Top IT and Cyber Risks to Include in Your Audit Plan

HCCA – Compliance Institute
April 15, 2018

Johan Lidros CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, ITIL-F
President Eminere Group

Presenter

- Johan Lidros, Founder and President of Eminere Group
- Has provided information technology governance and information security services in the healthcare industry for 20 years in Europe and in the United States
- Well-versed in accepted IT and information security standards/frameworks (ISO27000, HITRUST, NIST, COBIT, CIS, etc.) and has participated in several related committees
- Certifications: CISA, CISM, CGEIT, ITIL-F, CRISC, HITRUST CCSFP

eminere group

HCCA Health Care Compliance Association

Table of Contents

- ❑ **Introduction**
- ❑ **Key IT and Cyber Risks and Opportunities**
- ❑ **What Risks to Audit?**
- ❑ **Board and Management Communication**
- ❑ **Trending Best Practice/Standards and Resources**
- ❑ **Conclusion**
- ❑ **Q&A**

Objectives

- ❑ What are the key IT and Cyber risks you need to be aware of?
- ❑ What IT and Cyber risks do you need to audit?
- ❑ What evolving IT and Cyber risks do you need to discuss with management?
- ❑ What IT and Cyber risk training do you need to provide to the audit committee/board?
- ❑ What are the most common hidden IT and Cyber opportunities?
- ❑ What are the most trending best IT governance/security, best practices and standards?
- ❑ Your Questions!!!

Auditing and IT Risk, Governance, etc

- ❑ **IIA 2120 - Risk Management**
  The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.
  - *Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:*
    - *Organizational objectives support and align with the organization's mission;*
    - *<u>Significant risks are identified and assessed;</u>*
    - *<u>Appropriate risk responses are selected that align risks with the organization's risk appetite;</u> and*
    - *<u>Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.</u>*

Table of Contents

- □ Introduction
- □ Key IT and Cyber Risks and Opportunities
- □ What Risks to Audit?
- □ Board and Management Communication
- □ Trending Best Practice/Standards and Resources
- □ Conclusion
- □ Q&A

IT Risks

The use and deployment of information technology (IT) is a critical success factor for most organizations. Designing, implementing, operating, maintaining and monitoring an efficient and effective IT solution is a difficult task. The speed of change, complexity and new requirements in the technology arena impact the risk environment:

- ❑ **Patient safety**
- ❑ **Patient satisfaction**
- ❑ **Costs**
- ❑ **Security and privacy**
- ❑ **Regulatory compliance**
- ❑ **Operational efficiency**

IT and Cyber Security Definitions

Information Security

- ❑ Protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide CIA:
  - **Confidentiality:** preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
  - **Integrity:** guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
  - **Availability:** ensuring timely and reliable access to and use of information.
- ❑ Information Security is concerned with information and the protection of information whether be it physical or computerized.

IT and Cyber Security Definitions

Cyber Security

❑ Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies
that can be used to protect the “cyber” environment and organization and user’s assets

[ITU-T X.1205].

❑ Cyberspace” is defined as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.

ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity

❑ *IT Security*

❑ *Protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security [The Free Dictionary].*

Health IT - Definition

- ❑ **The term "health information technology" (health IT) is a broad concept that encompasses an array of technologies to store, share, and analyze health information.**

  - Definition (Office for the National Coordinator of Health Information Technology)
  - “Health IT systems compromise the hardware and software that are used to electronically create, maintain, analyze, store, or receive information to help in the diagnosis, cure, mitigation, treatment, or prevention or disease.”

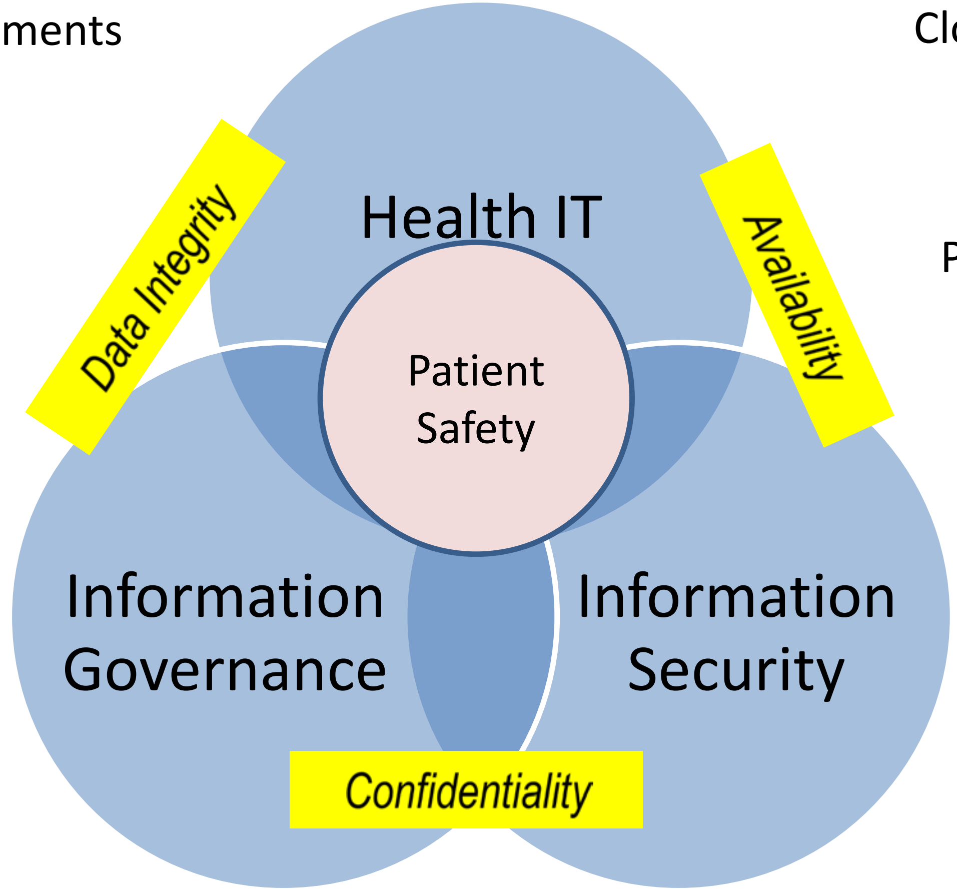
Key Drivers - Impacting Areas

Regulatory requirements

PII/EPHI Theft

Telehealth

Big data
Analytics



Cloud

Patient interaction

Social media

Portable devices

Healthcare IT Characteristics

- ❑ Diversified IT environment
- ❑ Medical Devices and IT System coming together
- ❑ EMR and HIE are changing the IT environment
- ❑ Cloud is getting common
- ❑ Many regulatory requirements
- ❑ Constantly new and changing threats/risks related to the use of technology
- ❑ Immature IT/Information Security

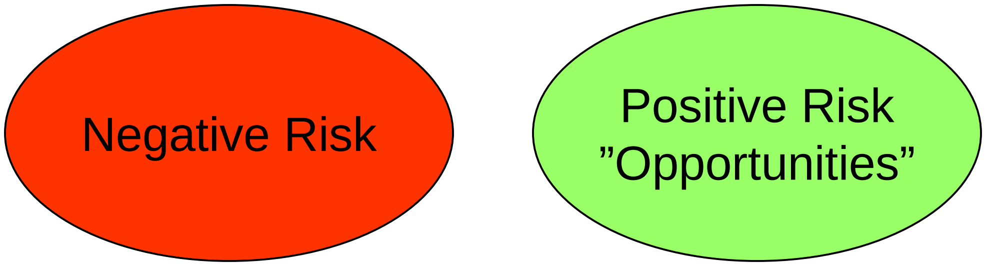
Shift the IT Perspective:

Area	From →	To
Scope:	Technical problem	Enterprise problem/opportunity
Ownership:	IT	Enterprise
Funding:	Expense	Investment
Application:	Platform/practice	Process
Approach:	Adhoc	Managed & Strategic

Risk Management

❑ **Risk and Value**

- Risk has two faces:
  - Protecting against value destruction
  - Value creation opportunities are not missed!
- Understanding risk and managing it is key for creating and safeguarding value



Negative Risk

Positive Risk
”Opportunities”

Results – Identified & Prioritized Risks

The table below lists examples of common IT security risk areas that been identified at healthcare systems.

Risk List	Risk List	Risk List
1. Vendor Management	12. Audit Trail and Logs	23. End-User Devices (Workstations, Tablets, Laptops, USBs, Smart phones, etc.)
2. Change Management	13. Data Warehouse and Other Data Repositories	24. Disposal of Electronic Media
3. Identity and Access Management	14. Internal and External Intrusion	25. PCI-DSS Compliance
4. EPHI Inventory and IT Asset Management	15. IT Governance	26. Problem and Incident Management
5. Network Availability	16. Business Continuity (Downtime)	27. Resources and IT Skills
6. Electronic Communication (Email, Texting, Faxing)	17. Disaster Recovery and Backup Management	28. Roles and Responsibilities
7. IT Risk Management	18. Disposal of Electronic Media	29. Facility/Utility Systems
8. Medical Devices	19. Security Incident Management	30. Grants with IT Requirements
9. Phone Systems	20. Medical Records Data Integrity	31. Cybersecurity
10. Security Awareness	21. Patch management	32. IT Cost
11. Internet Usage and Social Media	22. Physical Security and IT Environmental Controls	33. Affiliated Organizations
		34. Telehealth

Risk Management Approach

Identified IT high risk areas (at a gross risk level)

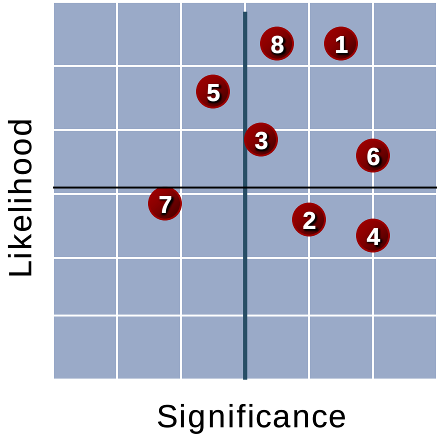
Assess risk management

● Gross risk

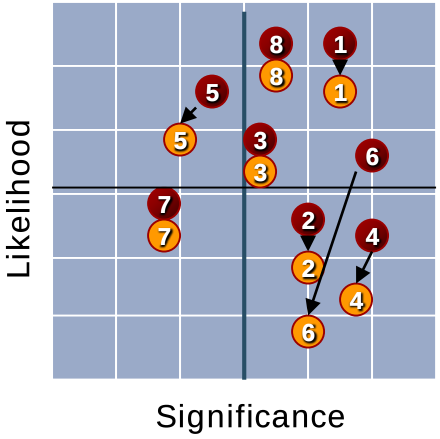
● Net risk

Risk acceptance – Can management accept the existing risk level?

