Copyright Notice

Legal Disclaimer

Legal Disclaimer. This information does not constitute legal advice and is for educational purposes only. This information is based on current federal law and subject to change based on changes in federal law or subsequent interpretative guidance. Since this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource regarding the matters covered, and may not be tailored to your specific circumstance. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND ADVICE PROVIDED HEREIN IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE. The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.

Information Risk Management Essentials

March 17, 2015

Kathy Jobes
Chief Information Security Officer
(757) 252-0637
kejobes@sentara.com
Sentara Healthcare

Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US
CEO
800-704-3394
bob.chaput@ClearwaterCompliance.com
Clearwater Compliance LLC

3

Discussion Flow

1. Introduction - Bob
2. Setting / Situation / Challenges - Kathy
3. Turning Point (Information Risk Management Maturity) – Kathy & Bob
4. Call to Arms – Kathy & Bob

CLEARWATER COMPLIANCE

SENTARA HEALTHCARE

”First, Do No Harm.”

-Hippocrates, 4th Century, B.C.E.

OR

-Auguste François Chomel (1788–1858),
Parisian pathologist and clinician

It’s a Patient Safety / Quality of Care *Journey* …
Not a HIPAA Compliance *Destination*

Discussion Flow

1. Introduction - Bob
2. Setting / Situation / Challenges - Kathy
3. Turning Point (Information Risk Management Maturity) – Kathy & Bob
4. Call to Arms – Kathy & Bob

Sentara Background

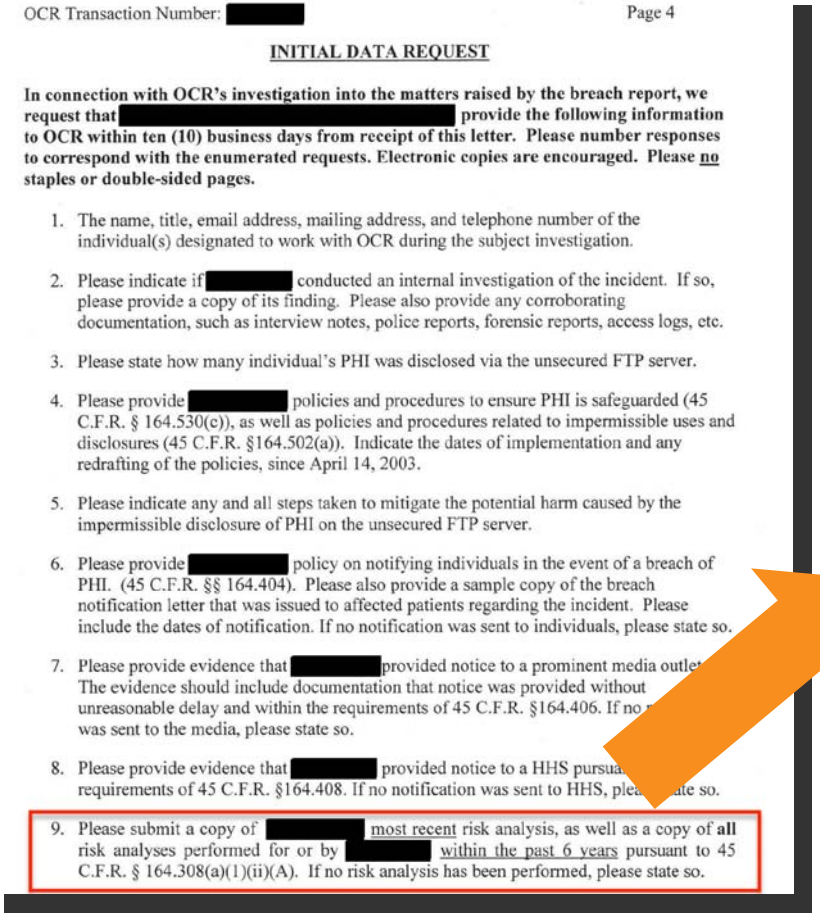
- 125-year not-for-profit history
- Headquartered in Norfolk, VA Sentara includes 12 hospitals, 5 medical groups, 3,800-provider medical staff, Optima Health plan, Advanced imaging centers, Home health and hospice, Nightingale air ambulance, Rehab and therapy centers, Nursing and assisted living centers
- Ranked as one of the nation's top integrated healthcare systems by Modern Healthcare magazine for more than a decade.

