Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where 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 and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*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.

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Initiative to Program

A Hospital CISO's Perspective on Cybersecurity Best Practices

August 24, 2022

Key Facts About Clearwater

- Leading provider of cybersecurity, risk management and HIPAA compliance software, consulting, and managed services - exclusively for healthcare
- Founded in Nashville in 2009, national firm with colleagues in 20+ states
- Portfolio company of Altaris Capital Partners, a healthcare PE firm with $5B under management
- Approximately 400 customers, spanning IDNs, physician practice groups, healthcare technology leaders and medical device manufacturers
- 100% success rate when deliverables submitted to the Office for Civil Rights (OCR)

Healthcare's Top-Rated Security Advisors

Healthcare's Top-Rated Compliance & Risk Management Solution

Sixth Consecutive Year

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Webinar Logistics

- ✓ Slide materials – Link will be in the chat box
- ✓ All attendees are in “Listen Only Mode”
- ✓ Please ask content related questions in **“Q&A”**
- ✓ Please complete the **Exit Survey** when you leave the webinar
- ✓ **Recorded version, Attendance Certificate, & final slides shared within 48 hours**

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Agenda

- Introductions
- Initiative to Program
  - Annual security initiatives - Owensboro's experience
  - Making the shift to a comprehensive program
- Results & Looking Ahead
  - Results
  - Critical elements of Owensboro Health's program
- Q&A

Your Presenters

Jackie Mattingly, CHISL, CISSP, HCISPP

CISO, Owensboro Health

- 20+ years experience in IT and 10 years in information security
- Bachelors in Computer Science and her Master's in Healthcare Administration
- Adjunct faculty at University of Southern Indiana
- AEHIS Board Member
- 14+ years Owensboro Health

