



The leading health information and technology conference

WHERE **THE WORLD** CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

The Cybersecurity Risk Management Framework Applied to Enterprise Risk Management

Session 43, March 6, 2018

Barry S. Herrin, JD, FAHIMA, FACHE

Founder, Herrin Health Law, PC

ENGAGED

www.himssconference.org



#HIMSS18

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.



Conflict of Interest

Barry Herrin, JD has no real or apparent conflicts of interest to report.

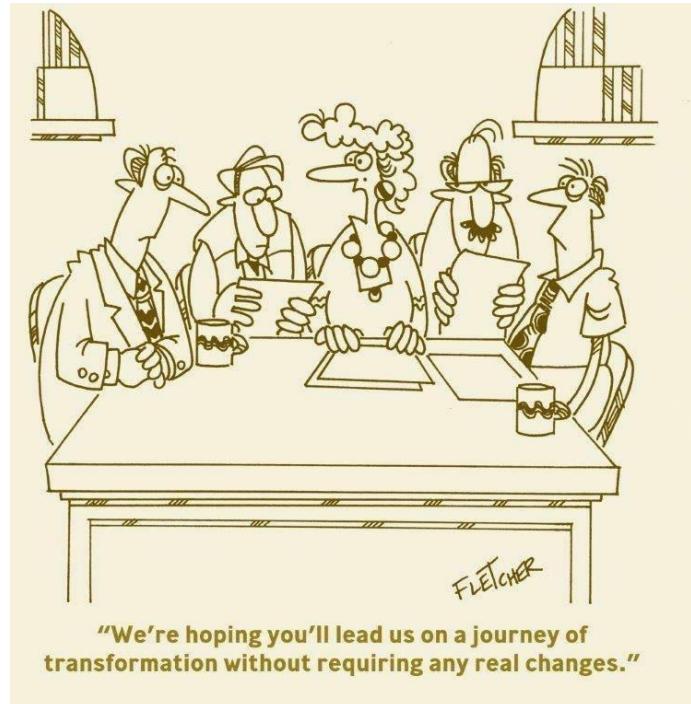
Agenda

- The Health Care Industry Cybersecurity Task Force Final Report
- NIST SP 800-39
- An Overview of the Cybersecurity Risk Management Framework
- NIST SP 800-53 Control Families
- Review of Certain Security Controls – Focus on People, Process, and Technology
- Focus on Privacy Controls
- Key Takeaways

Learning Objectives

- Show how to use a typical cybersecurity risk analysis to address privacy and other healthcare risks in the enterprise
- Describe the re-focus on people and processes to address cybersecurity risks within the healthcare enterprise typically dealt with by technology spending
- Apply how to re-orient thinking about healthcare enterprise risk management using the NIST Cybersecurity Framework

HOW CHANGE MANAGEMENT FEELS TO THE CHANGE ADVOCATE...



The Health Care Industry Cybersecurity (HCIC) Task Force Final Report June 2, 2017

- Of the three aims of cybersecurity (confidentiality, integrity, availability), **availability** is the most important. You cannot take care of patients without having availability of information. Having high availability of patient information is especially important with hospitals that operate 24x7 and 365 days a year.
- **Integrity** of data is important for protecting patient safety. Patient safety is also directly implicated when it comes to connected medical devices and patients whose health can be directly impacted by the operation of the medical device.

The Health Care Industry Cybersecurity (HCIC) Task Force Final Report June 2, 2017

- As the healthcare industry progresses towards more interoperability, healthcare data **confidentiality** must remain top of mind.
- The biggest barrier to cybersecurity program maturity in healthcare is the cultural barrier. **The cybersecurity threat is not understood and/or there are not enough resources available by some organizations to deal with the threat—especially small and rural healthcare providers.**

The Health Care Industry Cybersecurity (HCIC) Task Force Final Report June 2, 2017

- **Task Force Imperative No. 4:** Increase healthcare industry readiness through improved cybersecurity awareness and education
- “Cybersecurity can be an enabler for the healthcare industry, supporting both its business and clinical objectives, as well as facilitating the delivery of efficient, high-quality patient care.
However, this requires a holistic cybersecurity strategy.
Organizations that do not adopt a holistic strategy not only put their data, organizations, and reputation at risk, but also—most importantly—the welfare and safety of their patients.”