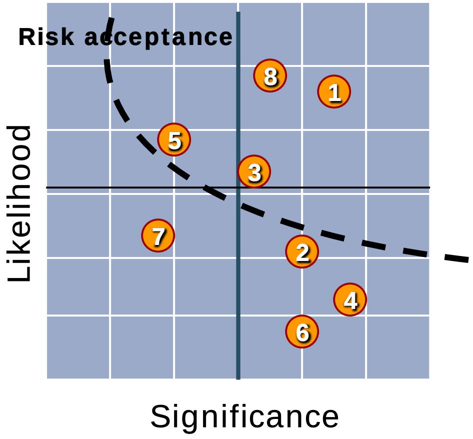
Gross Risk Map



Risk Management



Net Risk Map



High Reliability Organizations (HRO)

- ❑ **Patient safety is a long-recognized problem in health care**
  - ▪ “One-third of hospital admissions have an associated adverse event, a number ten times higher than previously reported. Despite a significant effort by the health care community over the last decade to improve patient safety, there has been no significant improvement overall.“*

** Source: Classen DC, Bates DW. Finding the meaning in meaningful use. New England Journal of Medicine. 2011;365(9):2011–2014.*

High Reliability Organizations (HRO)

❑ **Health IT – Where we are heading…**

- HRO Characteristics
  - High levels of safety and under inherently risky, technology complex and demanding conditions

- **“Healthcare organizations are striving to become HROs such as aviation, nuclear power, and the military”**

High Reliability Organizations (HRO)

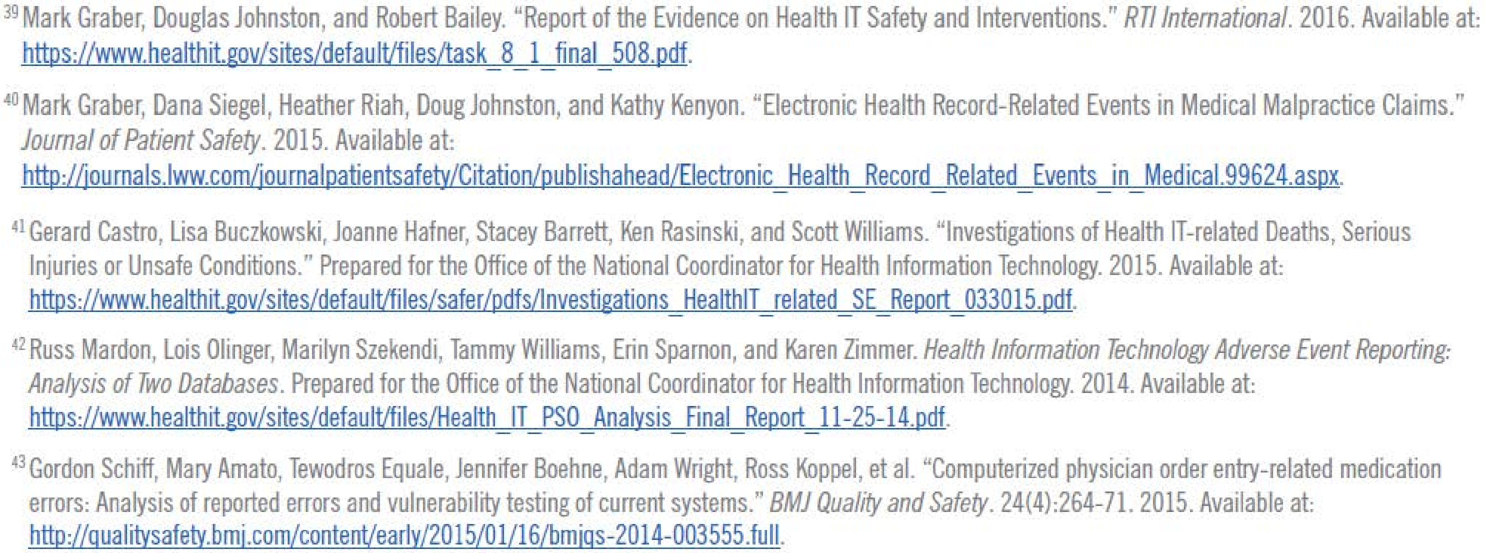
- ❑ **Other high-risk industries (aviation, military, and nuclear energy) have made significant improvements in safety despite their complexity.**
  - Conscientious efforts to ensure that errors do not lead to harm.
  - “commercial airline pilots and air traffic controllers make approximately two errors for every hour flown, yet U.S. air travel is extremely safe.”
  - Safe System Approach – High Resilience

Patient Safety and Information Technology

"A review of numerous studies indicates that health IT has been a factor from anywhere from 2 % to nearly 7 % of the total safety events reported. "

May 2017 Report: Patient Safety and Information Technology – Improving Information Technology's Role in Providing Safer Care

Bipartisan Policy Center



[39] Mark Graber, Douglas Johnston, and Robert Bailey. "Report of the Evidence on Health IT Safety and Interventions." *RTI International*. 2016. Available at: https://www.healthit.gov/sites/default/files/task_8_1_final_508.pdf.

[40] Mark Graber, Dana Siegel, Heather Riah, Doug Johnston, and Kathy Kenyon. "Electronic Health Record-Related Events in Medical Malpractice Claims." *Journal of Patient Safety*. 2015. Available at: http://journals.lww.com/journalpatientsafety/Citation/publishahead/Electronic_Health_Record_Related_Events_in_Medical.99624.aspx.

[41] Gerard Castro, Lisa Buczkowski, Joanne Hafner, Stacey Barrett, Ken Rasinski, and Scott Williams. "Investigations of Health IT-related Deaths, Serious Injuries or Unsafe Conditions." Prepared for the Office of the National Coordinator for Health Information Technology. 2015. Available at: https://www.healthit.gov/sites/default/files/safer/pdfs/Investigations_HealthIT_related_SE_Report_033015.pdf.

[42] Russ Mardon, Lois Olinger, Marilyn Szekendi, Tammy Williams, Erin Sparnon, and Karen Zimmer. *Health Information Technology Adverse Event Reporting: Analysis of Two Databases*. Prepared for the Office of the National Coordinator for Health Information Technology. 2014. Available at: https://www.healthit.gov/sites/default/files/Health_IT_PSO_Analysis_Final_Report_11-25-14.pdf.

[43] Gordon Schiff, Mary Amato, Tewodros Equale, Jennifer Boehne, Adam Wright, Ross Koppel, et al. "Computerized physician order entry-related medication errors: Analysis of reported errors and vulnerability testing of current systems." *BMJ Quality and Safety*. 24(4):264-71. 2015. Available at: http://qualitysafety.bmj.com/content/early/2015/01/16/bmjqs-2014-003555.full.

Patient Safety and Information Technology

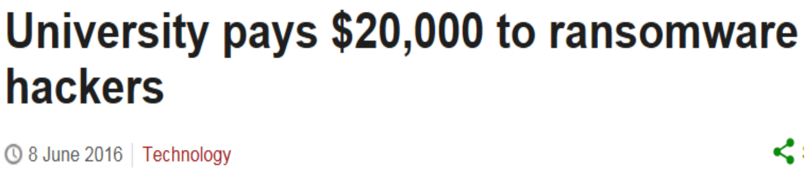
Improving Information Technology's Role in Providing Safer Care

May 2017

BIPARTISAN POLICY CENTER

War Stories – Confidentiality / Availability

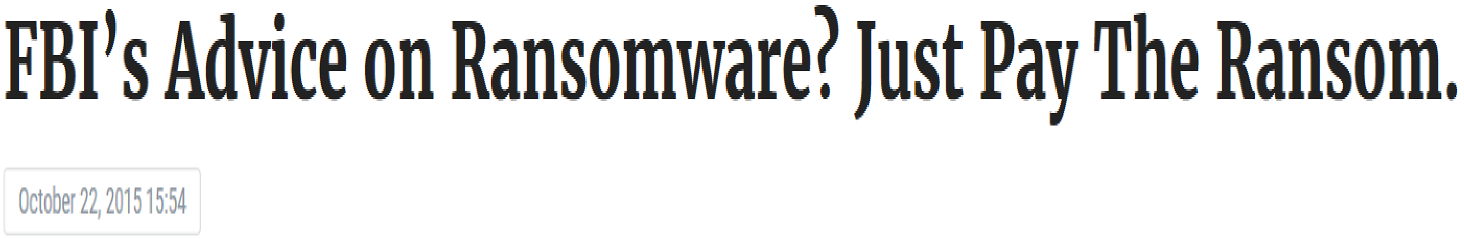
Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money



University pays $20,000 to ransomware hackers

8 June 2016 | Technology

In February 2016, the Hollywood Presbyterian Medical Center paid $17,000 to restore access to its system.



FBI's Advice on Ransomware? Just Pay The Ransom.

October 22, 2015 15:54

War Stories – Integrity

Cybersecurity Predictions – Integrity Attacks

By Matthew Rosenquist

Unlike denial-of-service attacks which undermine the availability of entire systems or data breaches which steal away confidential data, integrity focused attacks maliciously modify data or transactions.

The growth of *Integrity*-attacks could be the unexpected shift which will fuel significant change in perspectives, expectations, and controls.

Such cyber events will probably be some form of data sabotage, the subtle tweaking of data within transactions to gain some type of benefit.

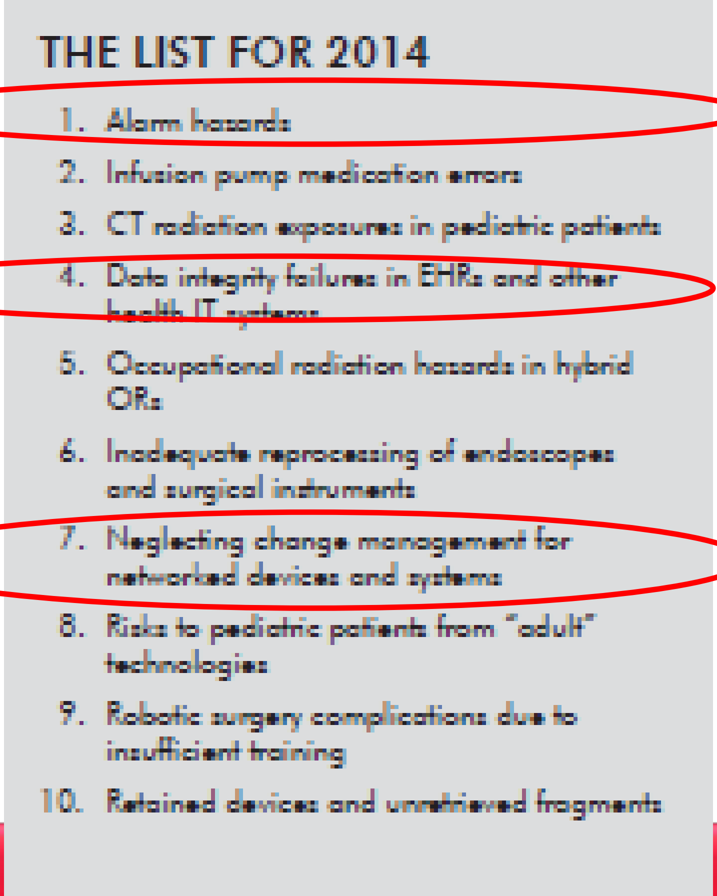
Banking infrastructure malware Carbanak, which was discovered in 2015, infected banks and selectively modified systems to create a small number of fraudulent transactions which fleeced hundreds of millions of dollars in a single coordinated campaign.

"That's the interesting thing about integrity attacks — they can be highly beneficial to the attacker in that they can often achieve their goals more effectively than a traditional attack," said Steve Grobman, chief technology officer of Intel Security Group

Fraudulent messages crafted from executive's accounts to account-payable departments, instructing money transfers be made immediately to a 3rd party.

