

A decorative graphic featuring a grid of colored squares in blue, green, purple, orange, and red. A blue line with an arrow points from the top left towards the title, and a red line with an arrow points from the bottom right towards the date.

Health Care Chief Security Officer Best Practices Roundtable

September 16, 2016

Meet Your Panelists



Rob Lucas, CISSP
Chief Information Security Officer
Tanana Chiefs Conference

Kathy Jobes
Chief Information Security Officer
OhioHealth

Jacki Monson, JD, CHC, CHPC
Chief Privacy and Information
Security Officer
Sutter Health

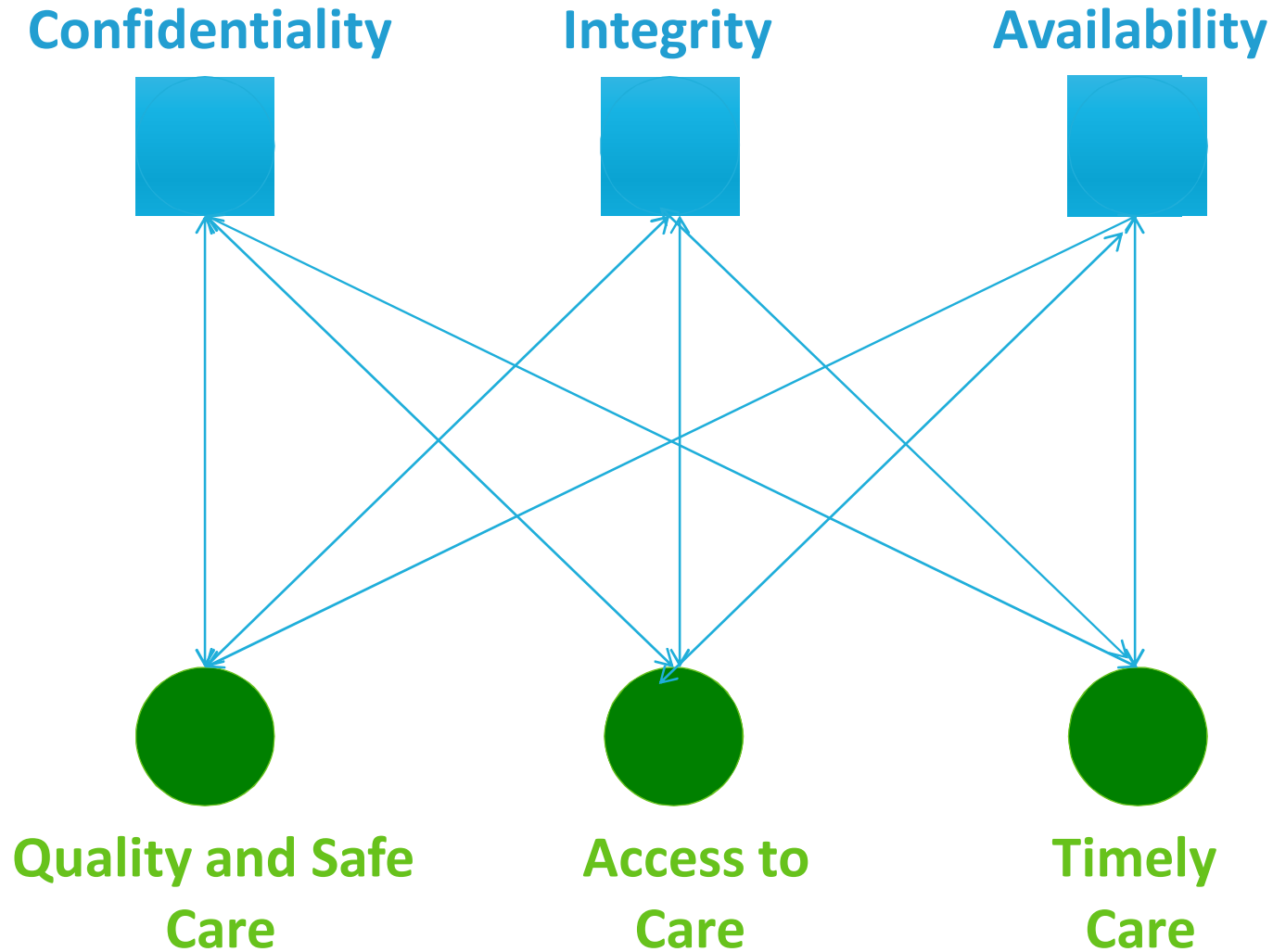
**Bob Chaput, CISSP, HCISPP, CRISC,
CIPP/US**
CEO
Clearwater Compliance