NIST SP 800-39: Managing Information Security Risk - Organization, Mission, and Information System View

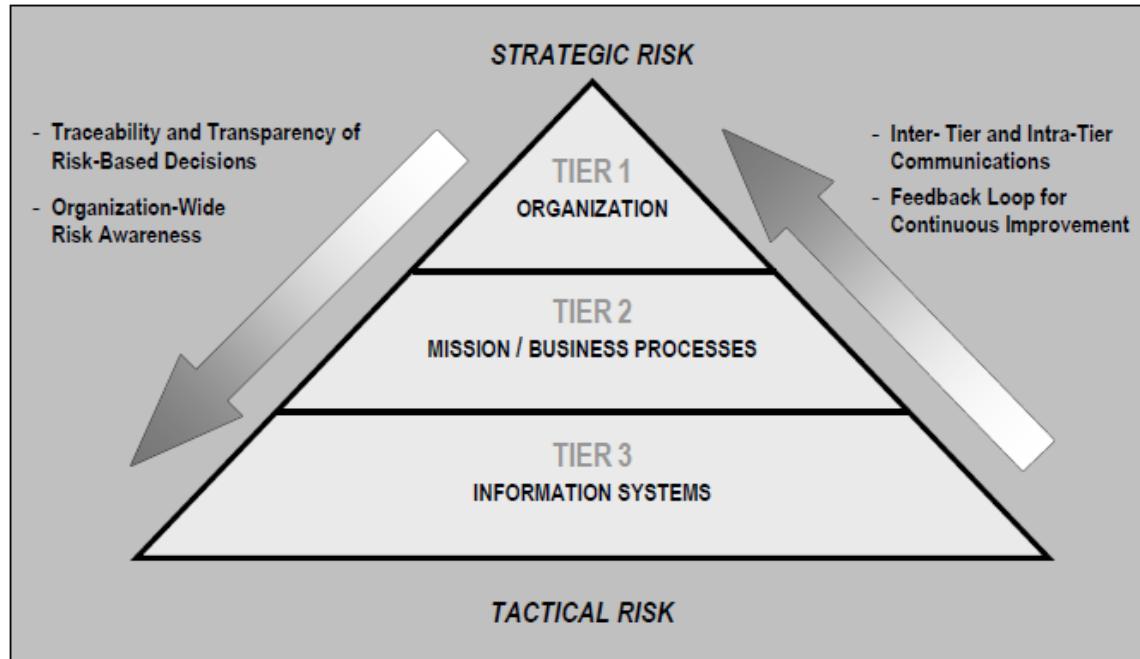
- Organizational risk can include many types of risk (e.g., program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk). ***Security risk related to the operation and use of information systems is just one of many components of organizational risk that senior leaders/executives address as part of their ongoing risk management responsibilities.*** Leaders must recognize that explicit, well-informed risk-based decisions are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure. ***Managing information security risk, like risk management in general, is not an exact science. It brings together the best collective judgments of individuals and groups within organizations responsible for strategic planning, oversight, management, and day-to-day operations—providing both the necessary and sufficient risk response measures to adequately protect the missions and business functions of those organizations.***