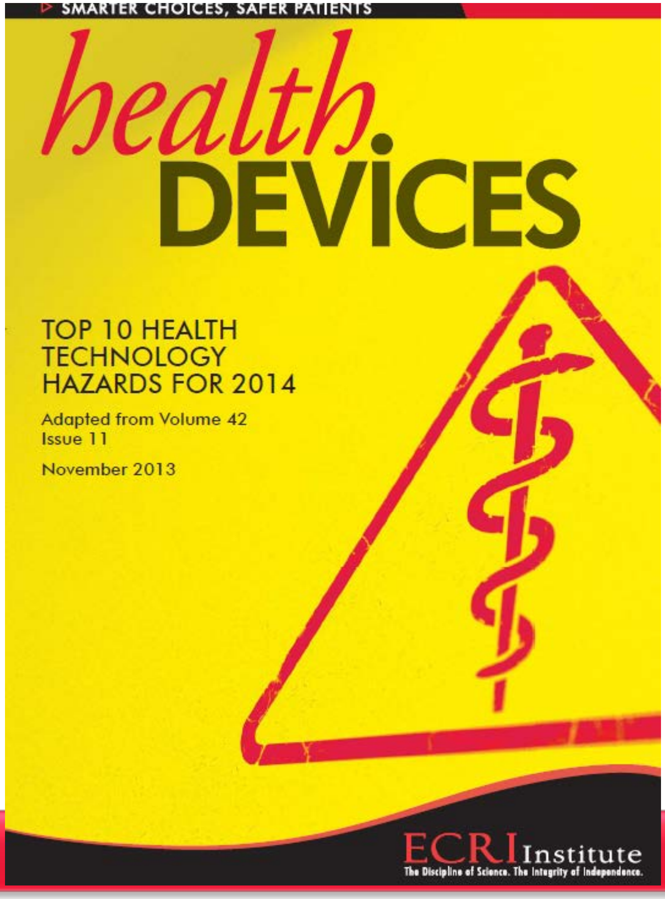
Top 10 Health Technology Risks 2014

- ❑ **ECRI institute annual report**



THE LIST FOR 2014

1. Alarm hazards
2. Infusion pump medication errors
3. CT radiation exposures in pediatric patients
4. Data integrity failures in EHRs and other health IT systems
5. Occupational radiation hazards in hybrid ORs
6. Inadequate reprocessing of endoscopes and surgical instruments
7. Neglecting change management for networked devices and systems
8. Risks to pediatric patients from "adult" technologies
9. Robotic surgery complications due to insufficient training
10. Retained devices and unretrieved fragments



▷ SMARTER CHOICES, SAFER PATIENTS

health DEVICES

TOP 10 HEALTH TECHNOLOGY HAZARDS FOR 2014

Adapted from Volume 42 Issue 11

November 2013

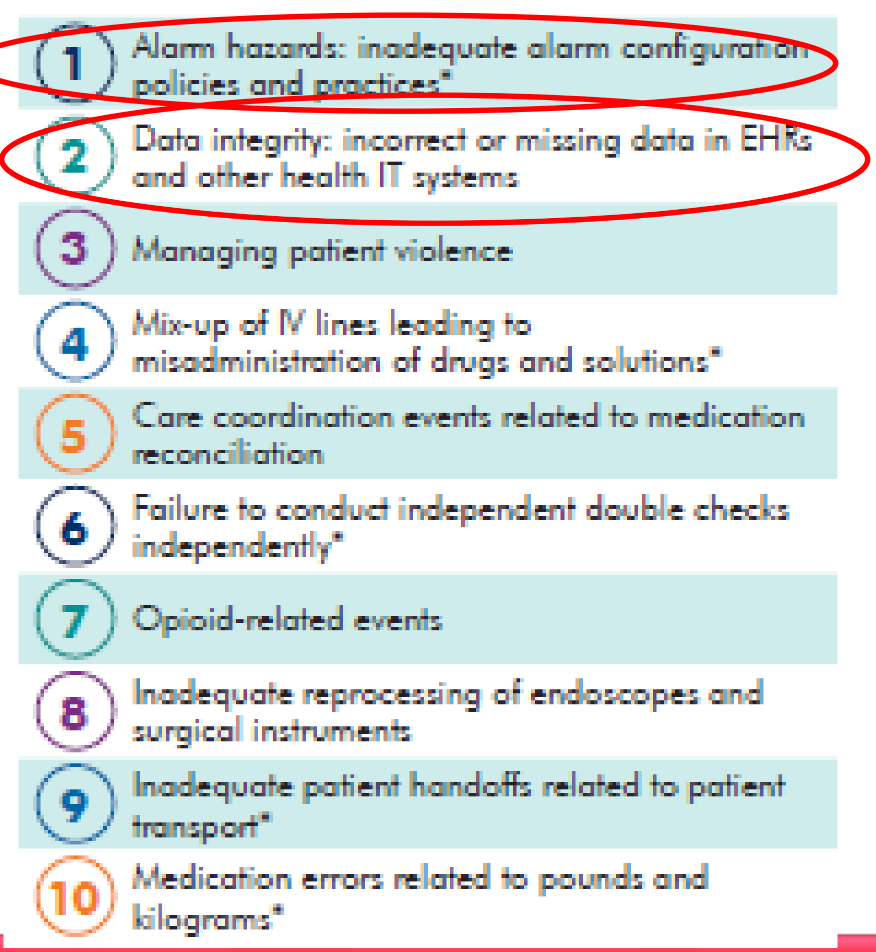
ECRI Institute

The Discipline of Science. The Integrity of Independence.

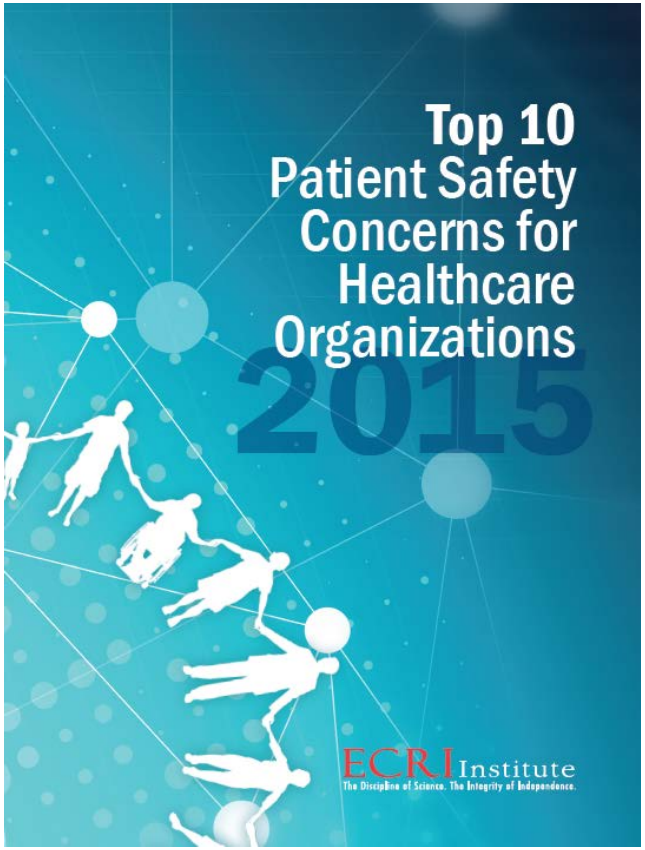
Top 10 Health Technology Risks – ECRI 2014

- ❑ 1. Alarm Hazards
- ❑ 2. Infusion Pump Medication Errors
- ❑ 3. CT Radiation Exposure in Pediatric Patients
- ❑ 4. Data Integrity Failures in EHRs and other Health IT Systems
- ❑ 5. Occupational Radiation Hazards in Hybrid ORs
- ❑ 6. Inadequate Reprocessing of Endoscopes and Surgical Instruments
- ❑ 7. Neglecting Change Management for Networked Devices and Systems
- ❑ 8. Risks to Pediatric Patients from "Adult" Technologies
- ❑ 9. Robotic Surgery Complications due to Insufficient Training
- ❑ 10. Retained Devices and Unretrieved Fragments

Top 10 Patient Safety Concerns 2015



1. Alarm hazards: inadequate alarm configuration policies and practices*
2. Data integrity: incorrect or missing data in EHRs and other health IT systems
3. Managing patient violence
4. Mix-up of IV lines leading to misadministration of drugs and solutions*
5. Care coordination events related to medication reconciliation
6. Failure to conduct independent double checks independently*
7. Opioid-related events
8. Inadequate reprocessing of endoscopes and surgical instruments
9. Inadequate patient handoffs related to patient transport*
10. Medication errors related to pounds and kilograms*



Top 10 Patient Safety Concerns for Healthcare Organizations 2015

ECRI Institute

The Discipline of Science. The Integrity of Independence.

Top 10 Patient Safety Hazards ECRO 2016

- ❑ 1. Health IT Configurations and Organizational Workflow That Do Not Support Each Other
- ❑ 2. Patient Identification Errors
- ❑ 3. Inadequate Management of Behavioral Health Issues in Non-Behavioral-Health Settings
- ❑ 4. Inadequate Cleaning and Disinfection of Flexible Endoscopes
- ❑ 5. Inadequate Test-Result Reporting and Follow-up
- ❑ 6. Inadequate Monitoring for Respiratory Depression in Patients Prescribed Opioids
- ❑ 7. Medication Errors Related to Pounds and Kilograms
- ❑ 8. Unintentionally Retained Objects despite Correct Count
- ❑ 9. Inadequate Antimicrobial Stewardship
- ❑ 10. Failure to Embrace a Culture of Safety

Top 10 Health Safety Hazards 2017

- □ **1. Infusion Errors Can Be Deadly If Simple Safety Steps Are Overlooked**
- □ **2. Inadequate Cleaning of Complex Reusable Instruments Can Lead to Infections**
- □ **3. Missed Ventilator Alarms Can Lead to Patient Harm**
- □ **4. Undetected Opioid-Induced Respiratory Depression**
- □ **5. Infection Risks with Heater-Cooler Devices Used in Cardiothoracic Surgery**
- □ **6. Software Management Gaps Put Patients, and Patient Data, at Risk**
- □ **7. Occupational Radiation Hazards in Hybrid ORs**
- □ **8. Automated Dispensing Cabinet Setup and Use Errors May Cause Medication Mishaps**
- □ **9. Surgical Stapler Misuse and Malfunctions**
- □ **10. Device Failures Caused by Cleaning Products and Practices**

EXECUTIVE BRIEF
Top 10 Health Technology Hazards for 2018
A Report from Health Devices
health DEVICES
ECRI Institute

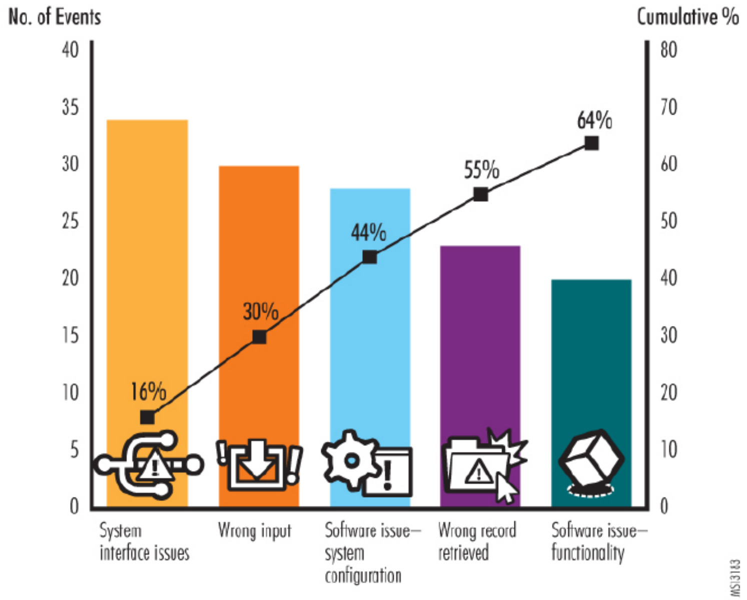
Top 10 Health Technology Hazards 2018

1. **Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients**
2. **Endoscope Reprocessing Failures Continue to Expose Patients to Infection Risk**
3. **Mattresses and Covers May Be Infected by Body Fluids and Microbiological Contaminants**
4. **Missed Alarms May Result from Inappropriately Configured Secondary Notification Devices and Systems**
5. **Improper Cleaning May Cause Device Malfunctions, Equipment Failures, and Potential for Patient Injury**
6. **Unholstered Electrosurgical Active Electrodes Can Lead to Patient Burns**
7. **Inadequate Use of Digital Imaging Tools May Lead to Unnecessary Radiation Exposure**
8. **Workarounds Can Negate the Safety Advantages of Bar-Coded Medication Administration Systems**
9. **Flaws in Medical Device Networking Can Lead to Delayed or Inappropriate Care**
10. **Slow Adoption of Safer Enteral Feeding Connectors Leaves Patients at Risk**

Reported Top Safety Issues Health IT - ONC

- □ System interface issues
- □ Wrong input
- □ Software issue – system configuration
- □ Wrong record retrieved/duplicate records
- □ Software issue – functionality

Figure 3. ECRI Institute PSO Deep Dive Identifies Top Five Safety Issues from Health IT Events



The percentage identified with each event type represents the accumulative total of that event type and any preceding event types as a portion of the 211 safety events.