Complexity, High-Growth, Lots of End Points

8

Setting / Situation

1. Narrowly Focused IT Security Efforts
2. Silo-ed Risk Assessment approach: business line / focus area
3. Multiple Roles & Hats: Care Provider, Health Plan, Business Associate, Vendor
4. Increasing Participation in Federal Programs
5. Meaningful Use Attestations



OCR Transaction Number: [redacted] Page 4

INITIAL DATA REQUEST

In connection with OCR's investigation into the matters raised by the breach report, we request that [redacted] provide the following information to OCR within ten (10) business days from receipt of this letter. Please number responses to correspond with the enumerated requests. Electronic copies are encouraged. Please no staples or double-sided pages.

1. The name, title, email address, mailing address, and telephone number of the individual(s) designated to work with OCR during the subject investigation.
2. Please indicate if [redacted] conducted an internal investigation of the incident. If so, please provide a copy of its finding. Please also provide any corroborating documentation, such as interview notes, police reports, forensic reports, access logs, etc.
3. Please state how many individual's PHI was disclosed via the unsecured FTP server.
4. Please provide [redacted] policies and procedures to ensure PHI is safeguarded (45 C.F.R. § 164.530(c)), as well as policies and procedures related to impermissible uses and disclosures (45 C.F.R. §164.502(a)). Indicate the dates of implementation and any redrafting of the policies, since April 14, 2003.
5. Please indicate any and all steps taken to mitigate the potential harm caused by the impermissible disclosure of PHI on the unsecured FTP server.
6. Please provide [redacted] policy on notifying individuals in the event of a breach of PHI. (45 C.F.R. §§ 164.404). Please also provide a sample copy of the breach notification letter that was issued to affected patients regarding the incident. Please include the dates of notification. If no notification was sent to individuals, please state so.
7. Please provide evidence that [redacted] provided notice to a prominent media outlet The evidence should include documentation that notice was provided without unreasonable delay and within the requirements of 45 C.F.R. §164.406. If no was sent to the media, please state so.
8. Please provide evidence that [redacted] provided notice to a HHS pursua requirements of 45 C.F.R. §164.408. If no notification was sent to HHS, plea ate so.
9. Please submit a copy of [redacted] most recent risk analysis, as well as a copy of **all** risk analyses performed for or by [redacted] within the past 6 years pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(A). If no risk analysis has been performed, please state so.

CLEARWATER COMPLIANCE

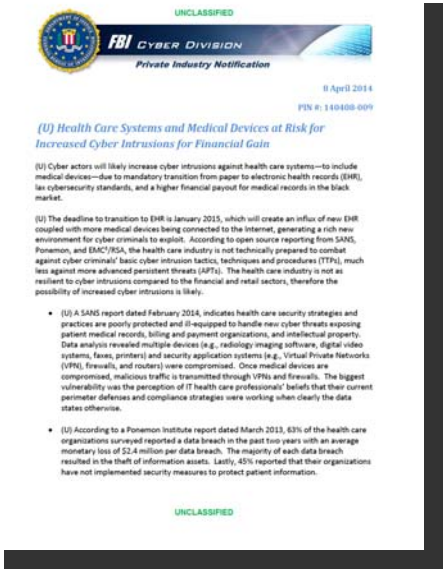
SENTARA HEALTHCARE

*"9. Please submit a copy of XYZ Hospital's most recent risk analysis, as well as a copy of **all** risk analyses performed for or by copy XYZ Hospital within the past 6 years pursuant to 45 C.F.R. § 164.308(a)(l)(ii)(A). If no risk analysis has been performed, please state so.*

10

Recent FBI Healthcare Alerts: April / August 2014

"Because the healthcare industry is not as "resilient to cyber intrusions [as] the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely"



UNCLASSIFIED

FBI CYBER DIVISION

Private Industry Notification

8 April 2014

PIN #: 140408-009

(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain

(U) Cyber actors will likely increase cyber intrusions against health care systems—to include medical devices—due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market.

(U) The deadline to transition to EHR is January 2015, which will create an influx of new EHR coupled with more medical devices being connected to the Internet, generating a rich new environment for cyber criminals to exploit. According to open source reporting from SANS, Ponemon, and EMC²/RSA, the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.

