2019 CIO Virtual Cybersecurity Symposium™

Session Details:

1. **July 11 | Session 1 – Host, Jon Moore**

   · Module 1 – The Evolving Cyber Risk Landscape: True Stories from the Field | Bob Chaput
   · Module 2 – OCR Enforcement: Past, Present and Future | Jon Moore

2. **July 18 | Session 2 – Host, Jon Moore**

   · Module 3 – A Framework for Analyzing Cyber Risk | Cathie Brown
   · Module 4 – The Risk Treatment Decision | Blaine Hebert

3. **July 25 | Session 3 – Host, Jon Moore**

   · Module 5 – Rethinking Cybersecurity Policy Governance: How to Turn Organizational Intent into Action | Wes Morris & Adam Nunn
   · Module 6 – Making the Case for Cyber Risk Management Investment | Baxter Lee

Overall Objectives

Protecting patient information is foundational to any healthcare organization's IT strategy. But as cybersecurity threats grow in frequency and complexity, many CIOs find themselves plugging holes in their system infrastructure to address vulnerabilities. This 3-session workshop is designed to help CIOs and healthcare leaders think about cyber risk holistically and build a program that ensures data is effectively protected.

Attendees will be requested and expected to:

- Engage in live polls conducted in each session
- Post questions and comments for Faculty to address
- Complete an evaluation after each session

Clearwater Faculty Presenters:

- Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US, Executive Chairman
- Jon Moore, MS, JD, HCISPP, Chief Risk Officer & SVP, Professional Services
- Cathie Brown, CGEIT, PMP, CISM, CISSP, VP of Professional Services
- Wes Morris, CHPS, CIPM, HCISPP, Managing Consultant, Professional Services
- Adam Nunn, Principal Consultant
- Blaine Hebert, MSIT, CISSP, HCISPP, Principle Consultant
- Baxter Lee, CFO

Session I – Thursday, July 11, 2019 at 12pm-2pm Eastern Time				
Eastern Time	**Instructional Module**	**Learning Objectives - Attendees Will Be Able To:**	**Faculty Member**	**Supplemental Material (in addition to presentation slides)**
12-12:10	Welcome	• Introductions & Symposium Overview		
12:10 pm – 1:00 pm (50 min.)	1. The Evolving Cyber Risk Landscape: True Stories from the Field	• Describe the anatomy of risk and set the foundation for the Symposium • Explain why cyber risk management is not just an "IT Problem" and must become an executive-led team sport • Leverage cyber risk management lessons-learned from key case studies	**Bob Chaput**, MA, CISSP, HCISPP, CRISC, CIPP/US	• Harnessing the Power of NIST | Your Practical Guide to Effective Information Risk Management (Clearwater White Paper) • Banner Health's Becky Havlisch and Bob Chaput on Nimble Cyber Risk Management • Cleveland Clinic's Charles Kolodkin and Clearwater's Bob Chaput Share Crucial Steps in Developing a Hospital Cyber Risk Management Strategy • National Children's Rebecca Cady and Clearwater's Bob Chaput discuss Managing Cyber Risk through an Insurance Captive • Business of Healthcare Interview with Michelle Johns and Bob Chaput | Insurance Captives: Innovation & Cost Savings for Providers
1:00 pm – 1:50 pm (50 min.)	2. OCR Enforcement: Past, Present and Future	• Identify applicable laws and regulations • Recognize common violations found by OCR • Compare year over year trends in OCR enforcement • Summarize OCR leadership's position on enforcement efforts • Predict the future of OCR enforcement efforts	**Jon Moore** MS, JD, HCISPP	• ARRA • HIPAA Omnibus Final Rule • OCR 2018 Audit Protocol • OCR Complaint Data • OCR Breach Data • OCR Resolution Agreements • Notification Enforcement Discretion
Session I Recap 1:50-2:00pm | Most Valuable Concepts/Processes/Practices | Evaluation Reminder				