Adam Nunn

Director, Consulting Services

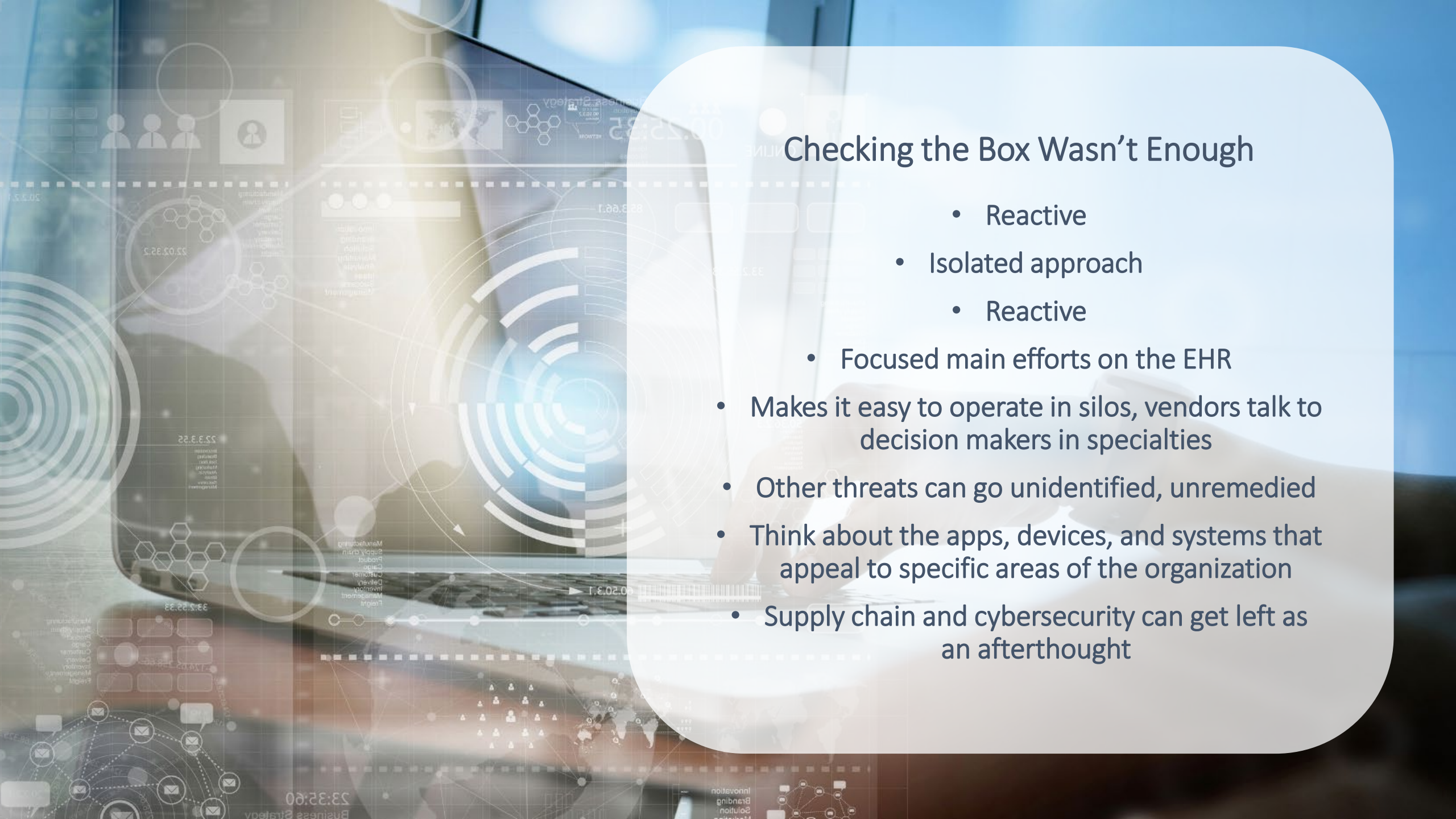
- Twenty-four years in cybersecurity and healthcare regulatory compliance
- As internal Chief Compliance Officer and Chief Information Security Officer, directly administered programs for hospitals and healthcare service organizations, including clinics, laboratories, pharmacies, business associates, and health plans.
- Cybersecurity and regulatory compliance experience in a wide range of organizational structures, from start-ups to multi-billion-dollar enterprises, including venture-capital, private-equity, not-for-profit, and publicly-traded organizations.
- CISSO from 2003-2013 with an ISSMP concentration.
- Former member of the HITRUST Leadership Roundtable.
- Former Officer of the Middle Tennessee Chapter of the Information Systems Security Association
- Active member of the Health Care Compliance Association and Information Systems Security Association

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Owensboro Health

- 4,800+ employees
- Serving an 18-county area in Western Kentucky & Southern Indiana
- Centrally located hospital
  - 477 beds
  - Serving over 30 specialties
- 3 outpatient Healthplex locations
- Healthpark

There are better strategies to managing risk that don’t involve rushing through an annual compliance check box



Checking the Box Wasn't Enough

- Reactive
- Isolated approach
- Reactive
- Focused main efforts on the EHR
- Makes it easy to operate in silos, vendors talk to decision makers in specialties
- Other threats can go unidentified, unremedied
- Think about the apps, devices, and systems that appeal to specific areas of the organization
- Supply chain and cybersecurity can get left as an afterthought

"suspicious network activity involving third parties"

- Tip from the FBI in 2015
- Keystroke logger malware had been placed on devices belonging to a hospital Owensboro Health later acquired
- Resulted in an OCR investigation
- Favorable termination of that investigation thanks to the strategy and documentation in place at the time