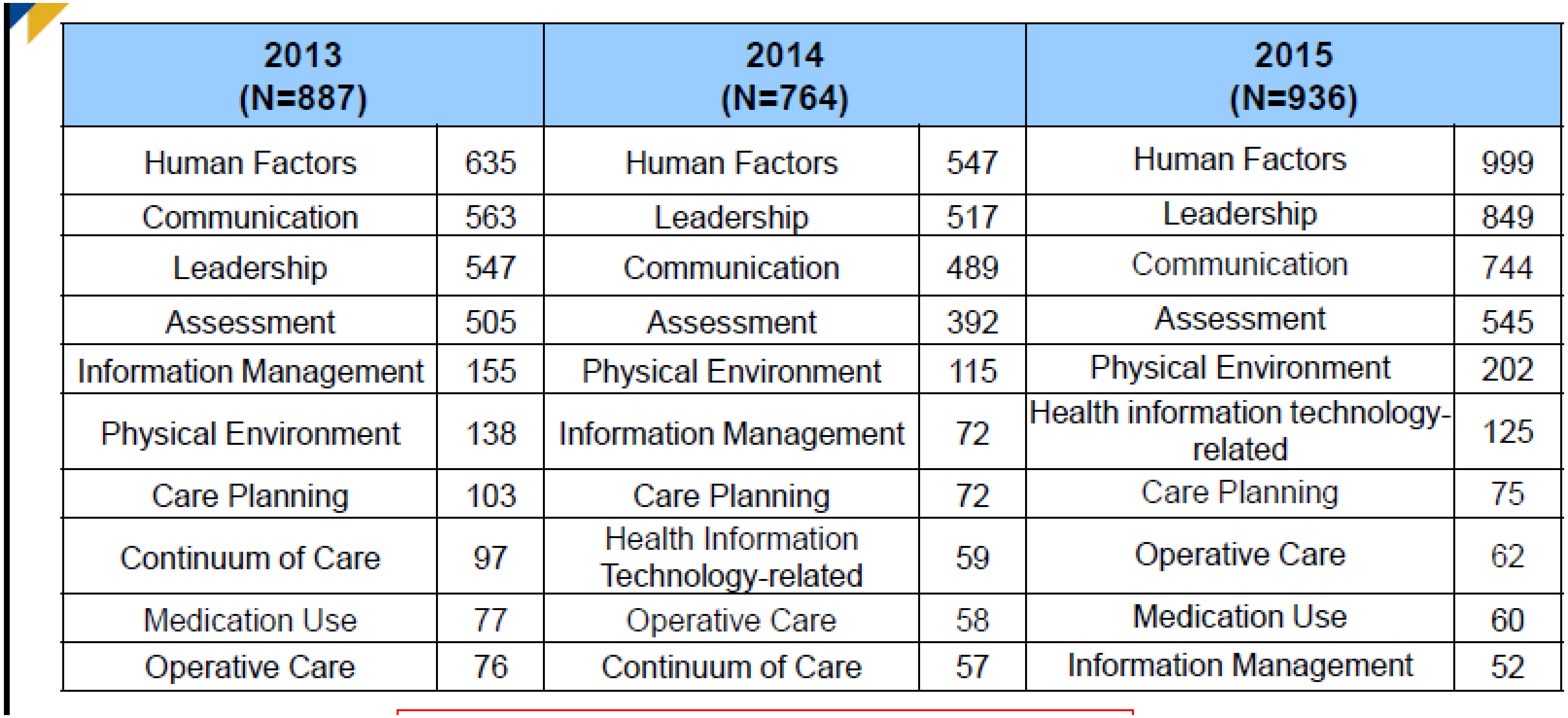
Most Common “IT” Issues – Patient Safety

❑ **Approximately 5% of reported patient safety issues in these studies were Health IT related with the conclusion:**

❑ **75% of these were preventable.**

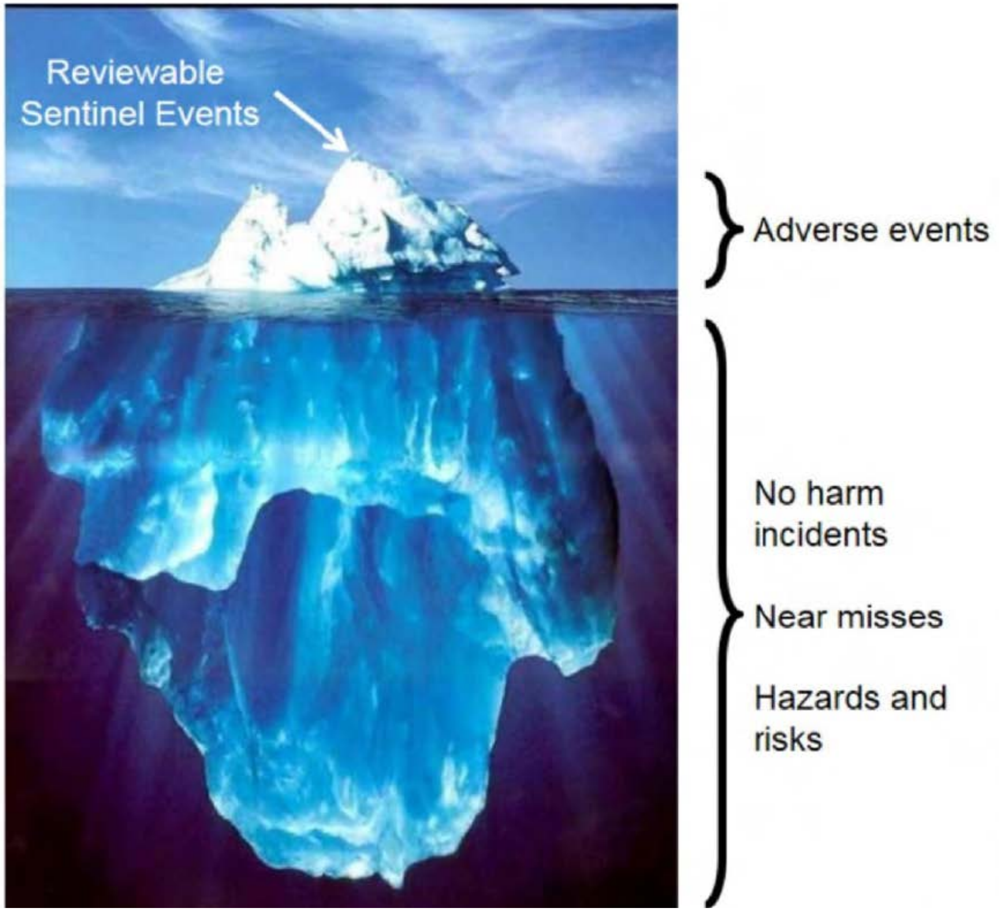
❑ **There were limited numbers of reported incidents related to access issues, network failures, hardware failures, security, malware or virus issues.**

Sentinel Event Data Joint Commission



2013 (N=887)		2014 (N=764)		2015 (N=936)	
Human Factors	635	Human Factors	547	Human Factors	999
Communication	563	Leadership	517	Leadership	849
Leadership	547	Communication	489	Communication	744
Assessment	505	Assessment	392	Assessment	545
Information Management	155	Physical Environment	115	Physical Environment	202
Physical Environment	138	Information Management	72	Health information technology-related	125
Care Planning	103	Care Planning	72	Care Planning	75
Continuum of Care	97	Health Information Technology-related	59	Operative Care	62
Medication Use	77	Operative Care	58	Medication Use	60
Operative Care	76	Continuum of Care	57	Information Management	52

Remember


Reviewable
Sentinel Events
Adverse events
No harm
incidents
Near misses
Hazards and
risks

Key Aspects – Root Causes

❑ **Limited awareness of the safety risks introduced by Health IT**

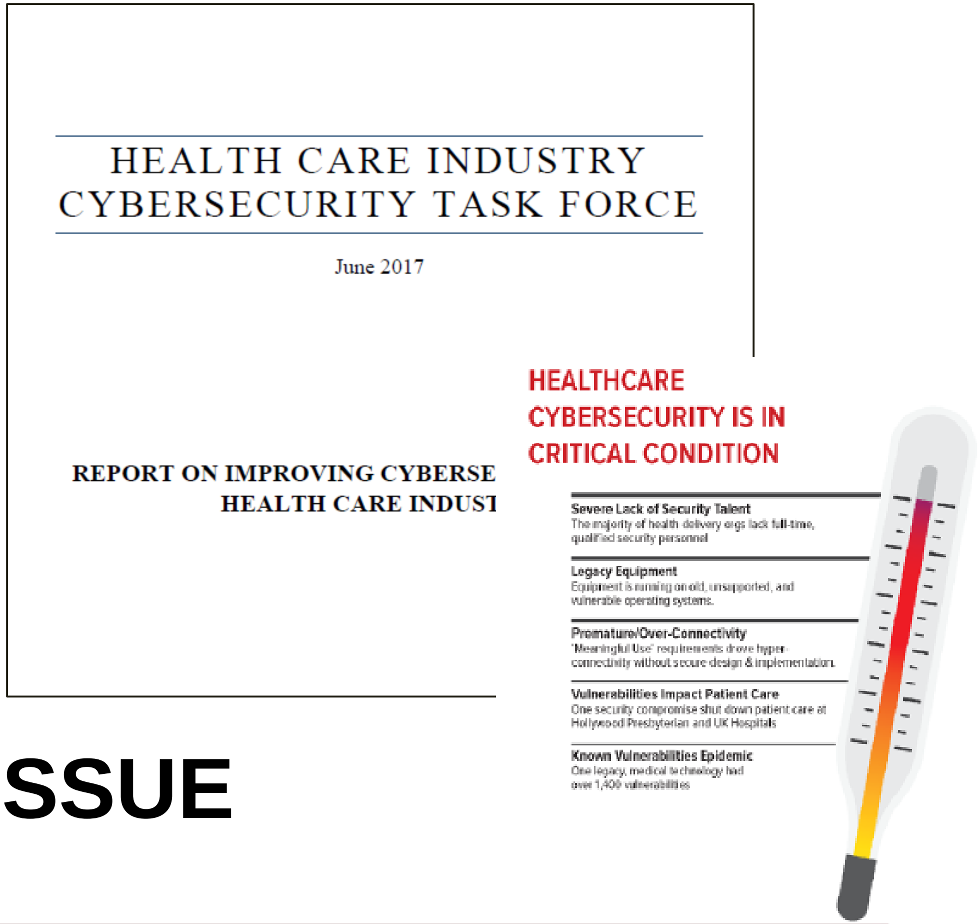
❑ **Traditional department "silos" between risk management, IT, and quality and safety management**

❑ **Urgent need for tools and metrics to manage Health IT safety risks.**

Health Care Industry Cyber Security Task Force Report

- ❑ **General Conclusions:**
  - Lack of Security Talent
  - Legacy Equipment
  - Lack of Standards
  - Meaningful Use drove unsecured connectivity
  - Not an IT issue -

