcare led the way with the number of records breached with 84.4 million records, or 34% of the total.

• There is a large ROI for hackers and unlike financial data you cannot just close an account or issue a new card for someone’s health data.

• Attack planning and methods are becoming more sophisticated but we should not confuse the planning and execution with the sophistication of some of the basic security paradigms that are being compromised.

*Healthcare informatics
Oh, but these are “sophisticated attacks” - right? What could we possibly do?

Many of the root causes of some of these attacks are poor security hygiene and practices.

• Old unpatched systems exposed to the Internet
• Having little visibility or understanding of their own networks
• Weak passwords or even using password instead of other security controls
• Too much access
• Applying inadequate security controls to your vendors
How can your organization be prepared?

• Keep systems updated. Take the time to test updates and apply them quickly. This includes keeping the operating system version up to date. If you have old systems that aren’t updated regularly, don’t expose them to the Internet.

• Increase your visibility into what’s happening on the network. This can be done by adopting a combination of products that provide intrusion protection, security information and event management (SIEM) and network traffic monitoring capabilities.
Be prepared (Cont’d)

• Build an internal security operations center (or outsource it to a managed security services provider) to monitor the alerts and events generated by your security systems, and follow up and investigate all “odd findings.”

• Create operational procedures for responding to common events such as server reboots, account lockouts and alerts generated by the anti-virus software. An event happening on an internal workstation may need to be handled differently than the same event on an Internet-facing server.
Be prepared (Cont’d)

• Make sure the level of logging is appropriate and that logs are stored centrally to make them hard to tamper with and easy to access during a security incident.

• Periodically perform penetration testing exercises to identify systems and applications showing vulnerabilities that have to be addressed quickly. Include your 3rd party vendors.

• Have a response plan and establish relationships with law enforcement and regulators now!
Ransomware: the new trend

Ransomware is malware that infects your systems and encrypts your data and then the attackers demand payment to unlock your system.

- What drives the success
- Lack of user awareness
- Poor patching procedures
- Not backing up data or not backing up data timely
Insider Threat

• Unknowingly compromised systems
  – APT targets
  – Organized crime and state sponsored
  – Cyber-crime underground

• Malicious insider
  – Disgruntled employee
  – Organized crime and state sponsored
  – Cyber-crime underground
Figure 3: An individual data breach can cost on average up to USD6.53 million, according to the 2015 Annual Cost of Data Breach Study: Global Analysis from Ponemon Institute (sponsored by IBM).
There is room to do better

“We have to get lucky all of the time, the adversary only have to get lucky some of the times.” – Robert Mueller
The Partnership

• A state of transition
  – CISO and CAO partnership
  – Risk assessment at enterprise and functional level
  – Initial focus on low hanging fruit

• Stabilize for growth
  – Ensure compliance
  – Promote best practices and ownership
Approach

- Shared objectives
- Coordinated effort
- Leverage respective points of influence to achieve results
- Areas of focus
  - Access and protection (data)
  - Networks
  - Development projects
Benefits

• Consistent message across the business
• Unified effort – efficiency through synergy
• Leveraged skills and resources
• Enhanced awareness and ownership across the business
Managing Security and Privacy in an Environment of Increased Risk and Threats
Case Scenario: MSKCC

Ed Taliaferro, CFA, CFE, CRMA
Patricia Skarulis, MA, LCHIME
MSKCC’s Working Relationships

• MSK Organization
• IT Governance Structure
• Internal Audit working with IS
  – Applications Inventory
  – Mapping IT Capabilities Against Prescribed Policies and Procedures
• Compliance working with IS
  – Monitoring PHI Access
  – Data Loss Prevention
MSK Internal Audit, Compliance, Information Security Organization Structure

All IT resources do not report to CIO

Managing Security and Privacy in an Environment of Increased Risk and Threats
Managing Security and Privacy in an Environment of Increased Risk and Threats
# Application Inventory

The application risk map is a single repository of all MSK applications which tracks the risks associated with each application.

<table>
<thead>
<tr>
<th>Department</th>
<th>Application</th>
<th>Description</th>
<th>Total Combi</th>
<th>Score</th>
<th>Included in Analysis</th>
<th>Department Validated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Physics</td>
<td>Kemper</td>
<td>Inventory of medical devices</td>
<td>171</td>
<td>H</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Clinical Information Center</td>
<td>PreOp Workflow (Vendor)</td>
<td>This application tracks the necessary patient documents that need to be completed prior to surgery. Documents are flagged within the application when completed and reviewed. (this application will be in production before year-end).</td>
<td>170</td>
<td>H</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Medical Physics</td>
<td>Metropolis</td>
<td>New planning system for patients receiving external beam radiation treatments.</td>
<td>170</td>
<td>H</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bernoulli</td>
<td></td>
<td>Intranet based management console for Respiratory Therapy’s ventilator machines.</td>
<td>169</td>
<td>H</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Clinical Information Center</td>
<td>Transcription Processing System</td>
<td>The Transcription Progress Notes System (Prognote) captures transcribed reports so they can be routed to physicians in baskets in the Electronic Signature System (ESIG)</td>
<td>169</td>
<td>H</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Finance</td>
<td>Disease Management System (DMS)</td>
<td>Change Control Document Repository</td>
<td>167</td>
<td>H</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fifteen risk factors are considered