Session II – Thursday, July 18, 2019 at 12pm-2pm Eastern Time				
Eastern Time	**Instructional Module**	**Learning Objectives - Attendees Will Be Able To:**	**Faculty Member**	**Supplemental Material (in addition to presentation slides)**
12-12:10	Welcome	• Introductions & Recap		
12:10 pm – 1:00 pm (50 min.)	3. A Framework for Analyzing Cyber Risk	• Recognize the need to make decisions in an uncertain world • Identify different types of risk • Define the components of information risk • Describe the importance of governance and framing • Justify investment in cyber risk reduction • Leverage the NIST Cybersecurity Framework to better manage and reduce cybersecurity risk • Implement the NIST IRM Process: Framing, Assessing, Responding to and Monitoring Risk • Mature your IRM program to proactively protect your organization's sensitive information • Ultimately, make higher quality decisions about information / cyber risks by adopting the NIST approach	**Cathie Brown,** CGEIT, PMP, CISM, CISSP	• NISTIR 7298 Revision 2 Glossary of Key Information Security Terms • Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) • Guidance on Risk Analysis Requirements under the HIPAA Security Rule • NIST SP800-39-final_Managing Information Security Risk • NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments • NIST SP800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach • NIST SP800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP800-115 Technical Guide to Information Security Testing and Assessment • HHS/OCR FAQ on 3rd Party Certifications • Framework for Improving Critical Infrastructure Cybersecurity • Cybersecurity Framework Industry Resources • OIG: HHS Needs to Strengthen Security and Privacy Guidance and Oversight • Cybersecurity Framework Frequently Asked Questions • NIST SP800-39-final_Managing Information Security Risk • Harnessing the Power of NIST | Your Practical Guide to Effective Information Risk Management (Clearwater White Paper) • Choosing an Information Risk Management Framework: The Case for the NIST Cybersecurity Framework in Healthcare Organizations

Session II – Thursday, July 18, 2019 at 12pm-2pm Eastern Time				
1:00 pm – 1:50 pm (50 min.)	4. The Risk Treatment Decision	• The HIPAA requirement to conduct a Risk Analysis • Now that you know, it's your responsibility to respond • Examining "Critical" or "Very Important" asset reviews and the associated risks • What will be your Risk Treatment decision? • Will that decision align with the Business? • Will that decision align with your Strategic vision? • Creating a simplistic Decision Tree • Following the NIST CSF	**Blaine Hebert**, MSIT, CISSP, HCISPP,	• NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments • NIST SP800-39-final_Managing Information Security Risk • Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)
Session II Recap 1:50-2:00pm Eastern Time | Most Valuable Concepts/Processes/Practices | Evaluation Reminder				

Session III – Thursday, June 27, 2019 at 12pm-2pm Eastern Time				
Eastern Time	**Instructional Module**	**Learning Objectives - Attendees Will Be Able To:**	**Faculty Member**	**Supplemental Material (in addition to presentation slides)**
12-12:10	Welcome	• Introductions & Recap		
12:10 pm – 1:00 pm (50 min.)	5. Rethinking Cybersecurity Policy Governance- How to turn organizational intent into consistent action	• List the challenges associated with defining, implementing and managing cybersecurity policies and procedures • Describe the traditional approach to cybersecurity policy management and its limitations • Explain a framework to more effectively define, organize, implement and manage organizational cybersecurity policy expectations • Apply governance principles to implement a principal-based policy framework.	**Wes Morris** CHPS, CIPM, HCISPP **Adam Nunn**	• Framework for Improving Critical Infrastructure Cybersecurity v1.1 (NIST Cybersecurity Framework Version 1.1) • Choosing an Information Risk Management Framework: The Case for the NIST Cybersecurity Framework (CSF) in Healthcare Organizations *(Clearwater White Paper)* • NIST's Matt Barrett's recorded 4/27 video introducing Version 1.1: https://youtu.be/NOqLyXgPNms • NIST PPT version of slides: https://www.nist.gov/file/449511

1:00 pm – 1:50 pm (50 min.)	6. Making the Case for Cyber Risk Management Investment	• Gain insights on statistics for assessing the likelihood of a breach or an OCR investigation
		• Learn the potential repercussions of a data breach
		• Understand how to present a compelling Return on Investment ("ROI") calculation for your Information Risk Management Program
		• Determine how to choose cost factors relevant to your organization
		• Learn how cyber commercial insurance might help reduce the impact
		• Prepare to calculate the cost of a date breach specific for your organization
		• Turn the breach cost into a compelling business plan to strengthen your security program
			Baxter Lee	• The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security (ANSI) (PDF)
				• Cost of a Data Breach Model (Excel)
				• Links to Supplemental Guidance from OCR
				  ○ HIPAA Guidance Materials
				  ○ OCR Resolution Agreements
				  ○ OCR Complaint Data
				  ○ OCR Breach Data
				  ○ FACT SHEET: Ransomware and HIPAA
				• HIPAA Privacy, Security and Breach Notification Audit Program

Session III Recap 1:50-2:00pm | Most Valuable Concepts/Processes/Practices | Evaluation Reminder				