NIST SP 800-39

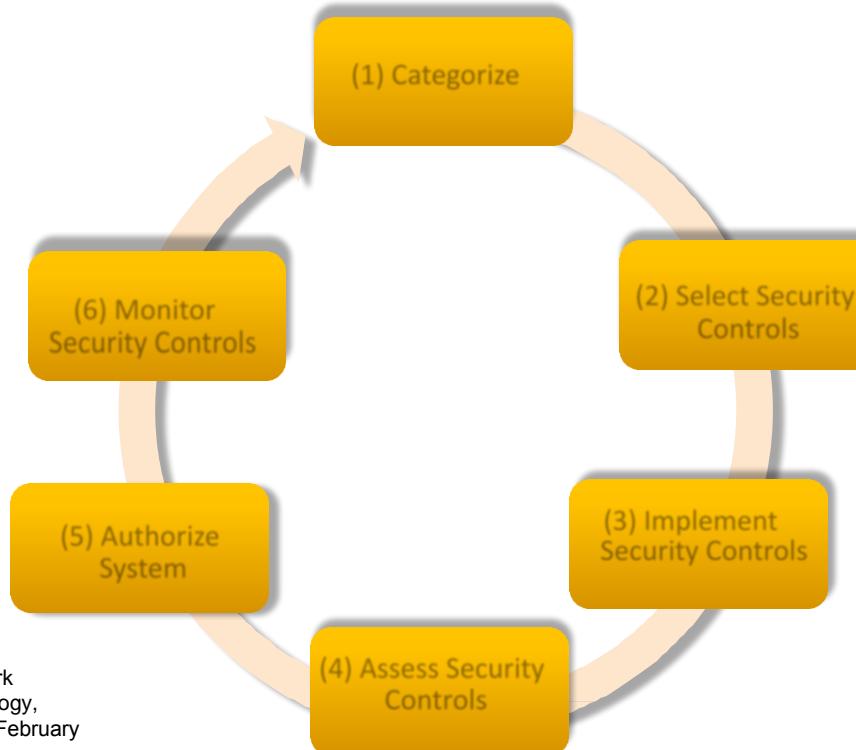
- Objectives:
 - Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate governance structures for managing such risk;
 - Ensure that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;
 - ***Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and***
 - ***Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.***

ENTERPRISE RISK MANAGEMENT TIERS

(from NIST SP 800-39)



CYBERSECURITY RISK MANAGEMENT FRAMEWORK



NIST Cybersecurity Risk Management Framework
Diagram courtesy of Georgia Institute of Technology,
"Cyber Risk Management for Decision-Makers", February
2017, Module 2.1, p. 161

TASK 1-CATEGORIZE SYSTEM

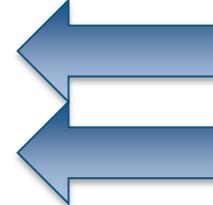
- Categorize the system based on impact analysis
 - Confidentiality, Integrity, AND Availability
- Security controls are the management, operational, and technical safeguards or countermeasures employed within an information system.
 - People, Processes, AND Technology
 - Incident Response Plan, Vulnerability Assessments, Anti-virus Software, User Training, Firewalls, Etc.

TASK 2 - SELECT SECURITY CONTROLS

- Select the initial set of security controls
- Select and apply security control overlays
- Tailor the set of security controls
- Supplement the tailored set of controls
- Identify common controls
- Document the security control baseline

TASK 3-IMPLEMENT SECURITY CONTROLS

- Design
- Purchase
- Install
- Configure
- Test



- This is where most IT folks forget about the people and processes and instead focus SOLELY on the technology
- If you change “Purchase and Install” to “Implement”...

NIST SP 800-53 Revision 5 – We're Ahead of Our Time (?)

- Making the security and privacy controls more outcome-based by changing the structure of the controls
- Fully integrating the privacy controls into the security control catalog creating a consolidated and unified set of controls for systems and organizations (***currently 2 separate appendices***)
- Separating the control selection process from the actual controls, thus allowing the controls to be used by different communities of interest including systems engineers, software developers, enterprise architects; and mission/business owners
- Eliminating the term “information system” and replacing it with the term “system” so the controls can be applied to any type of system including, for example, general purpose systems, cyber-physical systems, industrial/process control systems, and IoT devices

NIST SP 800-53 Revision 5—More Changes

- De-emphasizing the federal focus of the publication to encourage greater use by nonfederal organizations
- ***Promoting integration with different risk management and cybersecurity approaches and lexicons, including the Cybersecurity Framework***
- Clarifying the relationship between security and privacy to improve the selection of controls necessary to address the full scope of security and privacy risks
- Incorporating new, state of the practice controls based on threat intelligence and empirical attack data, including controls to strengthen cybersecurity and privacy governance and accountability