**Primary Factors**
- Development of the Application
- Program Change
- Pervasiveness
- Application Complexity
- Interfaces With Other Applications
- IT Hosting Environment
- Proximity to Financial Management
- Proximity to Patient Care
- Compliance Requirements

**Secondary Factors**
- Access by External Entity
- Maturity of Application
- Internal Audit History
- Results of Prior Internal Audits
- Other Considerations
- Management of Application
IT Capabilities Workbook

✓ Allows for assessment of IT capabilities of Central IS and individual Departmental IT organizations.

✓ IT Capabilities measured across six domains.

✓ Assessment used to evaluate Central IS against global benchmarking data.

✓ Allows Central IS to evaluate individual department’s IT Capabilities.
IT Capabilities Workbook

- Management of IT
- Physical and Environmental Control
- Information Security
- Continuity of Systems
- Change Management
- Systems Development

See handout for additional details on definitions of IT Capabilities.
## IT Capabilities Workbook

### Managing Security and Privacy in an Environment of Increased Risk and Threats

<table>
<thead>
<tr>
<th>Category</th>
<th>Topic</th>
<th>Epidemiology and Biostatistics</th>
<th>RTM</th>
<th>Radiation Oncology</th>
<th>Radiology</th>
<th>Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Score</td>
<td></td>
<td>Score</td>
<td>Score</td>
<td>Score</td>
</tr>
<tr>
<td></td>
<td>Board/Senior Management</td>
<td>3.0</td>
<td>2.0</td>
<td>3.0</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td></td>
<td>Involvement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT Planning</td>
<td>2.0</td>
<td>3.0</td>
<td>3.0</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>Cost Management</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>3.0</td>
</tr>
<tr>
<td></td>
<td>Management Reporting</td>
<td>3.0</td>
<td></td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Management of IT</td>
<td>Service Level Management</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>Legal compliance</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>4.0</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>Organization of IT</td>
<td>3.0</td>
<td>3.0</td>
<td>2.0</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Physical and Environment</td>
<td>End User Computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. No effective controls. Unauthorized personnel can readily gain access to equipment.
2. Access restricted to authorized staff, although no formal method of restricting access (e.g., no security force or mechanical access control devices).
3. Access restricted to authorized staff at authorized times. Formal access control (security force/mechanical access control devices) are used.
4. Access breaches monitored and reviewed.
5. Security breaches reviewed and followed up. Proactive action taken to ensure that breaches do not reoccur—e.g., redesign of security devices, review of procedures.
Mapping IT Capabilities Against Prescribed Policies and Procedures

Global Benchmark Data Provided by KPMG represented on a spider diagram

Benchmarked Global Ratings ~ 60 similar sized healthcare organizations (hospitals)

- **1st quartile** – IT Capability results from organizations with the top 25% of all scores
- **2nd quartile** – Results from organizations between the top 25% and the top 50% of all scores
- **3rd quartile** – Results from organizations between the bottom 50% and the bottom 25% of all scores
- **4th quartile** – Results from organizations in the bottom 25% of all scores
Monitoring Access to PHI

HIPAA Privacy & Security Rule Key Requirements

Appropriate safeguards for PHI
Access control & Minimum Necessary
  • Job-related need standard
Adequate audit trail (what, who, when) & “regular” review
  • Sanctions
  • Regulations not prescriptive on frequency or methodology

Patient Requests/Concerns

Ability to investigate & respond

Other Key Stakeholders:

Insurance Carriers, Board, Joint Commission
Expect appropriate controls, investigative tool, deterrence
Compliance Working with IS – Monitoring Access to PHI

**Goals:**
- Validate pattern of job-related access
- Identify & deter instances of unauthorized access

**Tools & Approaches:**
- Fair Warning application; internally-developed IS applications
- Routine
  - Random reviews
  - Monitored records
- For-Cause
  - Patient requests
  - Investigations
Compliance Working with IS – Monitoring Access to PHI (Sample FW Audit Trail)

