Information Security in 2016: What Will Your Program Look Like?

Phyllis A. Patrick, MBA, FACHE, CHC

The Twenty First National HIPAA Summit

February 20, 2013

Topics

- Trends Affecting Information Security Programs – What are the Key Themes?
- Re-defining the Role of the Information Security Professional – What skills will be needed?
- Organizational Models – What are some options for your organization?

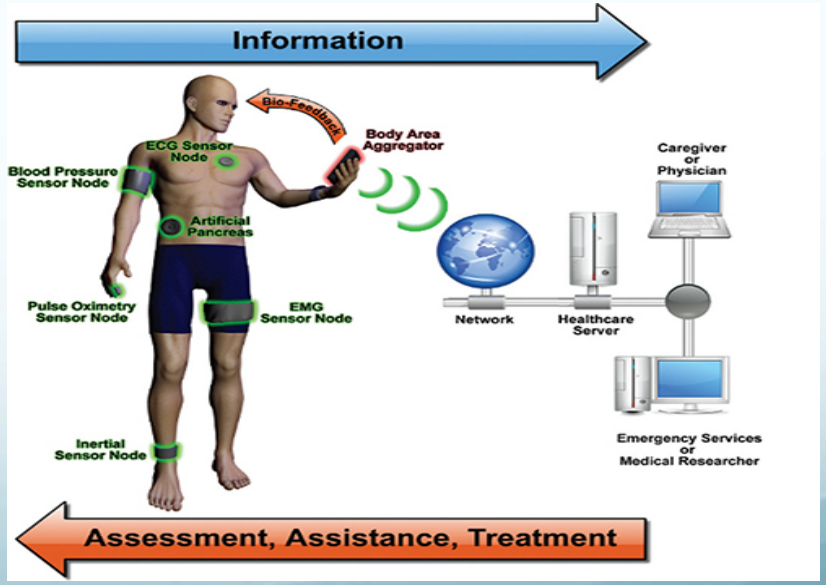
2016 and Beyond…

Trends Affecting Security Programs

- Explosion of data → Criticality of Information Assets
- New and expanded organizational models with large appetite for data (e.g., ACO, HIE, Research Communities)
- Mobility and Mobile Computing
- Social Media

Trends and Key Themes (cont'd)

- Consumer Expectations
- Regulation and Compliance
- New and Emerging Technologies
- Cloud Computing



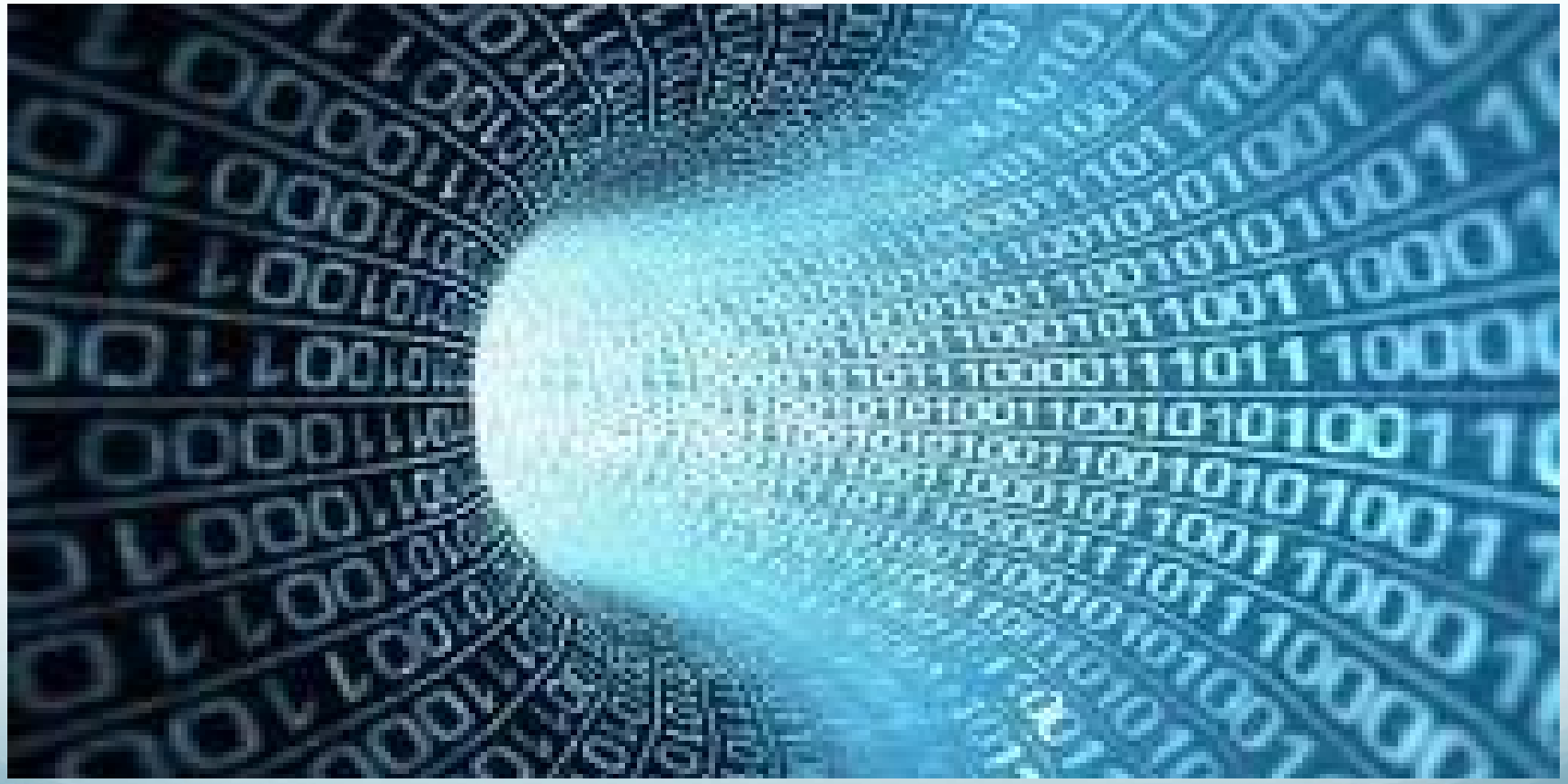
Trends and Key Themes (cont'd)