And, then there were 40...10 so far in 2016

Summary of HHS-OCR HIPAA Enforcement Actions

	Summary	\$20,314,800							
Settlement / CMP Amounts	\$52,589,700	\$5,550,000	\$2,750,000	\$2,700,000	\$650,000	\$2,200,000	\$750,000	\$3,900,000	\$1,550,000
Number of Individuals Affected	6,713,914	3,998,439	10,000	3,044	412	2	17,300	13,000	9,497
Settlement/Penalty per Individual Affected	\$7.83	\$1	\$275	\$887	\$1,578	\$1,100,000	\$43.35	\$300.00	\$163.21
Number of Settlement Agreements/CAPs	40	IL	MS	OR	PA	NY	NC	NY	MN
	Media/PHI Home	Desktop/Laptop	Laptop / Network Drive	Laptop / Thumb Drive	iPhone	Video Film	x-ray Films	Laptop	Laptop (BA)
Announcement Date	Summary	8/4/16	7/21/16	7/18/16	6/29/16	4/21/16	4/14/16	3/17/16	3/16/16
	RA Failures %	CE	CE	CE	BA	CE	CE	CE	CE-BA related (Accretive)
Key Finding and/or Corrective Action Plan	73%	Advocate Health Care Network	University of Mississippi (UMMC)	Oregon Health & Science University (OHSU)	Catholic Health Care Services (PHL)	NY Presbyterian Hospital	Raleigh Orthopaedic Clinic, P.A.	The Feinstein Institute for Medical Research	North Memorial Health Care of Minnesota
Develop / Revise Privacy, Breach Notification & Security PnPs	36	X	X	X	X	X	X	X	X
Implement (security awareness) training and sanctions for non-compliance	33	X	X	X	X Policies regarding	X	X	x - FIMR shall provide HHS	X
Conduct Risk Analysis Periodically	29	X	X	X	X			X	X
Establish Comprehensive Risk Management Plan and Process	26	X	X	X	X			X	X
Distribute and update policies and procedures	23				X- shall assess,			X	
Document Process for responding to security / privacy incidents	21		X UM failed to implement		x xPolicies regarding	x-Measures providing that			
Implement Reasonable Safeguards to control risks	25	X (facility access)	X-failed to implement					X	X

Safeguarding Patient Records or Patient Health?








“Hacking Hospitals” - Patient Records or Patient Health¹?