PATIENT SAFETY ISSUE



HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSE
HEALTH CARE INDUST

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

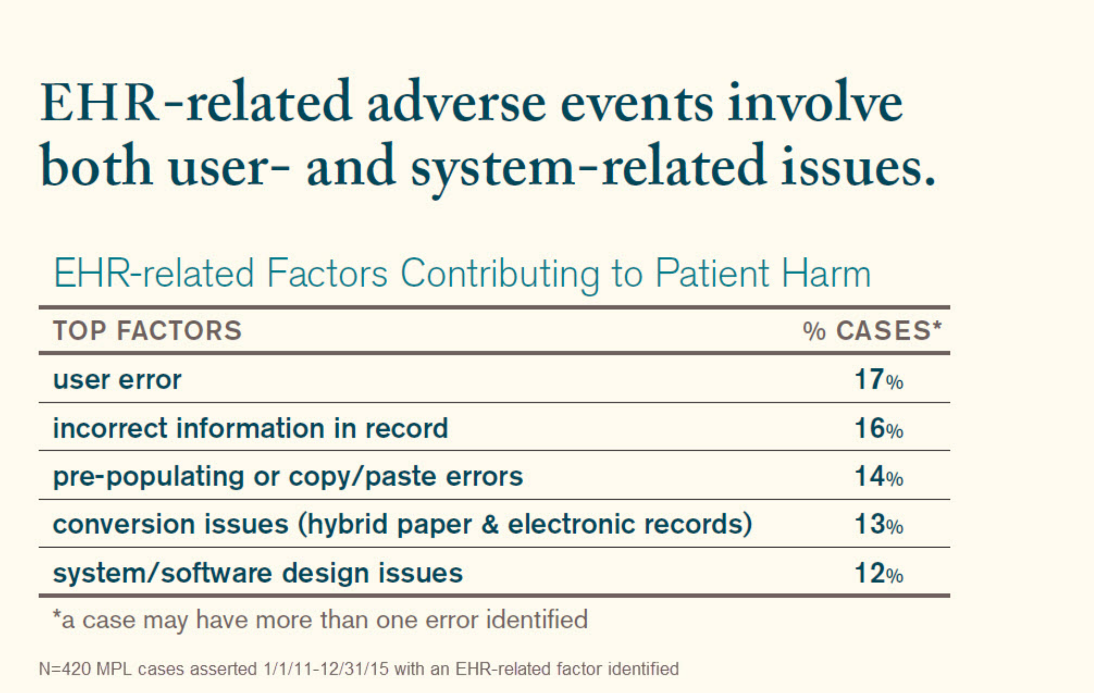
Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

CRICO - Malpractice Risks Associated with Electronic Health Records (06/2017)

- ❑ **A retrospective, cohort study of claims in the CRICO Strategies national Comparative Benchmarking System was conducted for medical malpractice cases coded using a specific coding taxonomy during the period January 1, 2011 through December 31, 2015**



EHR-related adverse events involve both user- and system-related issues.

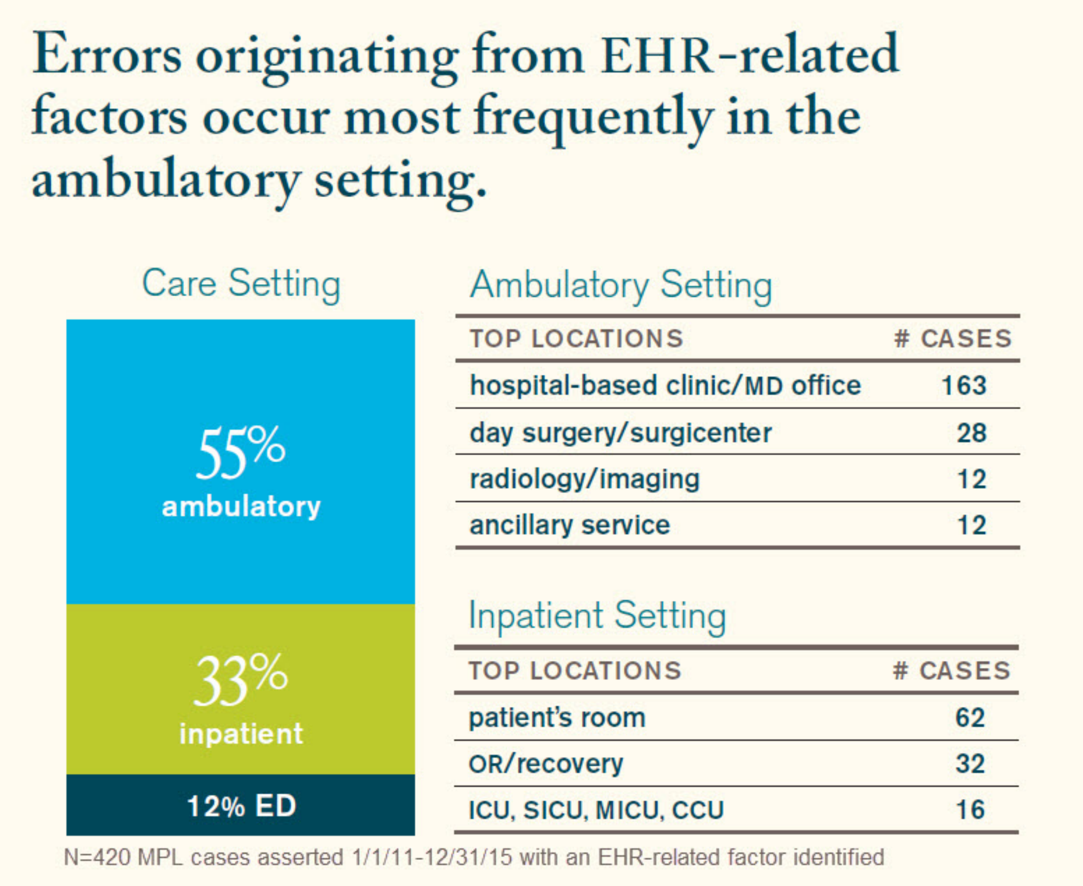
EHR-related Factors Contributing to Patient Harm

TOP FACTORS	% CASES*
user error	17%
incorrect information in record	16%
pre-populating or copy/paste errors	14%
conversion issues (hybrid paper & electronic records)	13%
system/software design issues	12%

*a case may have more than one error identified

N=420 MPL cases asserted 1/1/11-12/31/15 with an EHR-related factor identified

CRICO - Malpractice Risks Associated with Electronic Health Records (06/2017)



Errors originating from EHR-related factors occur most frequently in the ambulatory setting.

Care Setting

55% ambulatory

33% inpatient

12% ED

Ambulatory Setting

TOP LOCATIONS	# CASES
hospital-based clinic/MD office	163
day surgery/surgicenter	28
radiology/imaging	12
ancillary service	12

Inpatient Setting

TOP LOCATIONS	# CASES
patient's room	62
OR/recovery	32
ICU, SICU, MICU, CCU	16

N=420 MPL cases asserted 1/1/11-12/31/15 with an EHR-related factor identified

System related issues

- ❑ **PCP cannot access radiology studies during patient visit; results later filed without PCP review.**
  - ▪ **Result**: delayed diagnosis of lung cancer.
- ❑ **MD unable to access nursing ED triage note.**
  - ▪ **Result**: death from mismanaged subarachnoid hemorrhage.
- ❑ **When the complaint field was too small to record "sudden onset chest pain w/burning epigastric pain," the patient's complaint was shortened to "epigastric pain."**
  - ▪ **Result**: mismanaged workup and subsequent cardiac event.

User-related issues (training and education)

- ❑ **OB could not access patient's clinic notes documenting abnormal fetal size, citing lack of training and no EHR password.**
- ❑ **MD received an amoxicillin allergy alert but ordered it anyway, causing allergic reaction.**
- ❑ **Patient developed amiodarone toxicity after history and medications copied from previous note did not document patient was already on this medication.**

NATIONAL HEALTHCARE QUALITY AND DISPARITIES REPORT

	Offices in PSC Quartile 1 (Bottom) %	Offices in PSC Quartile 2 %	Offices in PSC Quartile 3 %	Offices in PSC Quartile 4 (Top) %
Pharmacy contacts office to clarify or correct a prescription	37	27.9	25.4	18
Patient unable to get visit in 48 hours for acute problem	22.5	16	14	7.9
Medication list not updated at last visit	18.9	11	8.4	3.9
Results from lab or imaging test not available when needed	16.5	8.6	7.4	4.5
Information exchange problems with pharmacies	18.3	12.6	10.3	4.5
Information exchange problems with other offices	13.7	9.7	8.2	3.9
Information exchange problems with outside labs or imaging centers	12.8	9.6	8.7	4.4

Produced with the help of an Interagency Work Group led by the Agency for Healthcare Research and Quality and submitted on behalf of the Secretary of the Department of Health and Human Services

Table of Contents

❑ Introduction

❑ Key IT and Cyber Risks and Opportunities

❑ **What Risks to Audit?**

❑ Board and Management Communication

❑ Trending Best Practice/Standards and Resources

❑ Conclusion

❑ Q&A

What are our IT Audit Challenges?

❑ **Lack of information**

❑ **Resources**

❑ **Skills**

❑ **Reactive instead of pro-active**

❑ **Evolving area**

Fines Biggest Risk?

- ❑ **1. Hollywood, Fla.-based Memorial Healthcare System agreed to implement a corrective action plan and paid HHS $5.5 million to settle claims it violated HIPAA.**
  - Unauthorized employee access
  - Terminated employee affiliated organization
  - No regular review
- ❑ **2. HHS' Office for Civil Rights fined Children's Medical Center of Dallas $3.2 million for failing to comply with HIPAA on multiple occasions.**
  - 2010 unencrypted device
  - 2013 unencrypted device
- ❑ **3. MAPFRE Life Insurance Company of Puerto Rico agreed to implement a corrective action plan and pay $2.2 million to HHS' Office for Civil Rights to settle claims it violated HIPAA.**
  - Unencrypted device
  - Risk management plan and action

Reported Security Breaches to OCR 2009-2016 per Type

- ❑ **480 Unauthorized access/disclosure**
- ❑ **266 Hacking**
- ❑ **795 Theft**
- ❑ **154 Loss**
- ❑ **63 Improper Disposal**

Root Causes

- ❑ **Lack of Policies in Key Areas, no IT Standards and Limited/Weak Formal Procedures in Key Areas**
- ❑ **Managements and Business/Information owner's responsibilities for IT Security is Not Well Defined and Communicated**
- ❑ **Risk Management Plan and Risk Analysis Goals/Measurement/ Reporting**
- ❑ **Lifecycle Management – Hardware/Software**
- ❑ **Resources in Key Areas e.g. networks, system administrators, disaster recovery, security governance**
- ❑ **Weak Critical Foundational IT Processes**
  - ▪ Patch management
  - ▪ Change management
  - ▪ IT Asset Management
  - ▪ Disaster recovery
- ❑ **IT Governance – ERM – Leadership**

Change in Security Landscape

- ❑ **Move from “careless” security breaches (lost of laptops) to a more active Cyber Crime as a business (ransomware/extortion)**

