Top IT and Cyber Risks to include in your Audit Plan: 2020 Update

HCCA – Compliance Institute
March 30, 2020
Nashville, TN

1

Today's 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

2

Table of Contents

- Introduction
- Key IT and Cyber Risks to Audit
- Board and Management Communication
- Best Practices and Additional Resources
- Wrap-up and Q&A

3

Objectives

- **You will learn:**
  - The latest key IT and Cyber Risks you need to monitor and audit;
  - How to discuss IT and Cyber Risks with management, and
  - How to turn IT and Cyber Risks into opportunities.
- **We will share:**
  - Trending IT governance and security best practices;
  - Accepted industry standards, and
  - Sources for further research.
- **Your Questions!** We welcome your questions – don't save them for the end!

4

4

Introduction

- Information technology (IT) is critically important for healthcare organizations.
- The complexity and rate of change of technology can dramatically impact risk and compliance.
- The latest IT and cyber threats can challenge a healthcare provider's ability to deliver quality outcomes.
- Improvements in IT Governance can help prepare organizations for to manage Health IT and traditional IT risks
- A wealth of best practices and industry standards are available to help healthcare organizations improve their cyber-security, IT Audit and IT Risk compliance.

5

Healthcare System Challenges

IT Drivers (examples)

- Homecare, Telehealth, Personal Health Devices
- Automation and Digitalization of Processes
- Automation of Algorithms (ML/AI)

Technology offers powerful tools, but is not – by itself – the solution!

- Availability of and Access to Care
- Affordability of Care
- Quality of Care

Patient Trust and Safety

IT Security is an Enabler

- Confidentiality, Integrity, Availability
- System Reliability and Usability
- Compliance and Privacy Enablement

Cybersecurity can be an enabler – but is often seen as an inhibitor!

6

Common Attack Vectors-Weakest Link

- Email
- Authentication
- Privileged Accounts
- Web Application

Equifax Breach – What happen?

Equifax Process and Control Failures

1. No asset inventory (CSC01
2. No software inventory (CSC02)
3. No file integrity monitoring
4. No network segmentation
5. Broken SSL Visibility Appliance
6. Broken SSLV failed open
7. SSLV lacked certs for key systems
8. SAST failed to find Struts (user error)
9. No anomaly detection on web servers
10. Custom snort rule didn't work
11. Custom snort rule wasn't tested.
12. Network scanner didn't find Struts
13. Failed to detect webshells
14. Failed to detect interactive activity
15. File with cleartext creds accessible
16. Additional database access
17. DB queries were not restricted
18. No DB anomaly monitoring
19. No field-level encryption in DBs
20. No data exfiltration detection
21. DAST scanning failed to detect vulns
22. Ineffective IR plan/procedures
23. No owners assigned to apps or DBs
24. Comms issues due to corp structure
25. Lack of accountability in processes
26. Patching process lacked follow up
27. Old audit findings were not addressed
28. Insecure NFS configs
29. Logs retained for less than 30 days

- https://www.databreachtoday.com/blogs/learn-from-how-others-get-breached-equifax-edition-p-2870?rf=2020-02-13

Maersk – notpetya – World Forum Davos

"It cost us between 250-300 million dollars, and yet I argue it was a very important wake-up call…."

"Average is not good enough… "

"stop being naïve…"

"we have to be pro-active… "

"need for radical improvement of infrastructure for all organizations… "

- https://www.youtube.com/watch?v=VaqIYlYmDbA

9

9

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;*
    - *Significant risks are identified and assessed;*
    - *Appropriate risk responses are selected that align risks with the organization's risk appetite; and*
    - *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.*

10

10

Table of Contents

11

Health IT - Definition

- The term "Health IT" is broadly used currently and refers to an array of technologies to store, share, and analyze health information.

"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."