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

CONTROL FAMILIES

- AC Access Control
- AT Awareness & Training
- AU Audit & Accountability
- CA Security Assessment & Authorization
- CM Configuration Management
- CP Contingency Planning
- IA Identification & Authentication
- IR Incident Response
- MA Maintenance
- MP Media Protection
- PS Personnel Security
- PE Physical & Environmental Protection
- PL Planning
- PM Program Management
- RA Risk Assessment
- SC System & Communications Protection
- SI Systems & Information Integrity
- SA Systems & Services Acquisition
- **Authority and Purpose (AP)**
- **Accountability, Audit, and Risk Management (AR)**
- **Data Quality and Integrity (DI)**
- **Data Minimization and Retention (DM)**
- **Individual Participation and Redress (IP)**
- **Security (SE)**
- **Transparency (TR)**
- **Use Limitation (UL)**
- *Bold family members are PRIVACY additions to rev. 4 of NIST SP 800-53*

ACCESS CONTROL

- Usually considered a “technical” control
- Focus on user access and account management
 - Assign risk categories based on job description
 - Rescreen users when changing job descriptions/level of responsibility
- Liken it to “key control” of a physical plant
 - Not everybody needs a master key
 - Policies can prevent universal access
 - Technology REINFORCES policies

Access Control - Examples

- AC-2j – *The organization reviews accounts for compliance with account management requirements (set frequency)*
- AC-2k – *The organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group (can be automatic within the system)*
- AC-6(1) – *The organization explicitly authorizes access to defined systems (no default access)*
- AC-6(3) – *The organization documents the rationale for access across a network in the security plan for the ~~information system~~ enterprise*

AUDIT & ACCOUNTABILITY

- Also usually considered a “technical” control
- “You only get what you measure”
- Understanding the regulatory environment in which your systems operate is critical
- Healthcare systems must operate within HIPAA, HITECH, FDA, CMS “meaningful use”, and other parameters – not all of which are technical

Audit & Accountability - Examples

- AU-2(b) – *The organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.*
- AU-6a(3) – *The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. (Also AU-16 – Cross-Organizational Auditing)*
- AU-6a(6) – *The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity*
- AU-13 – *The organization monitors open source information and open source information sites for evidence of unauthorized disclosure of organizational information (more than a sophisticated RSS feed; includes social media sites)*

AWARENESS & TRAINING

- Clearly an “operational” control
- Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior
 - Easier to keep out than to kick out
 - Don’t just shuffle the bad apple into a new barrel
- Train employees on expected behavior
- Train supervisors to respond to employee behavior outside of accepted norms
 - Investigate uniformly
 - Discipline uniformly
- Train employees on reporting inappropriate behavior

Awareness & Training - Examples

- AT-2 – *The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) ... when required by information system changes. (Guidance: The content also addresses awareness of the need for operational security AND recognizing and reporting indicators of insider threat)*
- AT-3 – *The organization provides role-based security training to personnel with assigned security roles and responsibilities. (Guidance: including the employment and operation of physical security controls)*
- ***Do you think this might help with identifying rogue actors who might become insider threats?***

IDENTIFICATION & AUTHENTICATION

- Also viewed as a “technical” control
- Do you verify people’s resumes, references, training, certifications?
- Do you do criminal and permissible credit background checks?
- Do you re-screen upon promotion or lateral movement?
- Are persons with access to financial access bonded?
 - Permits higher level financial security checks

Identification & Authentication - Examples

- IA-4a – *The organization manages information system identifiers by receiving authorizations to assign an individual, group, role, or device identifier from specified individuals (Guidance: authorization requires multiple forms of personal identification to prevent fraud and an initial in-person request)*

INCIDENT RESPONSE

- Now more important than ever due to changes in CMS policy effective November 2016 participating providers to plan for natural and man-made disasters, train for disaster preparedness, and test emergency plans.
- March 24, 2017 memo clarified that participating providers are expected to meet the requirements of the final rule by November 15, 2017, or face citations for non-compliance.
- Participating providers are to “seek out and participate in a full-scale, community-based exercise with their local and/or state emergency agencies and health care coalitions and to have completed a tabletop exercise by [November, 2017].”
- ***Clearly, then, the IR criteria cannot be focused simply on information system security***

Incident Response - Examples

- *IR-4b – The organization coordinates incident handling activities with contingency planning activities (Guidance: “Organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems.”)*
- *IR-8a – The organization develops an incident response plan that provides a high-level approach for how the incident response capability fits into the overall organization*
- *IR-8a7 – The organization defines the resources and management support needed to effectively maintain and mature an incident response capability*