+

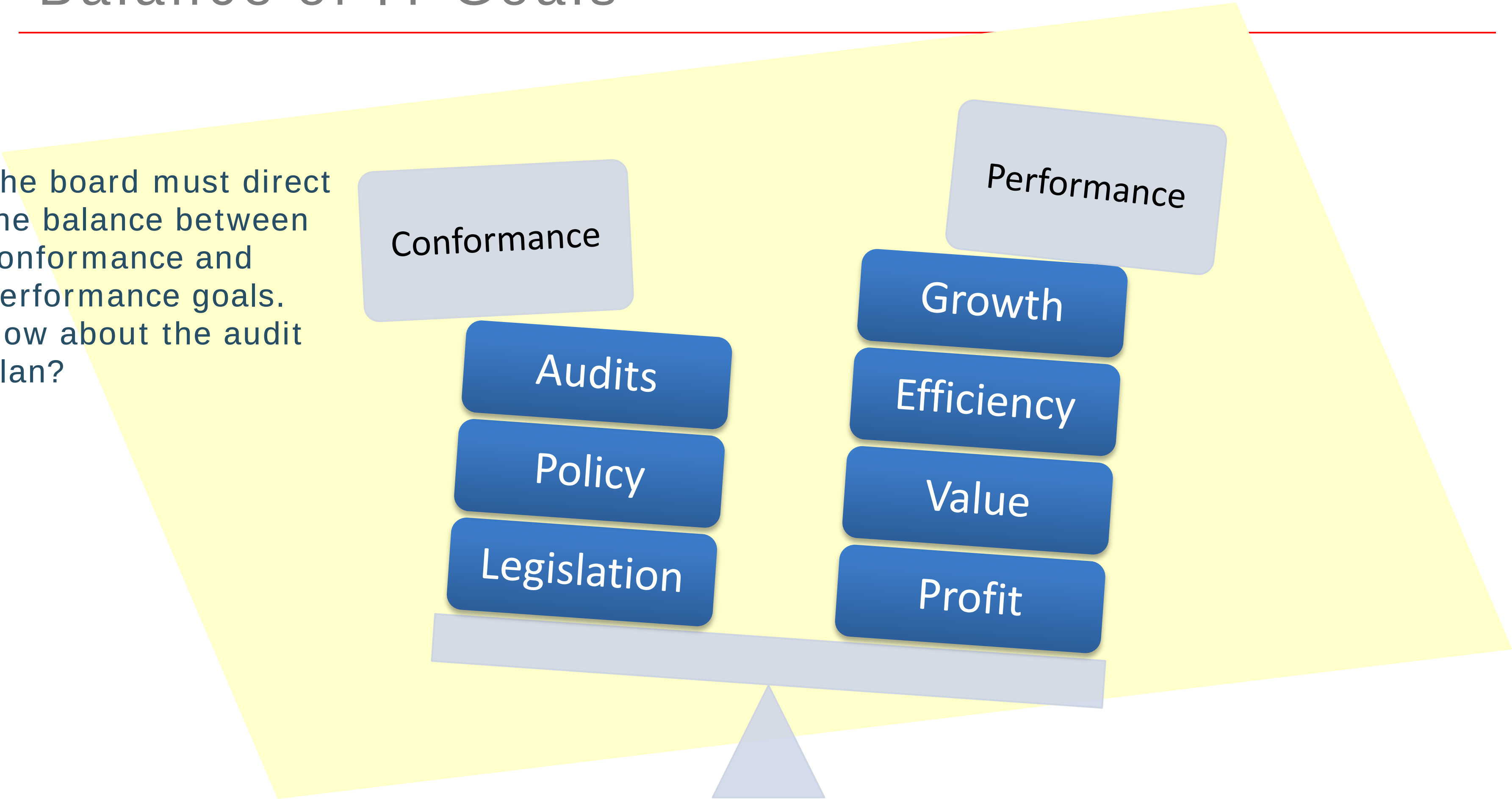
- ❑ **More than 40% of Breaches are due to “unintentional employee negligence” which can be attributed to inconsistent organizational policies, processes not being followed, and uncertainty by staff with different levels of training and experience**

  (Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/)

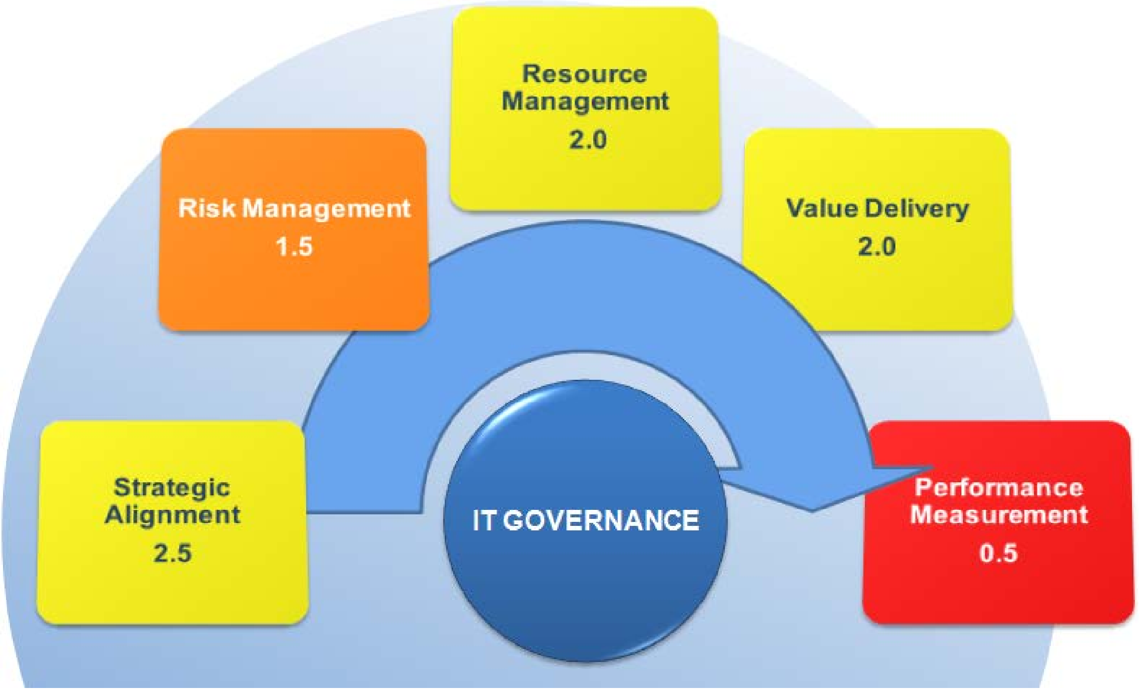
- ❑ **Information security risks are now undermining healthcare’s intellectual property, brand, and mission, and threatening patient care and safety in the process.**

Balance of IT Goals

The board must direct the balance between conformance and performance goals. How about the audit plan?



IT Governance Areas



Process Maturity Rating	
0	**Non-existent:** The process (control/procedures) does not exist.
1	**Initial/Ad hoc:** The process is informal, undocumented and reactive.
2	**Repeatable:** The process is repeatable but may be applied inconsistently as needed.
3	**Defined:** The process is documented and communicated.
4	**Managed:** The process is implemented and measurable.
5	**Optimizing:** Managed process with continuous performance improvements utilizing best practices.
N/A	**Not Applicable:** The process is not applicable to the review or has not been reviewed for other reasons.

IT Governance

“you can not manage what you can not measure.”

Roles/Responsibilities

❑ ACCOUNTABILITY

- Accountability applies to those who own the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific Risk IT processes.

❑ RESPONSIBILITY:

- Responsibility belongs to those who must ensure that the activities are completed successfully.

❑ Legend of the table:

- When a cell is YELLOW, the role carries responsibility and/or partial accountability for the process
- When a cell is GREEN, the role carries main accountability for the process. Only one role can be the main accountable for a given process.

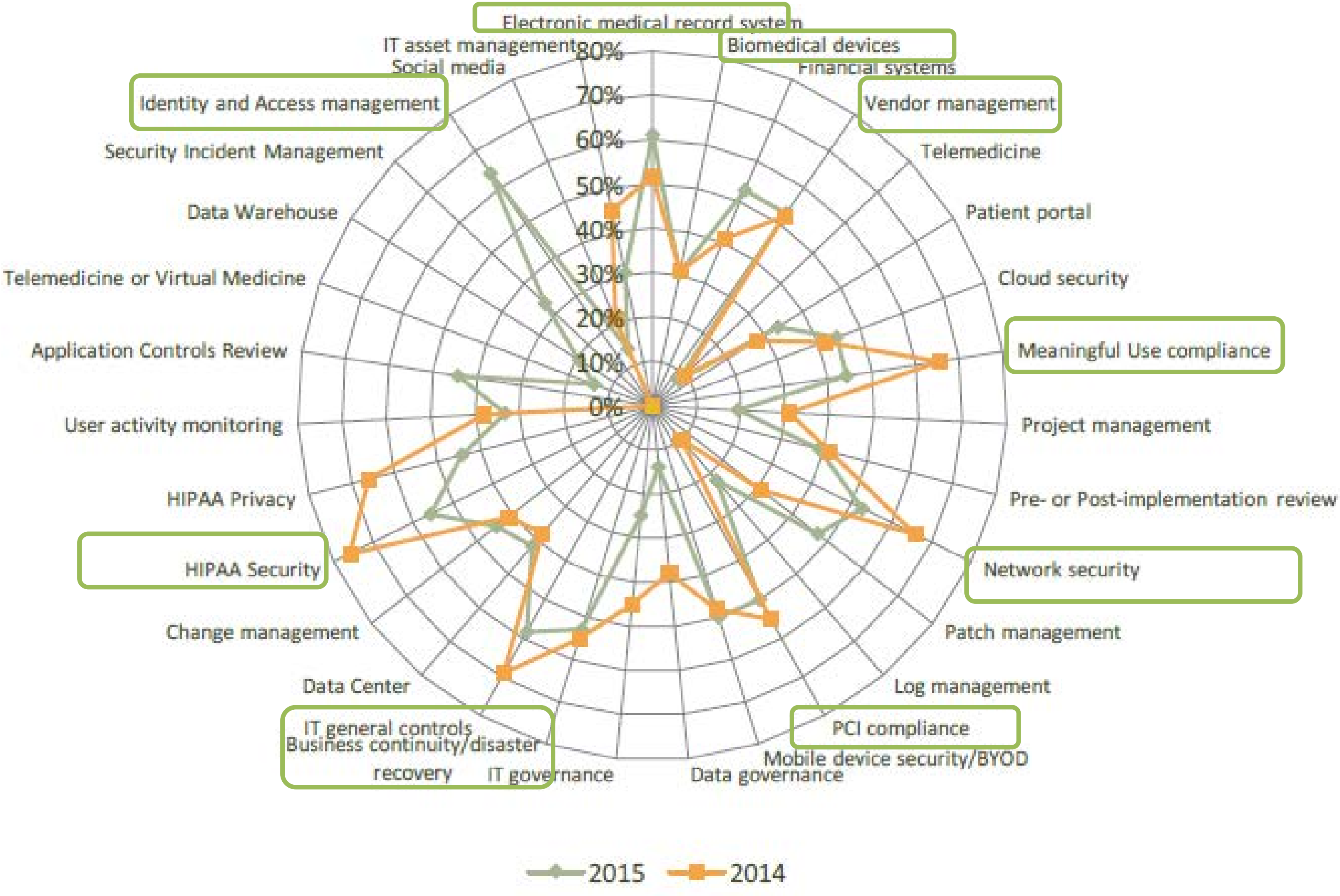
Responsibilities & Accountability (RISK-IT)

ROLE DEFINITIONS, RESPONSIBILITIES & ACCOUNTABILITY		RISK GOVERNANCE			RISK EVALUATION			RISK RESPONSE		
Role	Definition of the Role	Common Risk View	Integrate with ERM	Risk-Aware Decisions	Collect Data	Analyze Risk	Maintain Risk Profile	Articulate Risk	Manage Risk	React to Events
Board	This group of most senior and/or non-executives of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources.	A								
Chief Executive Officer (CEO)	The highest ranking officer who is in charge of the total management of the enterprise.	R							A	
Chief Risk Officer (CRO)	The individual who oversees all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.	R	R	R	A	R	R	A	R	R
Chief Information Officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. The CIO typically chairs the governance council that manages the portfolio.	R	R	R	R	R	R	R	R	R
Chief Financial Officer (CFO)	The most senior official of the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks.	R								
Enterprise Risk Committee	The group of executives of the enterprise who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management activities and decisions.	R		R		R		R		
Business Management	Business individuals with roles related to managing (a) programme(s).	R	R	A		A	A	R	R	R
Business Process Owner	The individual responsible for identifying process requirements, approving process design and managing process performance. In general, a business process owner must at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities.	R	R	R	R	R	R	R	R	A
Risk Control Functions	The functions in the enterprise responsible for managing specific risk domains (e.g. Chief Information Security Officer, business continuity plan – disaster recovery, supply chain, Project Management Office).	R	R	R	R	R	R	R	R	R
Human (HR)	The most senior official of the enterprise who is accountable for planning and policies with respect to all human resources	R								

A (Accountable)

R (Responsible)