Office for the National Coordinator of Health Information Technology

12

12

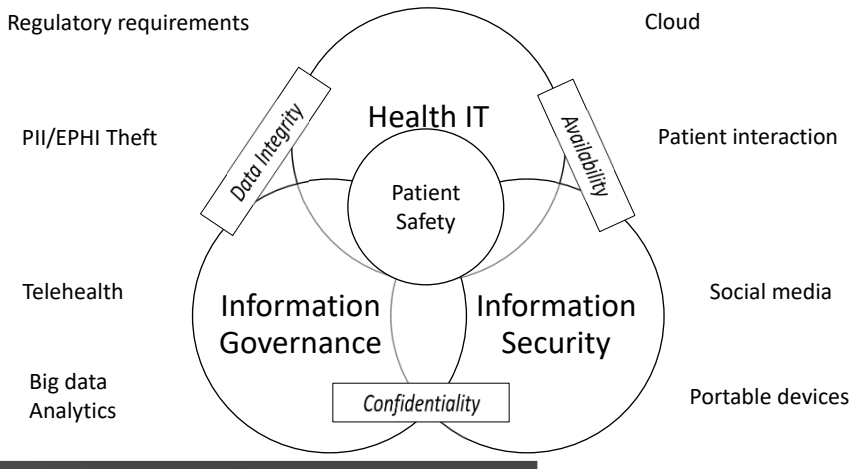
Typical Health IT Systems

Health IT Systems	Example
Administrative/billing or practice management system	• Coding/billing system • Master patient index • Registration/appointment scheduling system
Automated dispensing system	• Medication dispensing cabinet
Computerized medical devices	• Infusion pumps with dose-error-reduction capability • Patient monitoring systems (e.g., cardiac, respiratory, fetal)
Electronic health record (EHR) or EHR component	• Bar-coded medication administration • Clinical decision support system • Clinical documentation system (e.g., progress notes) • Computerized provider order entry • Pharmacy system
Human interface device	• Keyboard, • Monitor/display/Touchscreen • Mouse • Speech recognition system
Laboratory information system	• Microbiology system • Pathology system • Test results
Radiology/diagnostic imaging system	• Picture archiving and communication system

13

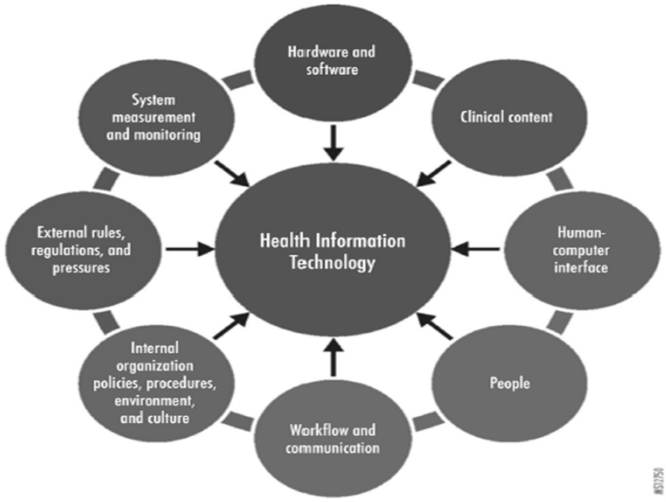
13

Key Drivers Impacting Health IT



14

Health IT – Enterprise Impact



15

Healthcare IT Characteristics

- Diversified IT environment
- Medical Devices/Biomedical/Health Technology and IT systems coming together
- EMR and HIE are changing the IT environment – Still…
- Location of healthcare services provided
  - On-site
  - Telehealth
  - Internet of Things
- Cloud is getting common and more outsourcing
- Many regulatory requirements and more to come….
- Constantly new and changing threats/risks related to the use of technology
- The "value" of information
- Immature IT/Information Security