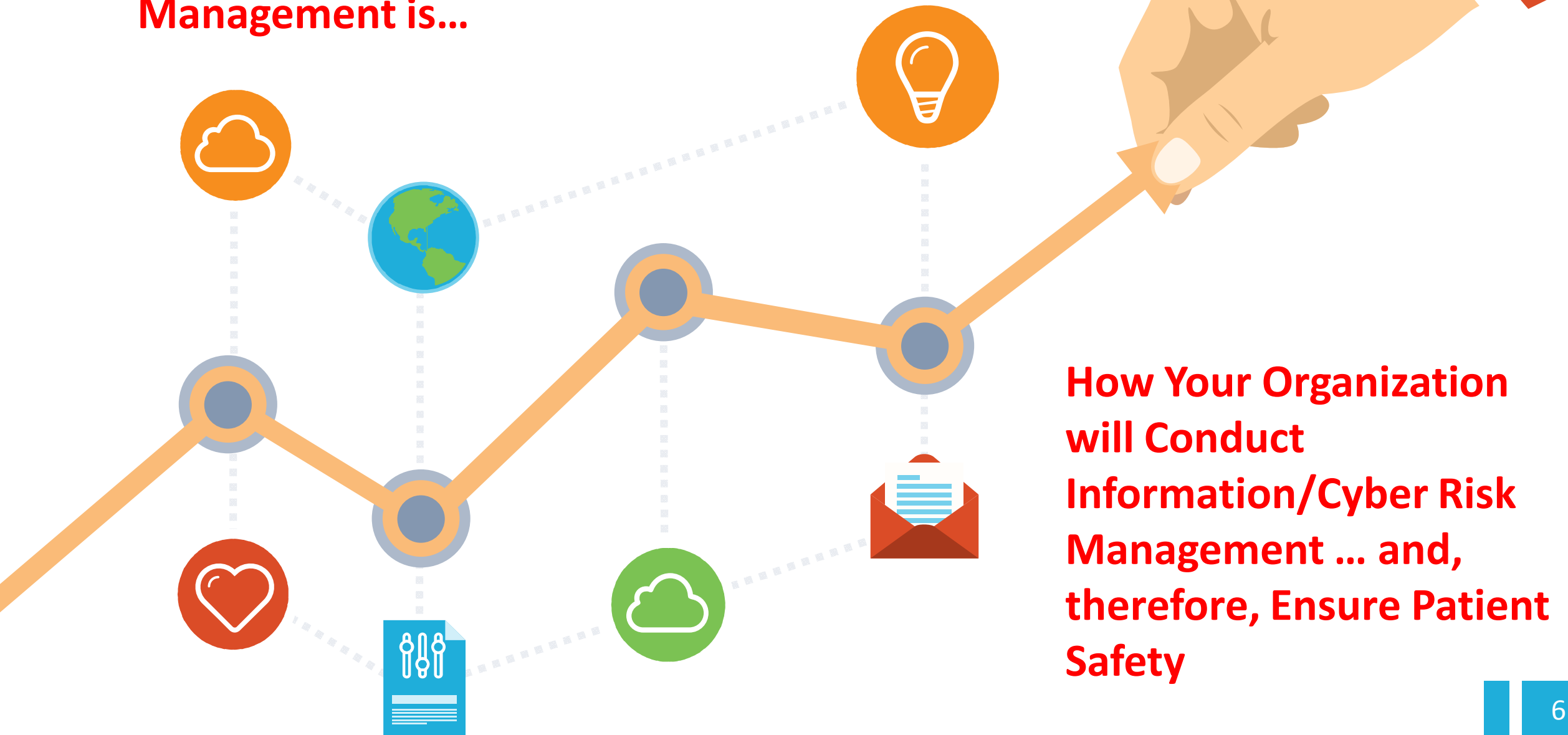
Patient Health



Patient Records

Adversary		Targeted (Specific Victims)	Untargeted (Indiscriminate)	Targeted (Specific Victims)	Untargeted (Indiscriminate)
	Individual / Small Group				YES
	Political Groups / Hacktivists /			YES	
	Organized Crime	YES		YES	YES
	Terrorism / Terrorist Org.	YES	YES		
	Nation States	YES	YES	YES	YES

The Single Biggest Decision Your Organization will Make Regarding Information/Cyber Risk Management is...



Chief Security Officer Best Practices



Strategically | *Overarching theme*

Information risk management should be part of enterprise risk management. HIPAA security compliance risks and cyber risks have become increasingly more significant business risk management issues with links to patient safety, financial, brand, talent acquisition and numerous other risks.