<table>
<thead>
<tr>
<th>Event Timestamp</th>
<th>Audit Source</th>
<th>User ID</th>
<th>User Name</th>
<th>User Title</th>
<th>User Department</th>
<th>Activity Description/Event Name/Document Description</th>
<th>Patient Name</th>
<th>Patient MRN</th>
<th>User Manager</th>
<th>Workstation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-08-31 08:40:39.0</td>
<td>STREAMLINE EMR</td>
<td>00001</td>
<td>Employee B</td>
<td>Clinical Nurse II</td>
<td>Nursing</td>
<td>Access/View Document: Amb Nsg Adult Health Screening</td>
<td>Jane Doe</td>
<td>000000000</td>
<td>Manager B</td>
<td>WM531117</td>
</tr>
<tr>
<td>2015-08-31 13:12:21.0</td>
<td>UMP_ALLSCRIPTS</td>
<td>00002</td>
<td>Employee C</td>
<td>Clinical Nurse IV</td>
<td>GI Chemo</td>
<td>Print document</td>
<td>Jane Doe</td>
<td>000000000</td>
<td>Manager C</td>
<td>WM531113</td>
</tr>
<tr>
<td>2015-09-02 13:57:35.0</td>
<td>EPIC</td>
<td>00003</td>
<td>Employee D</td>
<td>Session Asst II</td>
<td>GI Medicine</td>
<td>Appointment desk accessed for patient (individually or in a group); Patient Demographics</td>
<td>Jane Doe</td>
<td>000000000</td>
<td>Manager D</td>
<td>WM531114</td>
</tr>
<tr>
<td>2015-08-31 18:05:21.0</td>
<td>GEIDX</td>
<td>00004</td>
<td>Employee E</td>
<td>Revenue Operations Associate</td>
<td>Charge Entry/PBD Operations</td>
<td>Batch Action: Enter Charges</td>
<td>Jane Doe</td>
<td>000000000</td>
<td>Manager E</td>
<td>WM531112</td>
</tr>
<tr>
<td>2015-09-01 08:04:48.0</td>
<td>SIEMENS_INVISION</td>
<td>00005</td>
<td>Employee F</td>
<td>Cancer Registrar II</td>
<td>Disease Management</td>
<td>Access Patient</td>
<td>Jane Doe</td>
<td>000000000</td>
<td>Manager F</td>
<td>WM531115</td>
</tr>
</tbody>
</table>
Data Loss Prevention (DLP)

Exact data match (EDM) on institutional database

Application scans outbound email/web/FTP

Privacy & IS set thresholds and rules to block/ auto-secure/quarantine

Triggers incident notifications to users, supervisors, Privacy & IS

Follow-up action
  • Privacy/IS review with user
  • Mitigation as needed
Data Loss Prevention (cont.)

Managing Security and Privacy in an Environment of Increased Risk and Threats
Synergy: Audit & Information Security

**Synergy**

The interaction or cooperation of two or more organizations, substances, or other agents to produce a combined effect greater than the sum of their separate effects.
Internal Audit is proactive

Internal audits of information systems or security processes and procedures involve a set of periodic, proactive compliance and assurance reviews that help in assessing information security control posture in an organization which helps accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Identifying the gaps (proactive) requires working with the subject matter experts to identify appropriate controls to mitigate those gaps.
Lessons Learned

Wisdom is the lesson learned, applied.

~RICK BENETEAU~
Resources and References

Information Systems Audit and Control Association

Association of Healthcare Internal Auditors

The Institute of Internal Auditors

System Administration, Networking, & Security Institute
Resources and References

National Institute of Standards and Technology

Office for Civil Rights

The Office of the National Coordinator for Health Information Technology

Association for Executives in Healthcare Information Security
Continued widespread adoption of Health IT

**Mission:** Improve health, healthcare, and reduce costs through the use of information and technology

Plan and updates required by HITECH regulations (2009)

Goals (5), Objectives (14) and strategies (73)
Ponemon Surveys

2015 Global Study on IT Security Spending & Investments

Independently conducted by Ponemon Institute LLC

Publication Date: May 2015
Managing Security and Privacy in an Environment of Increased Risk and Threats
Information Security Governance

- Introduction to Privacy and Information Security
- Evolution of Programs: From Regulation to Culture
- Risk Analysis and Risk Management
- A Paradigm: Privacy, Security, Quality, Safety
- Governance
- Evaluating…
- The Future…
Contact Information

Phyllis A. Patrick
Founder & President
Phyllis A. Patrick & Associates LLC
Phyllis@phyllispattern.com
914-417-8592
www.phyllispattern.com

Managing Security and Privacy in an Environment of Increased Risk and Threats
Contact Information

Alan Moorhead
Vice President, Audit Services
Email: amoorhead@Hanger.com
Telephone: 563-299-4475

Alan Mitchell
Hanger, Chief Information Security Officer
Email: AMitchell@Hanger.com
Telephone: 512-777-3614
Contact Information

Ed Taliaferro
Vice President,
Internal Audit & Compliance,
Chief Compliance Officer
Email: TaliafeE@mskcc.org
Telephone: 646-227-2955 (O)
646-204-1894 (M)

Patricia Skarulis
Senior Vice President,
Information Systems &
Chief Information Officer
Email: pskarulis@mskcc.org
Telephone: 646-227-3315 (O)
917-587-0330 (M)