- (U) A SANS report dated February 2014, indicates health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property. Data analysis revealed multiple devices (e.g., radiology imaging software, digital video systems, faxes, printers) and security application systems (e.g., Virtual Private Networks (VPN), firewalls, and routers) were compromised. Once medical devices are compromised, malicious traffic is transmitted through VPNs and firewalls. The biggest vulnerability was the perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise.
- (U) According to a Ponemon Institute report dated March 2013, 63% of the health care organizations surveyed reported a data breach in the past two years with an average monetary loss of $2.4 million per data breach. The majority of each data breach resulted in the theft of information assets. Lastly, 45% reported that their organizations have not implemented security measures to protect patient information.

UNCLASSIFIED

"…observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

FBI FLASH

FBI LIAISON ALERT SYSTEM

#A-000039-TT

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607.

SUMMARY

The FBI is providing the following information with HIGH confidence. The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.

TECHNICAL DETAILS

The FBI has received the following information pertaining to a recent intrusion into a health care system that resulted in data exfiltration. Though the initial intrusion vector is unknown, we believe that a spear phish email message was used to deliver the initial malware. Typically, these actors use Information Technology themed spear phishing messages which contain a malicious link that may connect to a new VPN site/service/client or a new Webmail site/software. Once access is obtained, the actors may collect and use legitimate account credentials to connect to the targeted system, usually through VPN.

The following are indicators of possible compromise:

Network-Based Indicator

Outgoing traffic through standard HTTP/HTTPS ports 80, 443 (and possibly others), but obfuscates traffic by XORing the traffic with 0x36. The below is a SNORT signature related to this activity:

alert tcp any any -> any any (content:"|66|"; depth: 1; content:"|36 36 36 58 36 36 36|"; offset: 3; depth: 7; msg: "Beacon C2"; sid: 1000000001; rev:0)

Host-Based Indicator

The malware runs as a Windows service "RasWmi (Remote Access Service)" from the malicious .dll C:\Windows\system32\system\rasemi.dll. The implant is installed from an executable file (the file has been observed under a variety of names) which drops the rasemi.dll file into the same directory and sets it to run as a service.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at either your local CTF or FBI CYWATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937

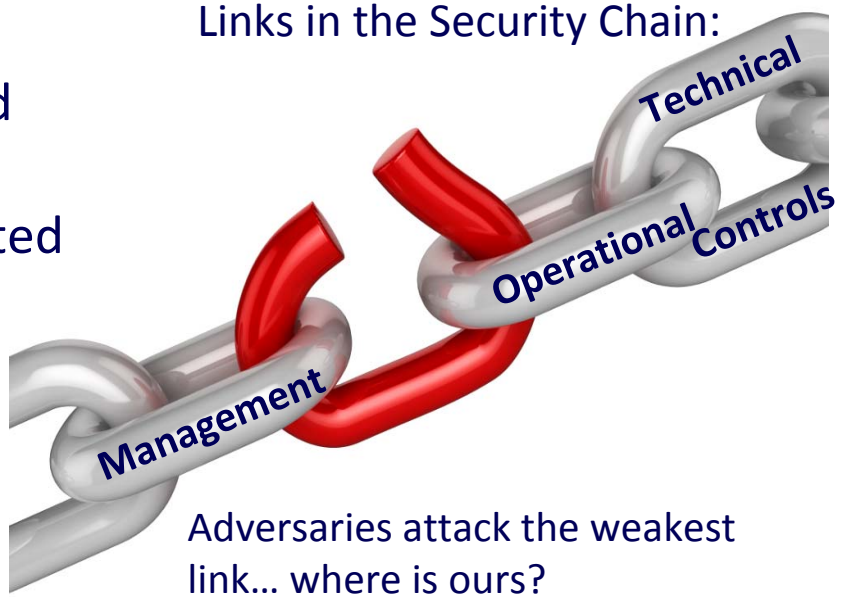
UNCLASSIFIED

Healthcare is the Next Cyber Security Battleground

Priorities / Challenges – December 2013

1. ***Un-quantified Risk = Undefined Risk Tolerance***
2. Distributed Security Functions and Responsibilities
3. Flat Landscape: Everything is treated Equal
4. Framework and Strategy
5. Information Security Integration: business, workforce, organization risk
6. Governance

Links in the Security Chain:



Adversaries attack the weakest link… where is ours?