16

16

Typical Key IT Risks

Risk List	Risk List	Risk List
1. Vendor/Supplier Management	13. Data Warehouse and Other Data Repositories	25. PCI-DSS Compliance
2. Change Management	14. Internal and External Intrusion	26. Problem and Incident Management
3. Identity and Access Management	15. IT Governance / IT Security Governance	27. Resources and IT Skills
4. EPHI Inventory and IT Asset Management	16. Business Continuity (Downtime)	28. Roles and Responsibilities
5. Network Availability	17. Disaster Recovery and Backup Management	29. Facility/Utility Systems
6. Electronic Communication (Email, Texting, Faxing)	18. Disposal of Electronic Media	30. Grants w. IT Security Requirements / Research (CMMC, DFARS, etc.)
7. IT Risk Management	19. Security Incident Management	31. Cybersecurity
8. Medical Devices/Health Technology	20. Information/Data Governance	32. IT Cost
9. Phone Systems	21. Patch management	33. Affiliated Organizations
10. Security Awareness	22. Physical Security, IT Environmental Controls	34. Telehealth
11. Internet Usage and Social Media	23. End-User Devices (Workstations, Tablets, Laptops, USBs, Smart phones, etc.)	35. Privacy/GDPR/State Privacy, etc.
12. Audit Trail and Logs	24. IoT	

17

Top 10 Health Technology Hazards– ECRI 2020

1. Misuse of Surgical Staplers
2. Adoption of Point-of-Care Ultrasound Is Outpacing Safeguards
3. Infection Risks from Sterile Processing Errors in Medical and Dental Offices
4. Hemodialysis Risks with Central Venous Catheters—Will the Home Dialysis Push Increase the Dangers?
5. Unproven Surgical Robotic Procedures May Put Patients at Risk
6. Alarm, Alert, and Notification Overload
7. Cybersecurity Risks in the Connected Home Healthcare Environment
8. Missing Implant Data Can Delay or Add Danger to MRI Scans
9. Medication Errors from Dose Timing Discrepancies in EHRs
10. Loose Nuts and Bolts Can Lead to Catastrophic Device Failures and Severe Injury

18

18

Health IT Risks – ECRI 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

Polling Question #1

- What is your organization's top IT Risk Challenge? Select your top 3.

A. Privacy – GDPR, CCPA – California Consumer Privacy Act (Jan 1, 2020)
B. IT Governance
C. Identity & Access Management (IAM)
D. Cyber Risk/Network Security
E. Medical Devices Management / IOT/ Health Technology
F. Business Continuity / Disaster Recovery
G. Mobile Devices - BYOD
H. IT Vendor Management
I. Security Awareness / Phishing
J. Blockchain
K. Others. Please list

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/Cybersecurity
- PCI
- Mobile Device Management
- Patch Management
- New Systems
- Privacy

Polling Question #2

What is your most critical System?

A. EMR

B. Financial System

C. Pharmacy

D. Data Warehouse

E. PACS

F. Password/Encryption key vault

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
- Departmental IT

Added Value Audits – Hidden Opportunities

- Life Cycle Management
  - Application/Tool functionality
  - Inventories
  - Cost
  - Age
  - Utilization, ownership
  - Budget/capacity/acquisition processes
- Identity and Access management
  - Number of systems
  - Authentication
  - Resources for management of access management (FTE/cost)
- IT Value/IT Cost
  - You cannot manage what you do not measure!

IT Audit Plan Considerations

- Comprehensive IT Risk Assessment
- Build Long Term IT Audit Plan
- IT Governance Audit
- 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 – Key Component for Effective and Efficient IT Risk Management

25

Table of Contents

26

Discussion Areas with Management / Board – Tone from the To

- Health IT
- IT Governance
- Information Governance
- Information Security
- IT Standards
- Measurements and Metrics