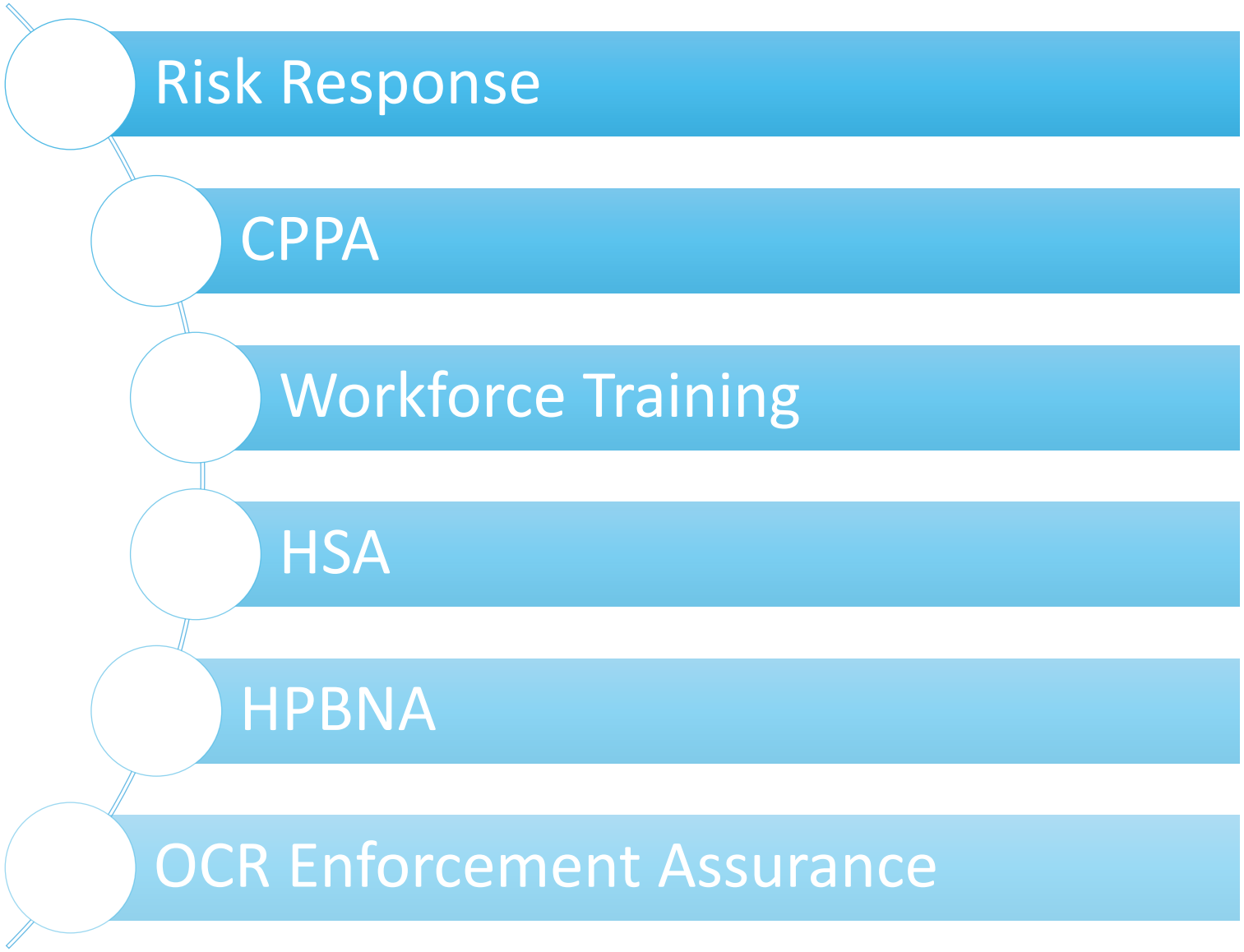
Making the Leap from Initiative to Program

Point-in-time vs. Ongoing Risk Analysis

	Point-in-time	Ongoing
Frequency	Annual	Ongoing/continuous
Method	Sampling	Comprehensive, Asset level
Risk Findings Report	Generalized	Tiered & prioritized
Meets Promoting Interoperability Requirements	Yes	Yes
Leverages previous lessons learned	No	Yes
Meet OCR's guidance for ongoing Risk Analysis/ NIST Framework	No	Yes

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Multi-Year Strategic Roadmap