12

Discussion Flow

1. Introduction - Bob
2. Setting / Situation / Challenges - Kathy
3. Turning Point (Information Risk Management Maturity) – Kathy & Bob
4. Call to Arms – Kathy & Bob

Turning Point – Q4 2014

1. Set Strategy and Vision
2. Identified and Vetted Candidate Partners
3. Choose Partner with Compatible Vision / Strategy to Create a Platform and "Teach Us How to Fish"
4. Adopted NIST Framework

Here's What We Heard You Say

- **Looking for a Partner to Implement Phases and Make Organization Self-Sufficient:**
  - I. PARTNER TO DO ONE FOCUSED RISK ASSESSMENT;
    - *A. SHOULDER TO SHOULDER-AND-OJT-/-KNOWLEDGE-TRANSFER-*
    - *B. FOCUSED-ON-FACILITY-OR-REGION-*
  - II. PARTNER TO ASSESS / REVIEW / GUIDE ✎ Teach us how to fish…
  - III. WITHIN 2014, TAKE LEAD IN FULL-BLOWN RA ON ENTERPRISE DATA CENTER ✎ Repeat I.
    - *A. MOVING-NOW,-SO-MUST-POSTPONE-UNTIL-MOVE-COMPLETE*

7

Embraced Information Risk Management Capability Advancement Model™ (IRMCAM™)

Actions Taken

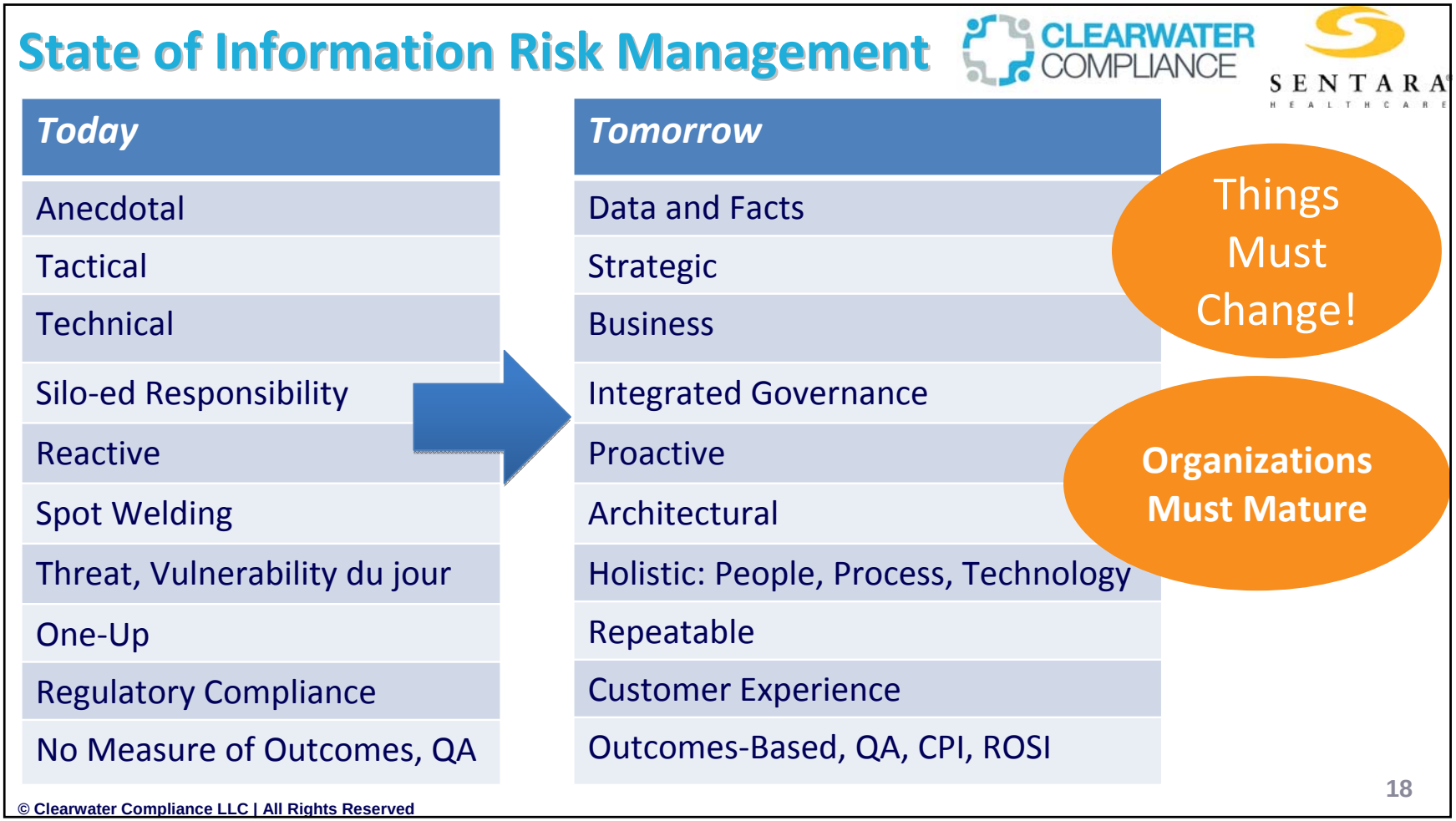
1. Assigned Responsibility and Authority
2. Formed Clearwater Partnership
3. Defined Program Elements: categorize, select, implement, assess, authorize, monitor (begin again)
4. Centralized Documentation
5. Standardized Tracking and Reporting Protocols
6. Engaged Leadership
7. ***Assessed Maturity Level***