Board

- **It Pays to Have a Digitally Savvy Board – MIT White paper**

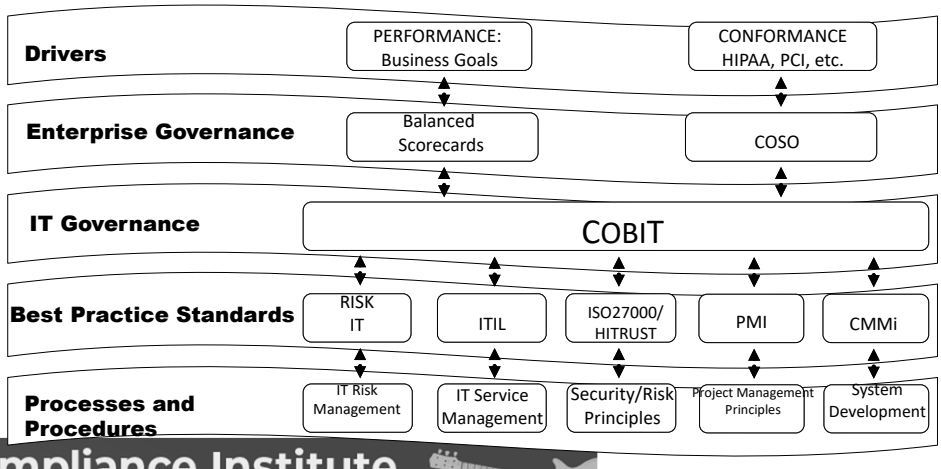
Magazine: Spring 2019 Issue Research Highlight March 12, 2019 Reading Time: 10 min https://sloanreview.mit.edu/article/it-pays-to-have-a-digitally-savvy-board/

Actions to Reduce Risk

- Leadership
  - Governance !!!
  - Multidisciplinary Involvement
  - Vendor selection and Involvement
  - Change management
  - Control effectiveness and efficiency
- Safety culture and process improvement
  - Comprehensive system analysis/risk assessments/failure mode and effects analysis
  - Shared involvement and responsibility
  - System implementation and upgrades

29

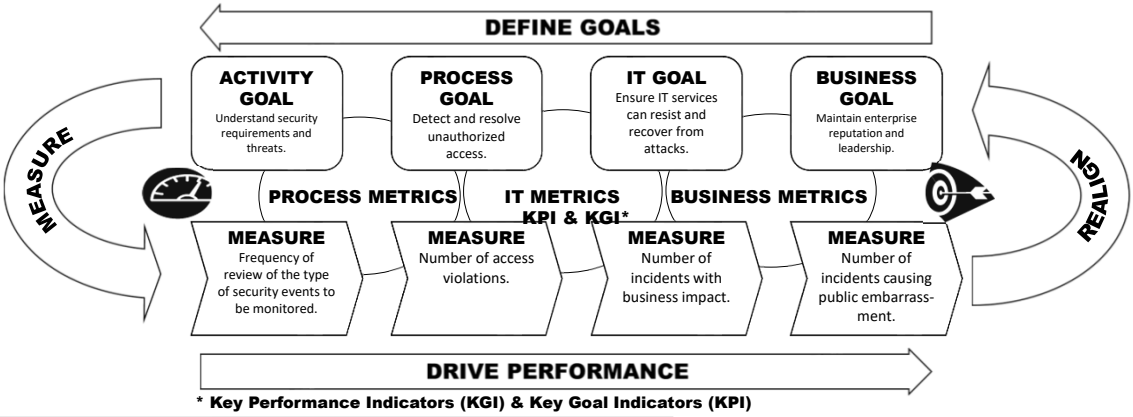
IT Governance Framework



30

IT Goals and Metrics-Key Performance Indicators & Key Goal Indicators

You cannot manage what you do not measure!



* Key Performance Indicators (KGI) & Key Goal Indicators (KPI)

31

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 assignment of ownership for assets containing sensitive 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	Privileged access is used to compromise data Terminated user access is not removed appropriately		37	34	△
Threat & Vulnerability Management	Internal and external vulnerabilities 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 mgmt., 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	▭
Physical & Environmental Controls	Physical perimeter controls at IT facilities are not established IT environmental controls (power, temp, etc.) to support IT operations are not sufficient		20	14	▭
Organization Security & Awareness	Users do not perform their security responsibilities Users do not understand their security responsibilities		5	4	▭
IT Compliance Management	Adequate mechanisms to monitor and remediate compliance issues are not implemented Compliance with legislative, regulatory or contractual obligations are not identified		~12	~2	△

Legend	
Risk Rating	Trend
Low	▲ Risk increasing
Medium	▼ Risk decreasing
High	▬ No change