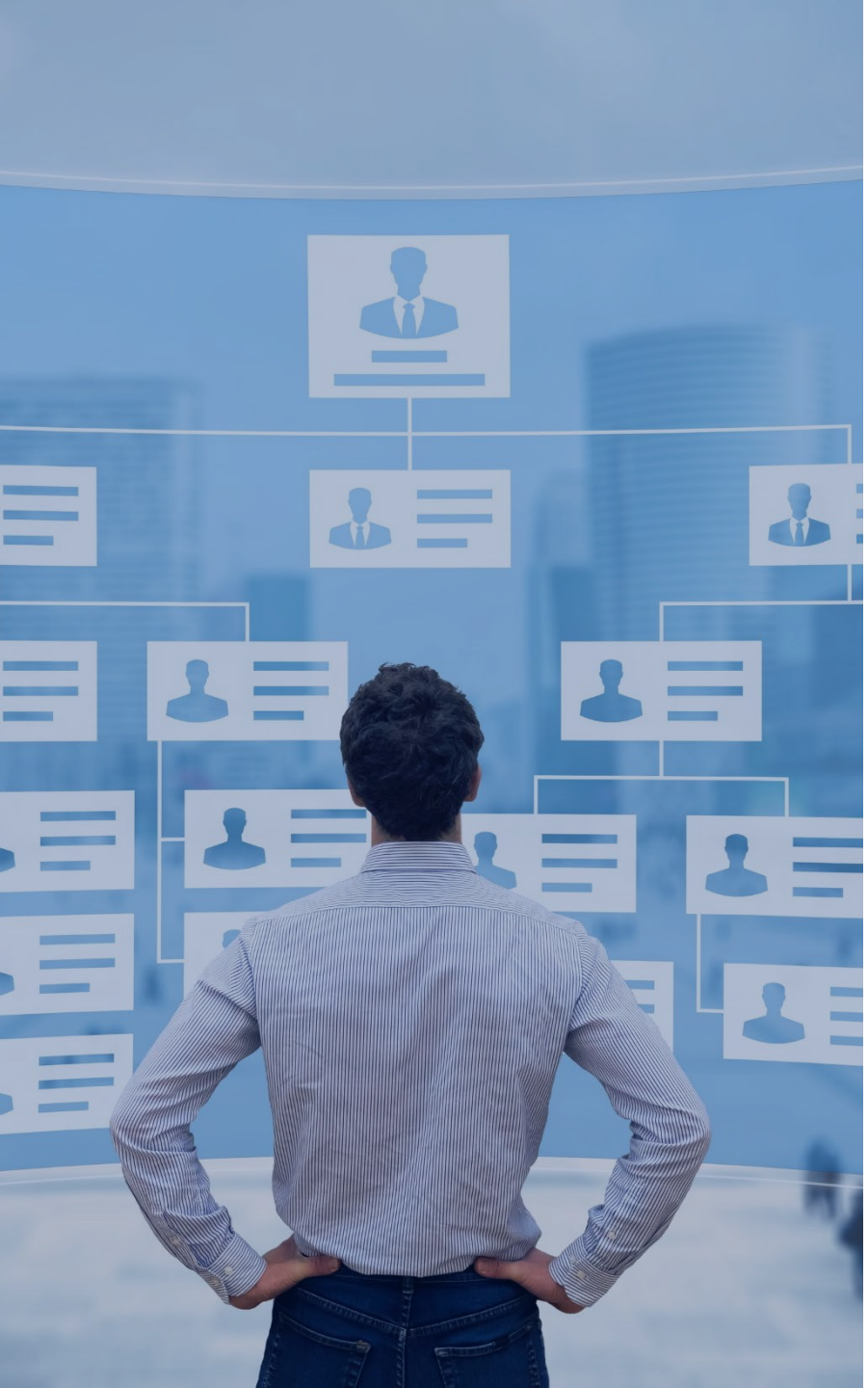


Look at the Supply Chain

- Medical devices
- Cloud solutions
- Web applications
- Homegrown solutions

Gaining Organizational Buy-in

- Explain the risk
- Leverage your partners/third-party experts
- Share the specifics with your stakeholders
    - Clinical directors
    - Department heads
    - “this doesn’t have….”
- Keep it centered on patients
- Isolate and segment technology doesn’t meet your security standards
- Hardening- removing unnecessary functions
- Have other backup controls identified so technology that’s best for clinical patient outcomes doesn’t jeopardize patient data
- Document, document, document



What Happens When the CISO Isn't a part of the IT Department?