Outcomes

1. Completed Bona Fide Risk Analyses:
   A. 11 Hospitals
   B. 133 EPs
2. Added Staff
3. Knowledge Transfer Started
4. Reporting Format Created
5. Established Governance
6. Executive Dashboard Under Development

Discussion Flow

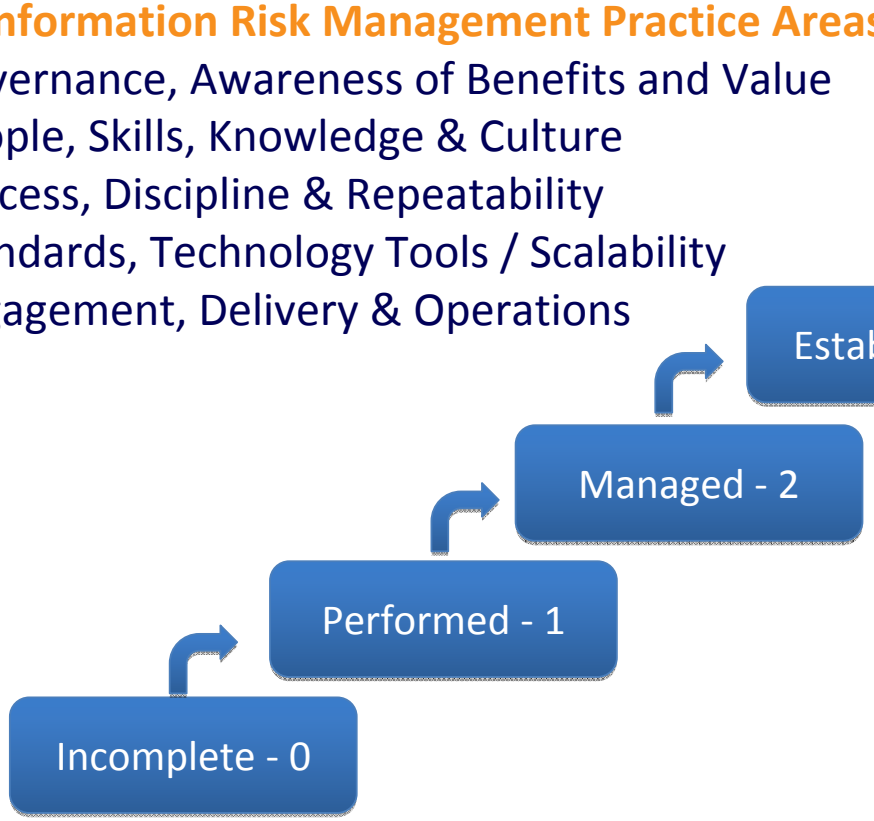
1. Introduction - Bob
2. Setting / Situation / Challenges - Kathy
3. Turning Point (Information Risk Management Maturity) – Kathy & Bob
4. Call to Arms – Bob