32

32

Regular Security Reporting

- **Risk Management Program**
  - Status management program – see example previous 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**
  - Program/projects

CMS Quality Measurements and Metrics - 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 and approved by data owner.	Data Owner	CISO

Polling Question #3

- How confident are you that you are providing executive leadership sufficient information to help them manage IT Risk?
  - Very Confident
  - Confident
  - Not Very Confident
  - Unsure

35

35

Polling Question 4

- Who should approve your IT risk management dashboard?
  a) CIO
  b) Board
  c) Executive Management
  d) All

36

Table of Contents

37

News on Standards

- NIST Privacy Framework
- TIR97 – Biomedical devices
- Pre-market Requirements for Medical Device Cybersecurity – Health Canada
- Core Cybersecurity Feature Baseline 2 for Securable IoT Devices – NIST 8529
- COSO INTERNAL CONTROL – INTEGRATED FRAMEWORK: An Implementation Guide for the Healthcare Provider Industry
- NACD – A Board Primer on Block Chain
- Essential Eight Maturity Model – Australian Cyber Security Center
- Penetration Testing for the Financial Industry GFMA, SIFMA, AFME, ASIFMA
- The Healthcare and Public Health Sector Coordinating Council (HSCC) – Several papers
- NIST -Identifying and Protecting Assets Against Ransomware and Other Destructive Events.
- https://www.healthit.gov/playbook/

38

38

Health IT Playbook

39

39

Resources

- Research Findings: Technology and Clinician Cognitive Overload – Easing the Pain. – HIMSS Analytics

40

40

Resources

- AAMI www.aami.org
  - TIR57: Principles for medical device security—Risk management
  - TIR97: Principles for medical device - Post-market security management for device manufactures
  - AAMI Medical Device Cybersecurity – A guide for HTM professional
- The Center for Internet Security (CIS)
  - Critical Security Controls for Effective Cyber Defense https://www.cisecurity.org/controls/
  - 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 v3 https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
  - Top Threats to Cloud Computing: Deep Dive
  - OWASP Secure Medical Device Deployment Standard
- CMS
  - CMS Acceptable Risk Safeguards (ARS) Includes detailed privacy and security controls mapped to HIPAA, and NIST
  - https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication
  - 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

- ISACA
  - COBIT – Leading IT Governance Framework
- FDA
  - Management of Cybersecurity in Medical Devices – Guidance for Industry and FDA Staff https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
- Healthcare Industry Cybersecurity Taskforce (HHS)
  - Report on improving cybersecurity in the healthcare industry https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
- Healthcare & Public Sector Coordinating Council (HSCC) with HSCC Joint Cybersecurity Working Group (JCWG)
  - MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN https://healthsectorcouncil.org/the-joint-security-plan/
  - Healthcare Industry Cybersecurity Practices https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx
- HITRUST
  - www.hitrustalliance.net
- MDiSS Medical Device Innovation, Safety and Security Consortium
  - MDISS Tool – security risk assessment medical devices Tool MDRAP https://mdrap.mdiss.org

Resources

- NACD – National Association of Corporate Directors
  - 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 https://csrc.nist.gov/
  - Core Cybersecurity Feature Baseline 2 for Securable IoT Devices – NIST 8529
  - NIST Privacy framework 1.0 privacy framework
  - IT Security Architecture to protect from Ransomware
  - Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. see: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events,
- ONC – Health IT
  - SAFER Guides - https://www.healthit.gov/safer/
  - 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
  - Health IT Playbook https://www.healthit.gov/playbook/
- OCR
  - HIPAA Audit Program (Privacy, Breach and Security)
- Penetration Testing for the Financial Industry GFMA, SIFMA, AFME, ASIFMA
  - https://www.sifma.org/cybersecurity-resources/
- Secured Culture Framworkd
  - Security Awareness Framework https://securityculturefra mework.net/
- Shared Assessments/BITS
  - IT Vendor Management. First developed for Financial industry now general vendor management and other industries including healthcare. https://sharedassessments.org/

Table of Contents

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??

Key weekly updates

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

47

Contact Johan

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

48