Tactically | *Overarching theme*

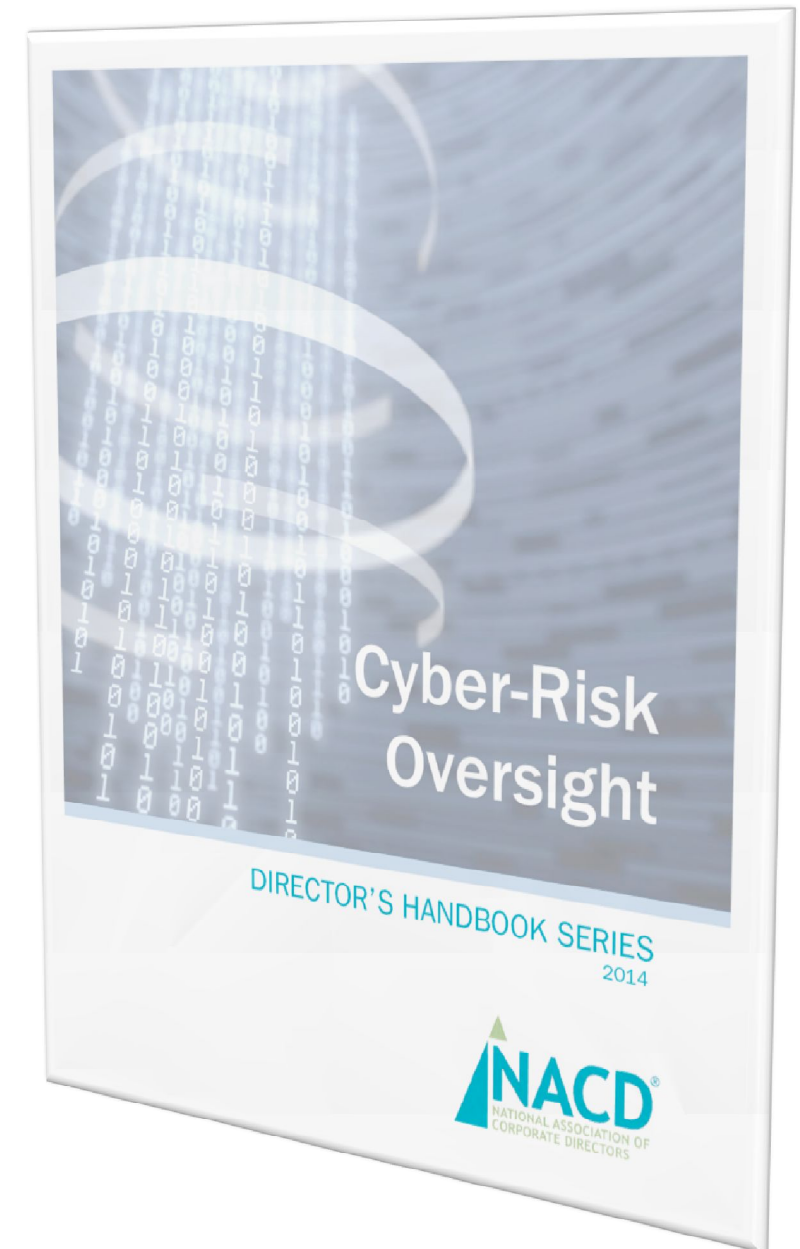
To effectively manage compliance and cyber risks, as with any long-term initiative, organizations must establish, implement and mature their cyber risk management programs. It appears that more organizations than not are operating in an “reactive-operational-technical-spot-welding” mode versus a more “proactive-strategic-business-architectural” manner.

Operationally | *Overarching theme*

At the end of the day, cyber risk management is about informed decision making... based on comprehensive, bona fide risk analyses. Some believe – we certainly do – that a major issue many organizations face is their inability or unwillingness to complete this foundational step required of any strong cyber risk management / information security program.

Strategic: Key Principles

- **PRINCIPLE 1** - Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
- **PRINCIPLE 2** - Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
- **PRINCIPLE 3** - Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
- **PRINCIPLE 4** - Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
- **PRINCIPLE 5** - Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.



Tactical: Program Elements

1. Governance, Awareness of Benefits and Value

Who makes what decisions, how and when, using what data and facts?



3. Process, Discipline & Repeatability

What policies, procedures, practices and processes will be used in what parts of the organization?



5. Engagement, Delivery & Operations

How will we implement IRM and embed risk considerations in business decision making?



2. People, Skills, Knowledge & Culture

What people, with what SKEs will create a risk-aware culture?



4. Standards, Technology Tools / Scalability

What industry standards and tools will we utilize to become effective and efficient?



Operational: Risk Analysis

What if my Sensitive Information is shared?
With whom? How?

CONFIDENTIALITY

ePHI,
PII, PCI Data,
MNPI, Trade Secrets,
Business Plans,
Software Code, Etc.

INTEGRITY

What if my Sensitive Information is not complete, up-to-date and accurate?

Don't
Compromise
C-I-A!

AVAILABILITY

What if my Sensitive Information is not there when it is needed?