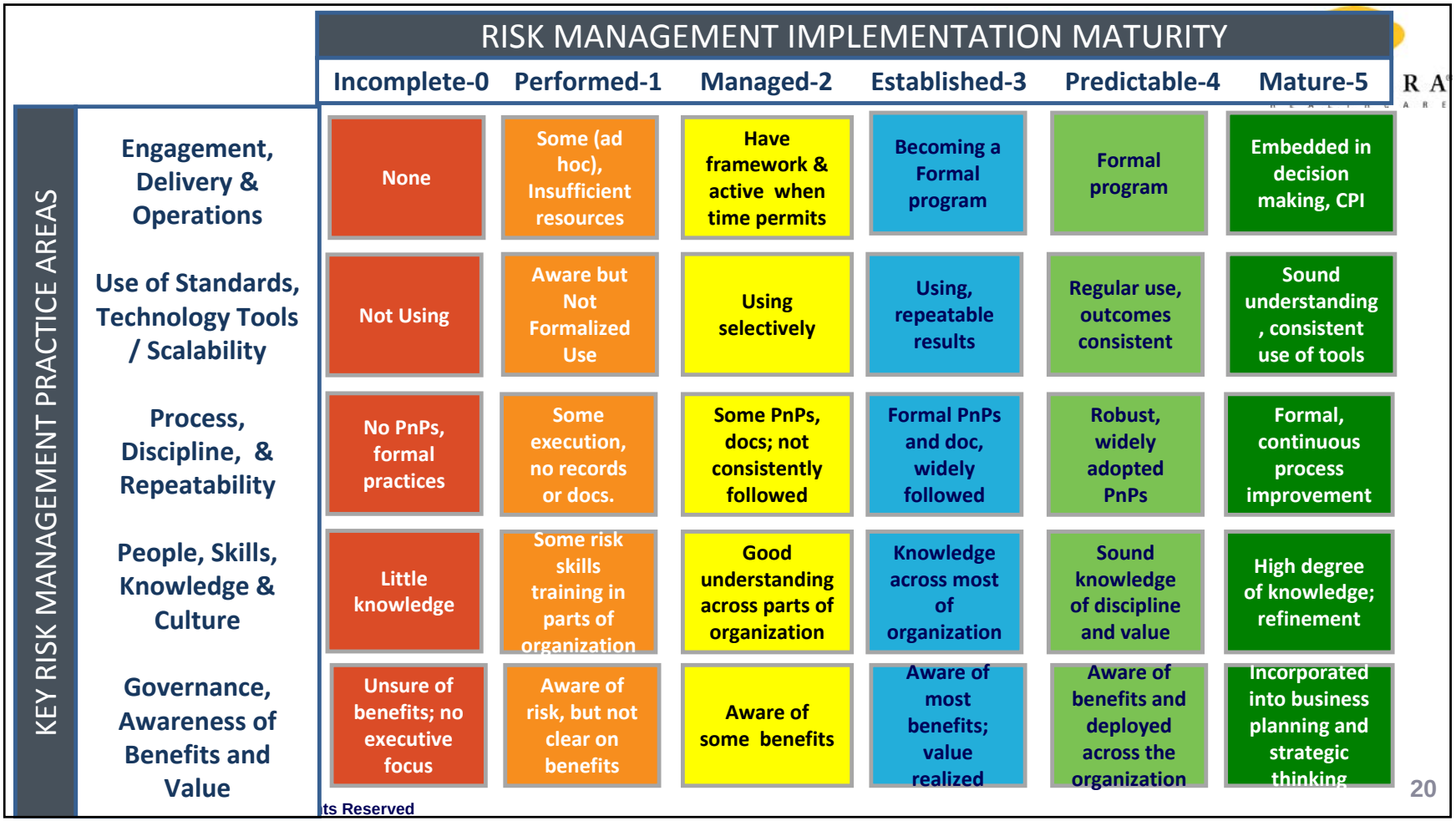
IRMCAM Index (IRMCAMi™) and Levels

Key Information Risk Management Practice Areas:

1. Governance, Awareness of Benefits and Value
2. People, Skills, Knowledge & Culture
3. Process, Discipline & Repeatability
4. Standards, Technology Tools / Scalability
5. Engagement, Delivery & Operations



As measured by the extent of adoption, implementation and / or achievement…



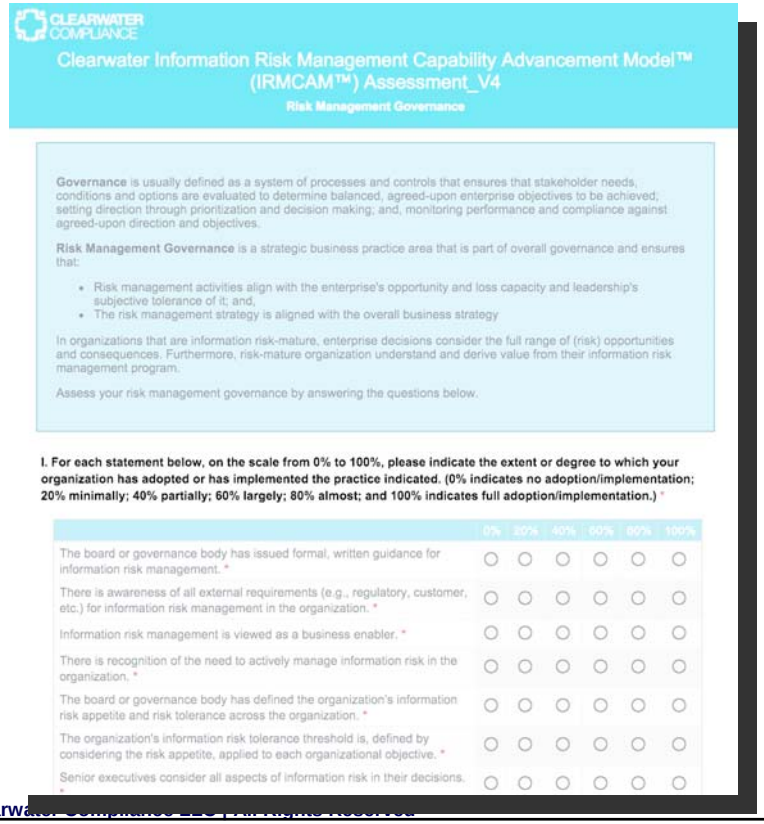
Latest White Paper

Industry Advisors

- David Finn | Health IT Officer | Symantec
- Meredith Phillips | Chief Information Privacy & Security Officer | HFH
- Eric Bergen | Independent Consultant
- Sam Homer, Ph.D. | Healthcare Technology Strategist | HCSC
- Kathy Jobes | CISO | Sentara Healthcare
- Ed Schreibman | Vice President of Healthcare Compliance | Expert Global Solutions, Inc.
- Ian Johansson | Corporate Compliance Officer | Aloha Care
- Deborah Schlesinger | Director Corporate Risk Management| SCAN Health Plan
- Adam Greene, JD | Attorney | Davis, Wright and Tremaine
- Matt Hanis | Vice President | Lockton
- Scott Blanchette | CIO | Kindred Healthcare
- Kyle Duke | CIO | TN Division of Health Care Finance & Administration
- Chris Dansie, Ph.D. | Assistant Professor | University of Utah

http://clearwatercompliance.com/thought-leadership/irmcam/

Clearwater Risk Management Capability Maturity Model Index (IRMCAMi™) – V4



1. Prepare to use the Clearwater Information Risk Management Capability Maturity Model™.
2. Set the desired information risk management maturity level for the organization.
3. Complete the Clearwater Information Risk Management Capability Maturity Model Index™ tool
4. Identify any gaps that may exist between the desired state of maturity and the current state.
5. Assess all identified gaps that may exist between the desired and the current state.
6. Rank order identified gaps and remediate the highest priority gaps.
7. Document results and repeat the assessment periodically.

Contact

Kathy Jobes
Chief Information Security Officer
(757) 252-0637
kejobes@sentara.com
Sentara Healthcare

Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US
CEO
800-704-3394
bob.chaput@ClearwaterCompliance.com
Clearwater Compliance LLC