- Outsourced and Managed Security Services/ Components
- Cyber Crime and Cyber Security
- Globalization - Impact on Privacy and Security
- Governance - Changes in Board and Senior Leader Interest and Responsibility

Explosion of Data

- Rapid accumulation of digital data
- Data banks include individual behavior and personal preferences
- Government data collection efforts and activities
  - Agencies and Departments: IRS, US Census, Dept. of Homeland Security, VA + many more
  - Laws: eGovernment Act, US Patriot Act
  - Global activities and collaborations – EU Third Pillar (counterterrorism)
  - Surveillance – cameras, devices, GPS, monitoring devices
- Combining of data bases, e.g., governmental & commercial

More types of data collected from more people in more ways, and shared with more entities.



New & Evolving Organizations with Appetite for Data

- Accountable Care Organizations
- Insurance Exchanges
- Health Information Exchanges (HIEs)
- National Health Information Exchange Network (NwHIN)

"Health information will follow the patient and be available for clinical decision making as well as for uses beyond direct patient care, such as measuring quality of care." (ONC)

Mobility and Mobile Computing

- Proliferation of devices is staggering and growing
- Mobile device management and security rank #1 or #2 concern by information security professionals in most surveys
- BYOD Phenomenon
- Mobile Device Protection Methods
  - Policy
  - Technology (encryption, network access control (NAC), mobile VPNs, remote lock-&-wipe functionality, mobile anti-malware, digital rights management (DRM))

BYOD Policy – How's that working for you?

Consider costs of BYOD

Social Media

- Recognized as a business tool, not just a personal tool
- Need/benefit of connecting with “customers”
- Security and IT often not involved – Marketing/PR take the ball and run with it
- Access to SM and Controls are key. No access vs. total access --- not an “either or”solution
- Protection Methods:
  - Policy
  - Technology (e.g., content filtering, web site blocking)

Consumer Expectations

- Engaging consumers is integral to ONC's strategy
  - Protecting Privacy and Security
  - Patient Safety
  - Promoting Exchange of health information
  - Engaging Consumers
  - Demonstrating Outcomes
- Meaningful Use and acceleration of EHR adoption
- Promotion of standards and interoperability, HIEs → NwHIN
- Innovation funding (Beacon, Sharp, e-Consenting)
- Assistance to providers to increase/enhance adoption (REC, Workforce training grants)

Consumer Expectations (cont'd)

- 80 percent of internet users seek health information online
- Social media used to find, evaluate, compare providers
- Consumers want VALUE and TRANSPARENCY
- Concern for privacy of medical information

- Policy changes → changing payment systems → incentives to stay healthy and greater consumer financial responsibility → informed health care shopper/negotiator
- Next generation of PHRs – Blue Button + Technology

Regulation & Compliance

- Omnibus Rules
- OCR, ONC and other mandates for auditing and compliance
- New privacy laws possible, e.g., employee privacy, video monitoring, smart devices (sensors, RFID)
- Compliance-driven information security requirements
- Global laws and trends, e.g.,
  - EU Data Protection Directive
  - Canada – from voluntary to required data breach notification
- Convergence of privacy regs, i.e., key principles across more economic sectors and technology-neutral approach

New & Emerging Technologies

New & Emerging Technologies

- Biometrics
- Radio-frequency identification (RFID)
- Building/home security and surveillance systems
- mHealth
  - Practice of medicine and public health, supported by mobile devices
  - Use of information and communication technology to provide health services and information to practitioners, researchers, and patients
  - Telemedicine
  - What is a “medical device”?