- Makes it easier to:
  - Establish expectations
  - Providing training
  - Audit to make sure operational components were put in place
- It's not just an IT issue
- A CISO who operates outside of IT can build a cohesive strategy
- Holistic security

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Target Zero Initiative

- Eliminating preventable harm
- Security's role in the goal
- Participation as a program champion
- Participate in departments and initiatives that don't have anything to do with compliance or security, build organizational support

Owensboro Health Muhlenberg Community Hospital Celebrates 358 Days Without A Serious Safety Event

Owensboro Health Muhlenberg Community Hospital is celebrating a safety milestone, with Tuesday, March 14 marking 358 days without a Serious Safety Event at that facility.

Dr. Bill Bryant

Dr. Bill Bryant, chief quality and patient safety officer at Owensboro Health, said a serious safety event (SSE) is an error that reaches a patient and causes moderate to severe harm. A 1999 report by the U.S. Institute of Medicine, titled "To Err is Human: Building a Safer Health System" found that as many as 98,000 people die each year from preventable medical errors. Since then, the goal nationally has been to improve safety to assure that these errors do not reach patients.

Dr. Bryant said Owensboro Health's efforts to improve safety include participating in the nationwide Target Zero initiative, which aims to eliminate these events. As part of Target Zero, Owensboro Health has implemented system-wide use of Error

Don’t Go It Alone

Trusted Experts Can:

- Help you define the roadmap and strategy
- Establish a multi-year program
- Position the organization to be proactive, staying ahead of risks and remediation
- Offer a consistent pulse on what’s happening across the industry, not just inside your own organization
- Help you tackle complex risks

Finding the Right Partner:

- Check their references and talk to their customers
- Look them up on KLAS
- Ask industry colleagues who they work with and why

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Owensboro Health's Program

Internal Cybersecurity Committee

- Evaluates new technology against organizational cybersecurity standards
- Determines when and how new solutions that don't meet the standards can still be utilized while reducing risk
- Ongoing risk analysis and risk response at the asset level allows the organization to stay on top of risk as changes are made and new systems are added or updated

ClearConfidence™ Managed Services Program

- Help establishing and chartering the oversight committee
- Aligning to a specific framework (NIST)
- IRM|Pro® Software
- On-demand access to SMEs and cybersecurity experts
- Program management
- Weekly meetings

ClearConfidence™

IRM|Pro®

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

We’re all in this together, fighting the same fight to protect our data and take care of our patients

Thank You & Questions

Jackie Mattingly

jackie.mattingly@owensborohealth.org

Adam Nunn

adam.nunn@clearwatercompliance.com

Thank you for taking the time to complete the survey when you leave the session. We value & use your feedback!