AHIA – IT Audit and IT Security Survey 2014-17



Most Common Audit Areas

- ❑ **Identity and Access Management**
- ❑ **EMR Core System**
- ❑ **IT General Controls**
- ❑ **HIPAA**
- ❑ **Financial Systems**
- ❑ **Vendor Management**
- ❑ **Business Continuity and Disaster Recovery**
- ❑ **Network Security**
- ❑ **PCI**
- ❑ **Mobile Device Management**
- ❑ **Patch Management**
- ❑ **Cybersecurity**
- ❑ **New Systems**

Additional Key Risks to Audit

- ❑ **Health IT**
  - ▪ Internet of Things
  - ▪ Telehealth
  - ▪ Apps (internet of things)
  - ▪ Risk Management
  - ▪ Medical Devices
- ❑ **Data Warehouse**
- ❑ **HIE**
- ❑ **Information Governance**
- ❑ **IT Governance**
- ❑ **Patient Communication/Portal**
- ❑ **Backup Management**
- ❑ **Security Awareness Training**
- ❑ **Emergency Management/BCP/DR**

Added Value Audits – Hidden Opportunities

- ❑ **Life Cycle Management**
  - Application/Tool functionality
  - Tools
  - Cost
  - Age
  - Utilization
  - Budget/capacity/acquisition processes
- ❑ **Identity and Access management**
  - Number of systems
  - Authentication
  - Resources for management of access management (FTE/cost)

IT Audit Plan Considerations

- ❑ **Comprehensive IT Risk Assessment**
- ❑ **Build Long Term IT Audit Plan**
- ❑ **Regular Audit of Key Control Areas**
  - ▪ Value added internal benchmarks
  - ▪ Trends
- ❑ **Framework Based**
  - ▪ Standard benchmark
- ❑ **Pro-Active Audits/Value Added Work**
  - ▪ Pre-implementation
  - ▪ Committees
- ❑ **Value – Cost – Investment – i.e. Performance**
- ❑ **Audit Tools**

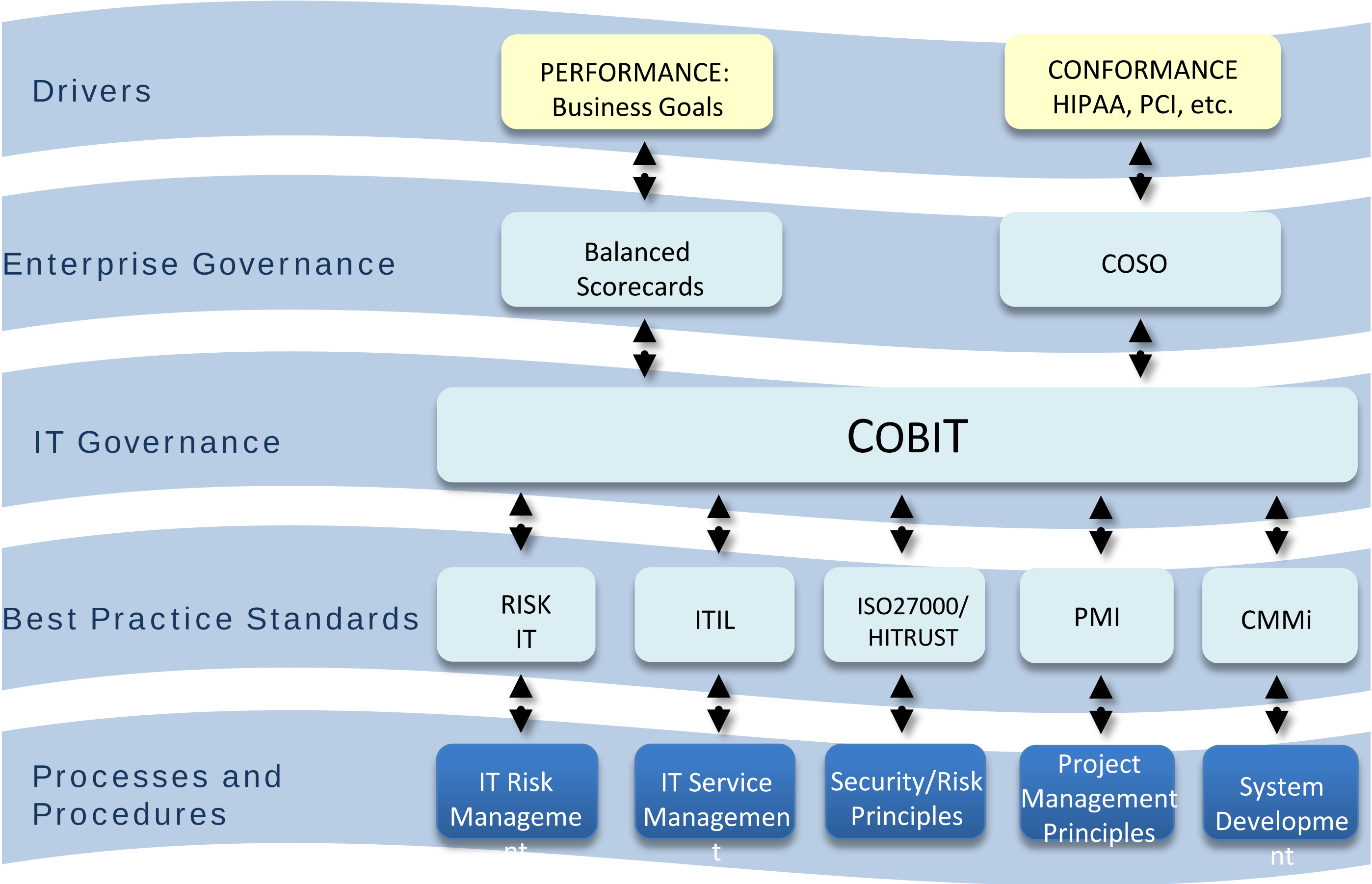
Table of Contents

- ❑ Introduction
- ❑ Key IT and Cyber Risks and Opportunities
- ❑ What Risks to Audit?
- ❑ **Board and Management Communication**
- ❑ Trending Best Practice/Standards and Resources
- ❑ Conclusion
- ❑ Q&A

Discussion Areas Management/Board

- ❑ **Health IT**
- ❑ **Information Governance**
- ❑ **Information Security**
- ❑ **IT Standards**
- ❑ **Measurements and Metrics**
  - ▪ Board
  - ▪ Executive Management
  - ▪ Management

IT Governance Architecture



Drivers

PERFORMANCE: Business Goals

CONFORMANCE HIPAA, PCI, etc.

Enterprise Governance

Balanced Scorecards

COSO

IT Governance

COBIT

Best Practice Standards

RISK IT

ITIL

ISO27000/ HITRUST

PMI

CMMi

Processes and Procedures

IT Risk Manageme nt

IT Service Managemen t

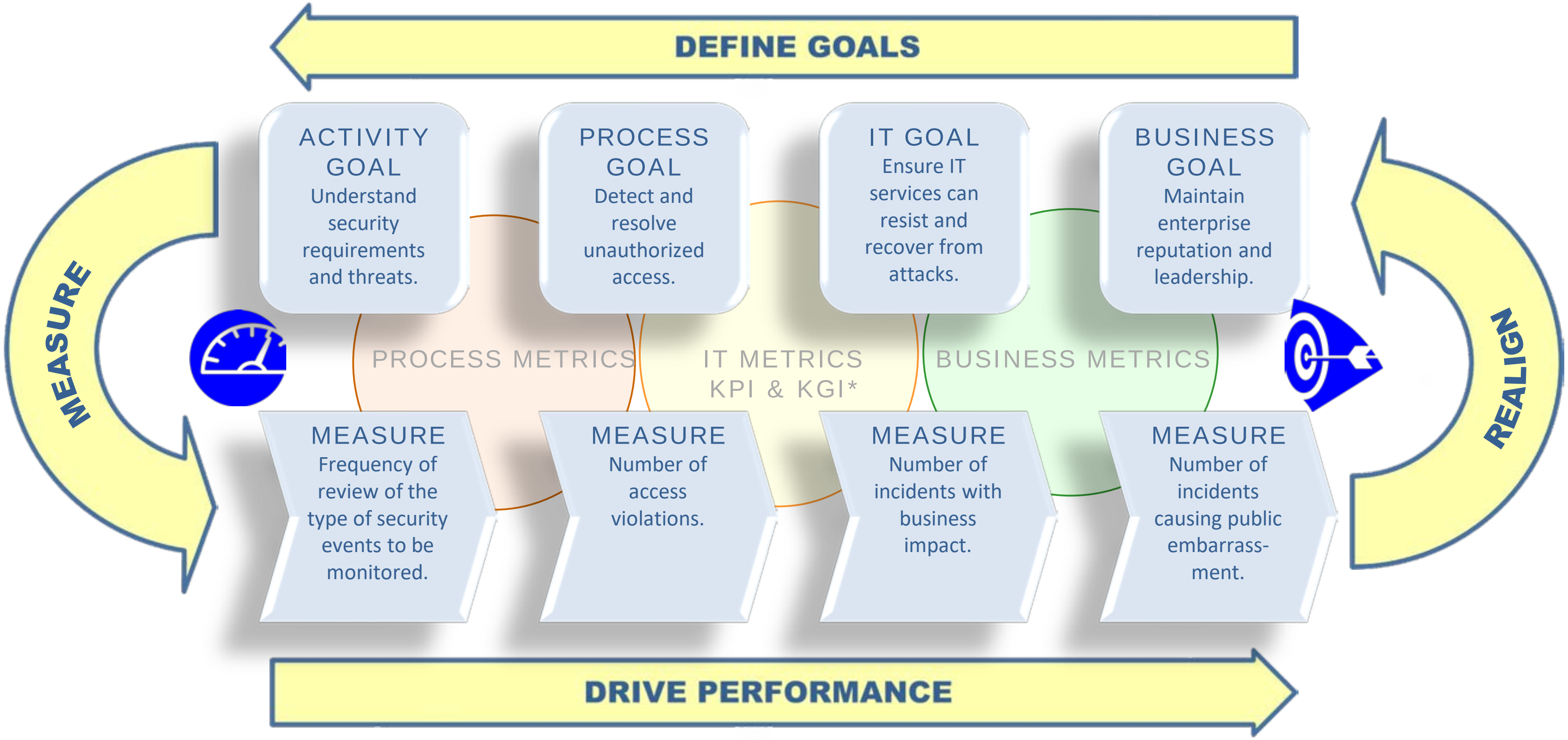
Security/Risk Principles

Project Management Principles

System Developme nt

IT Goals and Metrics

You cannot manage what you do not measure!


