2019 CISO Virtual Cybersecurity Symposium™

Session Details:

1. **August 1 | Session 1 – Hosted by 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. **August 8 | Session 2 – Hosted by Jon Moore**
    - Module 3 - A Framework for Analyzing Cyber Risk | Cathie Brown
    - Module 4 - Common Risk Analysis Failures | Iliana Peters & Jon Moore
3. **August 15 | Session 3 – Hosted by Cathie Brown**
    - Module 5 – Developing an OCR-Proof Risk Management Plan | Cathie Brown
    - Module 6 – Developing an Executive Plan of Action and Milestones | Blaine Hebert
4. **August 22 | Session 4 – Hosted by Jon Moore**
    - Module 7 – Rethinking Cybersecurity Governance | Wes Morris & Adam Nunn
    - Module 8 – Making the Case for Cyber Risk Management Investment | Baxter Lee
5. **August 29 | Session 5 – Hosted by Jon Moore**
    - Module 9 – Addressing New Threats: Medical Device and IoT Risk Management | Mark Sexton
    - Module 10 – Assessing Cyber Risk Management Program Maturity | Adam Nunn & Jon Moore

Overall Objectives

Faced with an onslaught of threats these days, healthcare chief information security officers (CISOs) need to take a deep breath and focus on cybersecurity best practices. The number and frequency of these threats—ransomware, cryptocurrency mining, data-stealing malware, advanced persistent threats, malicious insiders, and careless employees, to name a few—can be overwhelming. It can seem like healthcare CISOs and their teams are always one step behind the well-funded bad guys.

During this workshop, we will discuss the current risk landscape and the steps that organizations are taking to assess, respond and monitor information risks effectively.

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 the each session

Clearwater Faculty Presenters for the CISO Symposium

- Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US, Executive Chairman
- Jon Moore, MS, JD, HCISPP, Chief Risk Officer & SVP, Professional Service
- Cathie Brown, CGEIT, PMP, CISM, CISSP, VP of Professional Services
- Wes Morris, CHPS, CIPM, HCISPP, Managing Consultant, Professional Services
- Mark Sexton, MPA, CISSP, HCISPP, CISA, CCSK, Principle Consultant
- Adam Nunn, CREDS, Principal Consultant
- Blaine Hebert, MSIT, CISSP, HCISPP, Principle Consultant
- Baxter Lee, CFO
- Guest Presenter: Iliana Peters, JD, CISSP, Former Deputy Director of OCR/HHS, Shareholder, Polsinelli Law

Session I of V – Thursday, August 1, 2019, 12:00-2:00pm 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	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	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 2016 Audit Protocol • OCR Complaint Data • OCR Breach Data • OCR Resolution Agreements • Notification Enforcement Discretion
Session I Recap 1:50-2:00 pm Eastern Time | Most Valuable Concepts/Processes/Practices | Evaluation Reminder				

Session II of V – Thursday, August 8, 2019, 12:00-2:00pm 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	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
1:00 - 1:50	4) Common Risk Analysis Failures	• Understand general regulatory requirements for ongoing risk analysis • Cite the specific regulatory requirements for risk analysis • Identify common reasons OCR finds Risk Analysis to be insufficient	**Iliana Peters,** JD, CISSP	• Sample - HIPAA Security Risk Analysis FOR Report • Guidance on Risk Analysis Requirements under the HIPAA Security Rule • NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments • NIST SP800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach • 30-Minute Guide to Hiring The Best Risk Analysis Company | What to Look for in a HIPAA Risk Analysis Company & Solution • White Paper: How to Conduct a Bona Fide Risk Analysis (PDF) • Risk Analysis Cost Justification (PDF)
Session II Recap 1:50-2:00 pm Eastern Time | Most Valuable Concepts/Processes/Practices | Evaluation Reminder				

Session III of V – Thursday, August 15, 2019 12:00-2:00pm Eastern Time				
Eastern Time	**Instructional Module**	**Learning Objectives - Attendees Will Be Able To:**	**Faculty Member**	**Supplemental Material (in addition to presentation slides)**
	Welcome	• Introductions & Recap		
12:10 pm – 1:00 pm	5) Developing an OCR-Proof Risk Management Plan	• Understand the regulatory requirements and most effective standards for responding to risk • Know the four essential options for effective risk response • Evaluate alternatives to reduce risks in terms of effectiveness and Feasibility • Learn how to make sure risk responses get implemented through tracking new or improved controls and safeguards	**Cathie Brown,** CGEIT, PMP, CISM, CISSP	• Sample - HIPAA Security Risk Analysis FOR Report • Guidance on Risk Analysis Requirements under the HIPAA Security Rule • NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments • 30-Minute Guide to Hiring the Best Risk Analysis Company • Clearwater recorded webinar – "The Critical Difference: HIPAA Security Evaluation v HIPAA Security Risk Analysis"
1:00 – 1:50	6) Developing An Executable Plan of Action and Milestones	• Making the decision to use a POAM • How simple can it be? • Use the POAM to Initiate and track progress of the Risk Analysis • Identifying several key components of a standard POAM • Best Practices when using a POAM	**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 III Recap 1:50-2:00 pm Eastern Time | Most Valuable Concepts/Processes/Practices | Evaluation Reminder				

Session IV of V – Thursday, August 22, 2019 12:00-2:00pm 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 – 1:00	7) 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**	• NIST Cybersecurity Framework- A voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk. • NoticeBored Security Policies- Developed policies and procedures that align to a principle-based governance model and ISO27001:2013. • ISO 27001:2013- ISO/IEC 27001 is a standard providing requirements for an information security management system (ISMS). • NIST Cybersecurity Framework Introduction Video
1:00 - 1:50	8) Making the Case for Funding Your Cyber Risk Management Program	• 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 IV Recap 1:50-2:00 pm Eastern Time | Most Valuable Concepts/Processes/Practices | Evaluation Reminder				

Session V of V – Thursday, August 29, 2019 12:00-2:00pm 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 – 1:00	9) Addressing New Threats: Medical Device and IoT Risk Management	• Understand the challenges of updating medical device software • Identify medical devices which fall under the purview of a HIPAA Risk Analysis • Establish practical compensating controls to protect against new threats or legacy devices • Ensure that appropriate monitoring of both controls and medical devices is being conducted • Describe new technologies to assist healthcare in medical device discovery and risk management	**Mark Sexton,** MPA, CISSP, HCISPP, CISA, CCSK	• AAMI TIR57, Principles for medical device security – risk management • Guidance on Risk Analysis Requirements under the HIPAA Security Rule • IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities • ISO 14971 Medical devices — Application of risk management to medical devices • FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance • FDA Postmarket Management of Cybersecurity in Medical Devices • Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) • FDA – Medical Devices • THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY • NIST SP1800-8, Securing Wireless Infusion Pumps in Healthcare Delivery Organizations - DRAFT • NIST SP 800-30 Rev 1, Guide for Conducting Risk Assessments • NIST SP 800-37 Rev1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach • NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View 2018_A
1:00 – 1:50	10) Assessing Cyber Risk Management Program Maturity	• Explain the importance of a mature IRM program and framework • Describe the IRM Maturity Model • Determine your organization's current IRM level of maturity	**Adam Nunn & Jon Moore,** MS, JD, HCISPP	• NACD Cyber-Risk Handbook • COBIT • COBIT 2019 Toolkit – reference Capability and Maturity Section, Page 35 • NIST Cybersecurity Framework- A voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk. • NIST Cybersecurity Framework Introduction Video
Session V Recap 1:50-2:00 pm Eastern Time | Most Valuable Concepts/Processes/Practices | Evaluation Reminder				