NEW PRIVACY FAMILY CONTROLS – APPENDIX J TO NIST SP 800-53 rev4

- Organizations analyze and apply each privacy control with respect to their distinct mission/business and operational needs based on their legal authorities and obligations. Implementation of the privacy controls may vary based upon this analysis (e.g., organizations that are defined as covered entities pursuant to the Health Insurance Portability and Accountability Act [HIPAA] may have additional requirements that are not specifically enumerated in this publication). This enables organizations to determine the information practices that are compliant with law and policy and those that may need review. It also enables organizations to tailor the privacy controls to meet their defined and specific needs at the organization level, mission/business process level, and information system level.
- At the discretion of the implementing organization, **privacy controls may be documented in a distinct privacy plan or incorporated into other risk management documents (e.g., system security plans).**

NEW PRIVACY FAMILY CONTROLS – APPENDIX J TO NIST SP 800-53 rev4

- Organizational assessments of privacy controls can be conducted either by the [privacy official] alone or jointly with the other organizational risk management offices including the information security office.
- Specific overlays for privacy can also be considered to facilitate the tailoring of the security control baselines with the requisite privacy controls to ensure that both security and privacy requirements can be satisfied by organizations. ***Many of the security controls provide the fundamental information protection for confidentiality, integrity, and availability within organizational information systems and the environments in which those systems operate—protection that is essential for strong and effective privacy.***

NEW PRIVACY FAMILY CONTROLS – APPENDIX J TO NIST SP 800-53 rev4

- **Accountability, Audit, and Risk Management**
- AR-2 – The organization (a) documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and (b) conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.
 - Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII.
 - PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.

NEW PRIVACY FAMILY CONTROLS – APPENDIX J TO NIST SP 800-53 rev4

- Accountability, Audit, and Risk Management
 - AR-4 - The organization monitors and audits privacy controls and internal privacy policy [on an organization-defined frequency] to ensure effective implementation.
 - Regular internal risk assessments should address gaps in technical controls.
 - Reports should describe compliance gaps identified in programs, projects, and information systems.
 - Organizations should assess whether they embed privacy considerations into the life cycle of information systems, mission/business processes, and technology

NEW PRIVACY FAMILY CONTROLS – APPENDIX J TO NIST SP 800-53 rev4

- Accountability, Audit, and Risk Management
 - AR-7 - The organization designs information systems to support privacy by automating privacy controls.
 - To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents.

NEW PRIVACY FAMILY CONTROLS – APPENDIX J TO NIST SP 800-53 rev4

- **Data Quality and Integrity**

- DI-1a. – The organization confirms to the greatest extent practicable upon collection or creation of PII the accuracy, relevance, timeliness, and completeness of that information
- DI-1c. – The organization checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems
 - ***Guidance – each time data is collected the individual is asked to revalidate the information***

NEW PRIVACY FAMILY CONTROLS – APPENDIX J TO NIST SP 800-53 rev4

- **Data Minimization and Retention**

- DM-1a. and b. – The organization identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection and limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent
- THIS ALIGNS WITH THE GLOBAL DATA PRIVACY RULE AND HIPAA'S "MINIMUM NECESSARY" REQUIREMENT

NEW PRIVACY FAMILY CONTROLS – APPENDIX J TO NIST SP 800-53 rev4

- **Individual Participation and Redress**

- IP-1 – The organization:
 - a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;
 - b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
 - c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
 - d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

KEY TAKEAWAYS

- Don't assume that you need more budget to execute on security goals
- Remember PEOPLE, PROCESSES, AND TECHNOLOGY can be used to mitigate risk
- IT can be a thought leader in enterprise risk management if you use the RMF as your common toolkit
- In the rush to embrace availability and integrity, don't leave privacy and confidentiality behind
- You can't have true privacy without security and *vice versa*

Questions?

BARRY S. HERRIN, JD, FAHIMA, FACHE

404-459-2526

barry.herrin@herrinhealthlaw.com

www.herrinhealthlaw.com

PLEASE COMPLETE THE ONLINE SESSION EVALUATION