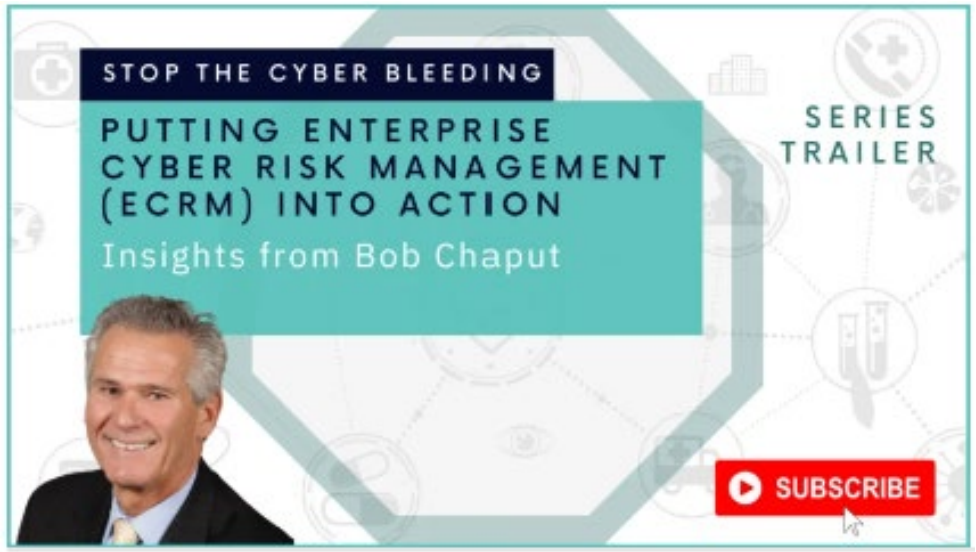
CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Upcoming Clearwater Web Events…

[Learn more & register today for these free web events & more here!]

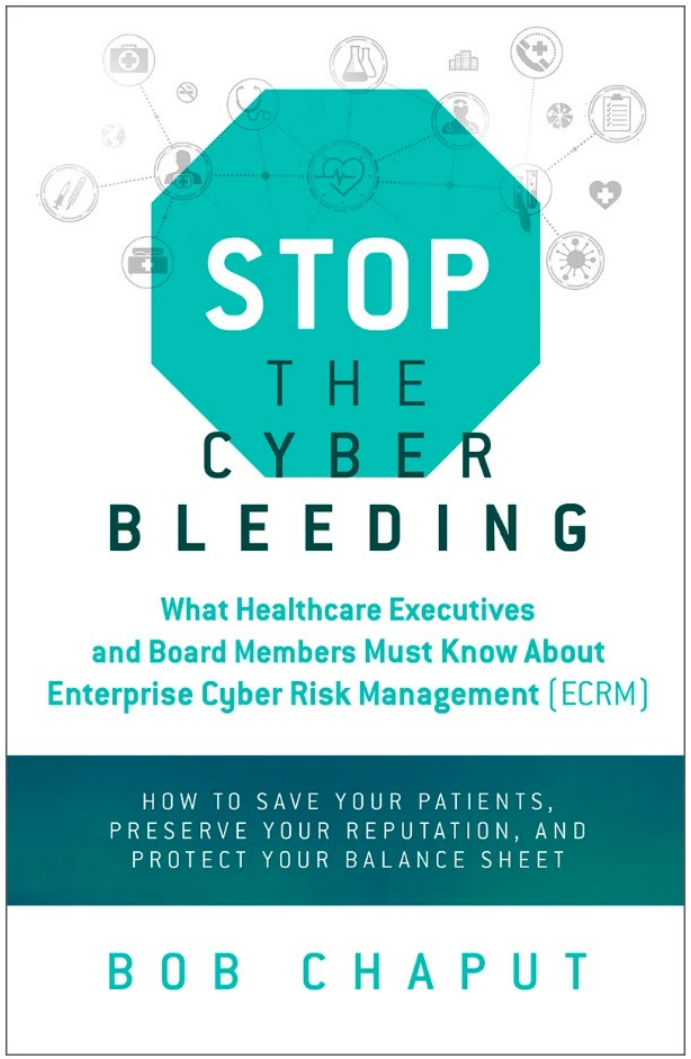
CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Additional Educational Resources…



Click to SUBSCRIBE

What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management



New Book Provides Healthcare Leaders with Guidance on How to Manage Growing Cyber Risk

GET YOUR COPY TODAY - Available in Audio, Digital, & Hard Copy

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

www.ClearwaterCompliance.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-compliance-llc/

Twitter | @clearwaterhipaa