DEFINE GOALS
ACTIVITY GOAL
Understand security requirements and threats.
PROCESS GOAL
Detect and resolve unauthorized access.
IT GOAL
Ensure IT services can resist and recover from attacks.
BUSINESS GOAL
Maintain enterprise reputation and leadership.
MEASURE
PROCESS METRICS
IT METRICS
KPI & KGI*
BUSINESS METRICS
REALIGN
MEASURE
Frequency of review of the type of security events to be monitored.
MEASURE
Number of access violations.
MEASURE
Number of incidents with business impact.
MEASURE
Number of incidents causing public embarrass-ment.
DRIVE PERFORMANCE

* Key Performance Indicators & Key Goal Indicators

Legend			
Risk Rating		Trend	
🟩	Low	▲	Risk increasing
🟨	Medium	▼	Risk decreasing
🟥	High	■	No change

Board / Executive IT Risk Dash Board

Capability	Key Risks	Risk Level	Risk Mgm Plan	Regulatory Findings	Trend
IT Risk Management	IT risks are not defined IT risks are not managed to acceptable levels	🟥	7	5	▲
Information & Asset Inventory	Processes and procedures for classifying, labelling and handling information and assets are not managed Identification and assingment of ownership for assets containg sensitve information has not been performed.	🟨	6	3	■
Information Protection	Processes for monitoring and tracking sensitive information throughout its lifecycle is not established Failure to restrict collection of personal information for only necessary purposes	🟥	~35	~22	▲
Information Security Program Management	The information security program is not aligned with business requirements Policies and procedures have been established for information security	🟨	13	13	■
Identity & Access Management	Priviliged access is used to compromise data Terminated user access is not removed appropriately	🟥	37	34	
Threat & Vulnerability Management	Internal and external vulerabilities go unmanaged Internal and external security threats go unmanaged	🟥	~120	~76	▲
Third Party Security	Security risks are not identified with third parties Security risks are not managed to acceptable levels with third parties	🟥	39	39	▲
IT Operations	Information security practices are not integrated into IT operations (change mgm, incident mgm, etc.) IT operations are not performing their Information security responsibilities	🟨	~26	~19	■
Business Continuity & Disaster recovery	Disaster recovery processes and procedures are not defined Ability to recover from an outage has not been tested	🟥	38	34	▲
Phyiscal & Environmental Controls	Physical perimeter controls at IT facilties are not established IT environmental controls (power, temp, etc.) to support IT operations are not sufficent	🟩	20	14	■
Organization Security & Awareness	Users do not perform their security responsibiliteis Users do not understand their security responsibilities	🟨	5	4	■
IT Compliance Management	Adequate mechanisms to monitor and remediate compliance isssues are not implemented Compliance with legislative, regulatory or contractural obligations are not identified	🟨	~12	~2	■

Regular Security Reporting

- ❑ **Risk Management Program**
  - Status management program – see example next page – Dash board
  - Number of risk assessments performed – Defined assessments and analysis per IT and organization projects, to include change control.
  - Time to remediate issues – The time between identification and remediation.
- ❑ **Vulnerability Management**
  - Issues by Status – When a vulnerability is identified on a system the first time, it is a new data point that should inform and, depending on the situation, drive an action.
  - Remediation Time - Measure the length of time from identification to remediation and is a measure of the efficiency of the patch and remediation cycle.
  - Mean time to Patch – The time between identification of a needed patch and the installation of the required patch.
- ❑ **Exceptions**
  - The number of information security policy exceptions requested and granted
- ❑ **Incident Management**
  - Number of Events - Events are activities or indicators that warrant further investigation and can be indicators of incidents.
  - Number of Incidents - Incidents occur when a material event or events have occurred and require a formal response activity.
- ❑ **Specific Initiatives**
  - CMS Quality Measurements

CMS Quality Measurements - Examples

Quality Area	Quality Requirements	CMS Reference	Goal	Current Status	Accountable	Responsible
Information System Assets (Medical Devices, Server, End User Computing Devices, Databases, Software, Data)	Identify and classify all information system assets Verify assets and classification annually and obtain data owner approval	CP-2(8) SE-1	100% of All Information System Assets Classified annually and approved by data owner	70% of all Information System Assets Classified	Data Owner	CISO

Table of Contents

- ❑ Introduction
- ❑ Key IT and Cyber Risks and Opportunities
- ❑ What Risks to Audit?
- ❑ Board and Management Communication
- ➡ ❑ **Trending Best Practice/Standards and Resources**
- ❑ Conclusion
- ❑ Q&A

Resources

- ❑ **AHIMA**
  - ▪ Information Governance Framework http://www.ahima.org/topics/infogovernance
- ❑ **AAMI**
  - ▪ TIR57: Principles for medical device security—Risk management www.aami.org
  - ▪ TIR97: Principles for medical device - Post-market security management for device manufactures (in development)
- ❑ **Bipartisan Policy Center**
  - ▪ Patient Safety and Information Technology: Improving Information Technology's Role in Providing Safer Care https://bipartisanpolicy.org/library/patient-safety-and-information-technology-improving-information-technologys-role-in-providing-safer-care
- ❑ **The Center for Internet Security (CIS)**
  - ▪ Critical Security Controls for Effective Cyber Defense v6.1 https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf
  - ▪ Regular updates OS security standards.
- ❑ **Center for Disease Control and Prevention (CDC) and HHS**
  - ▪ Healthcare Organization and Hospital Discussion Guide for Cybersecurity https://www.cdc.gov/phpr/healthcare/documents/healthcare-organization-and-hospital-cyber-discussion-guide.pdf
- ❑ **Cloud Security Alliance**
  - ▪ Cloud Controls Matrix version 3 September 2016 https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
- ❑ **CRICO**
  - ▪ Malpractice-Risks-Associated-with-Electronic-Health-Records https://www.rmf.harvard.edu/Clinician-Resources/Article/2017/Malpractice-Risks-Associated-with-Electronic-Health-Records?
- ❑ **CMS**
  - ▪ Recommendations to Providers Regarding Cyber Security January 13, 2017
  - ▪ Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers September 2016 https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Core-EP-Rule-Elements.html

Resources

- **FFIEC**
  - Information Security Booklet Released September 2016
  - Cyber security assessment framework https://www.ffiec.gov/cyberassessmenttool.htm
- **Healthcare Industry Cybersecurity Taskforce (HHS)**
  - Report on improving cybersecurity in the healthcare industry https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
- **HHS – Agency for Healthcare Research and Quality**
  - 2017 NATIONAL HEALTHCARE QUALITY AND DISPARITIES REPORT
  - https://www.ahrq.gov/research/findings/nhqrdr/chartbooks/patientsafety/index.html?utm_source=ahrq&utm_medium=en3&utm_term=&utm_content=3&utm_campaign=ahrq_en8_15_2017#_blank
- **HITRUST Updates**
  - CSFBASICs: Streamlined versions of the HITRUST CSF and supporting HITRUST CSF Assurance Program designed to help small and lower-risk healthcare organizations
  - Privacy
  - AICPA Trust Principles and Criteria for security, confidentiality and availability
  - HITRUST De-Identification Framework's assessment protocol for contextual data de-identification.
  - The addition of the Center for Internet Security Critical Security Controls (CIS CSC) v6,
  - Cybersecurity guidance from the President's Precision Medicine Initiative (PMI)
  - OCR Audit Protocol v2
  - FEDRAMP Support for Cloud and IaaS Service Providers
  - FFIEC IT Examination Handbook for Information Security.
- **Joint Commission.**
  - Sentinel event alert #54: safe use of health information technology. Oakbrook Terrace, IL: Joint Commission; 2015; Available from: www.jointcommission.org/safehealthit .
  - Sentinel event alert #42: Safely implementing health information and converging technologies. Joint Commission; 2008; Available from: www.jointcommission.org/safehealthit

Resources

- ❑ **NACD – National Association of Corporate Directors**
  - ▪ 2017 Cyber Risk Oversight http://boardleadership.nacdonline.org/Cyber-Risk-Handbook-GCNews.html
- ❑ **NIST**
  - ▪ Cybersecurity Framework - Framework for Improving Critical Infrastructure Cybersecurity version 1.1 January 2017
  - ▪ Cybersecurity Resource Center Beta https://beta.csrc.nist.gov/
  - ▪ Guide for Cybersecurity Incident Recovery https://beta.csrc.nist.gov/publications/detail/itl-bulletin/2017/02/guide-for-cybersecurity-incident-recovery/final
  - ▪ Baldridge Cybersecurity Excellence Builder https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf
- ❑ **ONC – Health IT**
  - ▪ Report of the evidence on Health IT Safety and interventions May 2016
  - ▪ SAFER Guides - https://www.healthit.gov/safer/
  - ▪ EHR Contracts Untangled SELECTING WISELY, NEGOTIATING TERMS, AND UNDERSTANDING THE FINE PRINT September 2016 https://www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf
  - ▪ How to Identify and Address Unsafe Conditions Associated with Health IT
  - ▪ The Role of Health IT Developers in Improving Patient Safety in High Reliability Organizations

- ❑ **ONC and OCR Office of Civil Rights (OCR)/HHS**
  - ▪ Security Risk Assessment – Small and Medium Entities https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
- ❑ **OCR**
  - ▪ HIPAA Audit Program (Privacy, Breach and Security)
- ❑ **Security Culture Framework https://securitycultureframework.net/**

Table of Contents

- ❑ Introduction
- ❑ Key IT and Cyber Risks and Opportunities
- ❑ What Risks to Audit?
- ❑ Board and Management Communication
- ❑ Trending Best Practice/Standards and Resources
- ❑ **Conclusion**
- ❑ Q&A

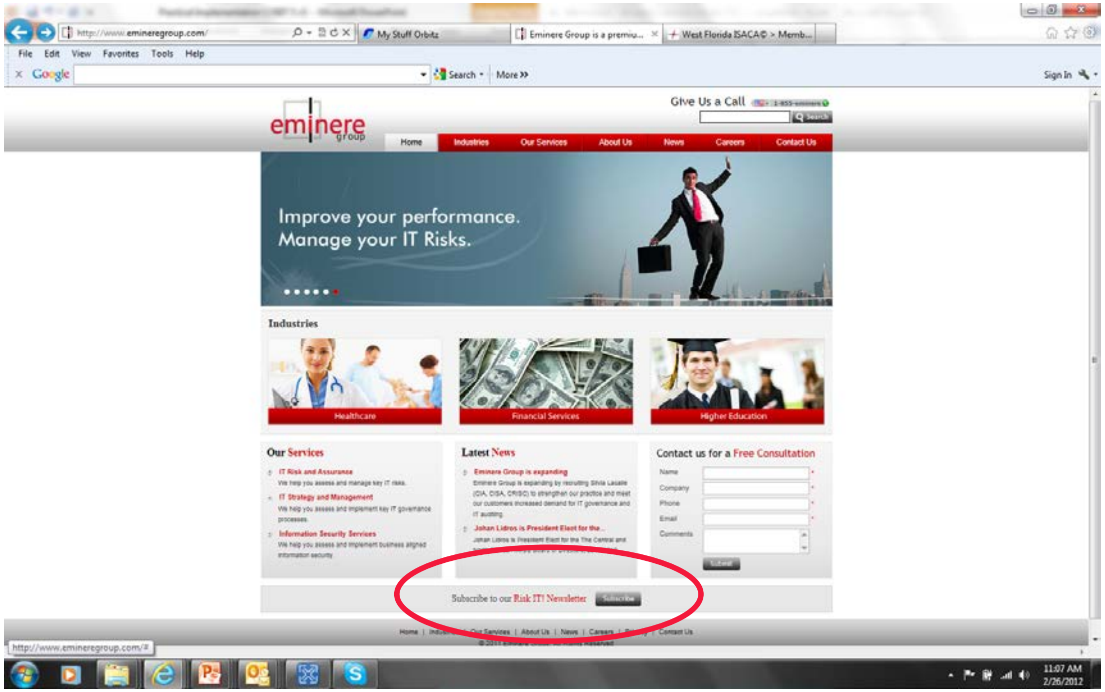
Conclusion

- ❑ **Risk based Long Term Audit Plan**
  - ▪ Health IT
  - ▪ Key Controls
  - ▪ Operational efficiency
- ❑ **Drive Measurements and Metrics**
  - ▪ Board and Management discussions
  - ▪ Audits
- ❑ **Several good practices and standards exist to guide you in most areas**

Questions?

Ongoing IT Governance and Risk Updates

- ❑ **Interested in on-going IT Governance and IT Security updates?**
  - Sign up for our weekly newsletter “RiskIT “at www.emineregroup.com



Improve your performance.
Manage your IT Risks.

Our Services

- **IT Risk and Assurance**
  We help you assess and manage key IT risks.
- **IT Strategy and Management**
  We help you assess and implement key IT governance processes.
- **Information Security Services**
  We help you assess and implement business aligned information security

Latest News

- **Eminere Group is expanding**
  Eminere Group is expanding by recruiting Silvia Lasalle (CIA, CISA, CRISC) to strengthen our practice and meet our customers increased demand for IT governance and IT auditing
- **Johan Lidros is President Elect for the...**
  Johan Lidros is President Elect for the The Central and [illegible]

Contact us for a Free Consultation

Subscribe to our Risk IT! Newsletter

© 2011 Eminere Group. All Rights Reserved

For questions please contact

❑ **Johan Lidros**

- Johan.lidros@emineregroup.com
- w (813) 832-6672 x9101
- c (813) 355-6104