Cloud Computing

- Enabler for powerful, flexible and scalable computing power
- How to protect security of data once it leaves the host organization
- Concerns: security, service disruption, lack of forensics, TRUST
- Need for more training on cloud computing
- Need for clear, strong contracts and business partnerships
- Cloud Computing Providers as Business Associates – who owns the data? How to resolve disputes? What is fair compensation for downtime?

Outsourcing Security Services

- Info Sec is difficult to outsource
- Need to define the function, including how information is created, recorded, manipulate, stored, disposed
- Need to clearly define scope of services required/desired and how security controls will be achieved
- Need to clearly define expected deliverables
- Decisions re. what to outsource – Info Sec is a PROGRAM, with many component parts

Outsourcing Security Services (cont'd)

- Info sec components that may be more conducive to outsourcing include:
  - Forensics
  - Business Continuity Planning
  - Disaster Recovery
  - Network Monitoring (e.g., DPS)
  - Security Operations
  - Penetration Testing
- Business Associate and sub-contractor relationships

Outsourcing Security Services (cont'd)

- Outsourcing security components may be a viable alternative for some organizations, but requires:
  - Performing due diligence
  - Managing the risks
  - Requiring, implementing, and maintaining Assurance Controls
  - Mitigating problems and issues
  - Re-evaluating and re-negotiating key contract terms
- Consider legal obligations, cost/benefit analysis, risk analysis, ethical obligations
- Information Security remains the organization's responsibility!

Cyber Crime & Cyber Security

- Cost of global consumer cyber crime is calculated to be $110 billion a year (Norton Cyber Crime Report, 2012)
- **ONC's Cybersecurity Checklist** (strong passwords, anti-virus **software, firewalls, access control, physical access control, network access limitations, good practices, etc.)**
- **Emphasis needs to be on DYNAMIC MONITORING** and Prevention Detection, not after the fact
- Digital identification of all parties who enter and leave network
- FTC – OnGuard Online Blog

Globalization

- Key trends and themes are global concerns, extending to all regions (e.g., mobile computing, social media, cloud computing)
- Research and collaborations span all regions
- Proliferation and use of data, concern for privacy and security are global issues
- Some regions ahead of U.S. on global issues, e.g.,
  - EU Privacy Laws and Data Directive
  - Canada – industry involvement in key laws
  - Asia/Pacific – spend more $ on security (personnel, hardware & software, professional services, outsourced and managed services)

Governance

- Board member interest focus on IT, not necessarily Information Security → IT = Info Sec
- PwC Study: 67% of trustees agree that their company's approach to managing IT risk and strategy provides the board with only "moderate" information to be effective, or the information "needs improvement." 40% saw IT as "somewhat important" or "more of a commodity."
- Approximately 1% of directors have some technology background (The Board Institute)

Governance (cont'd)

- Audit Committee is generally the focus. Few Boards have IT/Technology Committee. Fewer have Info Sec Committee.
- View of Audit Committee is "risk-averse", less emphasis on innovation or proactive outlook, required for effective Information Security governance.
- "Board members don't know what they don't know."
- CIO can be a champion for information security and educate/inform Board of risks, requirements, security as culture.
- "Protecting patients through good data security practice should be as second nature to health care practice as disinfection is." (ONC)

Your Information Security Program in 2016

The Info Sec Professional – New Skills Needed

- Strategic Planning
- Enhanced Technical Knowledge
- Contract Negotiation
- Budgeting
- Understanding of Cloud Computing and Software Development
- Facilitation skills and influencing capabilities
- Access to Legal Counsel
- Operations/business background a plus

Increase in Numbers of Professionals

- Estimates of Security Professionals, Worldwide:
  - 2010 -- 2.28 million
  - 2015 -- 4.2 million

  (*Source: Frost & Sullivan, Global Information Security Workforce Study*)
- Certifications considered valuable

The Paradigm Shift

From **Regulatory Compliance →**

Information Risk Management →

Information Governance →

Information Protection & Optimization

Security Models

- Information Security will become an integral organizational Program, with budget lines, plans, department goals, performance improvement plans.
- Privacy and Information Security will be more integrated.
- The role of the CISO/ISO will be re-defined in terms of information risk, policy, and strategy.
- The CISO/ISO reporting relationship will vary based on skill sets and organizational strengths. The CISO/ISO will not report to IT (conflict of interest potential) but could report to Risk, Legal, COO, or others.

Security Models (cont'd)

- Program foundation/security framework/model will extend beyond HIPAA/HITECH requirements → ISO standards, COBIT 5, etc.
- Metrics development and reporting will be key to program integrity and evaluation.
- Board members will receive regular reports and information regarding the Privacy and Information Security Programs.

Security Models (cont'd)

- Information Security and Privacy may join to become INFORMATION GOVERNANCE and/or INFORMATION RISK MANAGEMENT, with seat at the Executive table.
- Privacy and Information Security goals will be incorporated into the organization's strategic planning.
- Privacy and Information Security will be more integrated into the culture of the organization and not viewed as regulatory functions.

PHYLLIS PATRICK + Associates

Security | Privacy | Culture

phyllis@phyllispatrick.com
914-696-3622