

Cyber Risk Summit

NetDiligence® Career Pathways Program for Young Professionals Agenda for October 5, 2026

8:00 AM–9:00 AM	Check-In and Breakfast
9:00 AM–9:15 AM	Welcome and Opening Remarks from NetDiligence, YRP, and IWCRP
9:15 AM–9:45 AM	Part I: The Client's Perspective
@9:15 AM	CISO Perspective Hear directly from the client! The evolution and expansion of the Chief Information Security Officer (CISO) role has elevated their position to the executive leadership table, where they must inform and guide companies on all matters of cyber risk management. Hear about the practical concerns and the decisions that CISOs make, and explore how cyber insurance fits into their risk management planning. Speakers: Tammy Klotz, Trinseo; Donna Ross Cybersecurity/Risk/Compliance Executive; Anahi Santiago, ChristianaCare
9:45 AM–10:15 AM	Part II: Security Basics
@9:45 AM	Domain Security: Your First Line of Cyber Defense A strong domain security strategy helps prevent email spoofing, phishing, and domain impersonation by implementing controls such as SPF, DKIM, and DMARC while monitoring for lookalike domains and unauthorized use. This session will explain why protecting an organization's domain is foundational to reducing cyber risk, protecting brand reputation, and preventing costly fraud and insurance claims. Speaker: Michael Rogers, Markmonitor Group
@10:00 AM	EDR, MDR & XDR: Modern Endpoint Defense Learn how Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), and Extended Detection and Response (XDR) help organizations detect, investigate, and respond to cyber threats before they become major incidents. This session explains the differences between these technologies, why they are considered among the most effective security controls available today, and how they reduce cyber risk and improve organizational resilience. Speaker: Chase Cunningham, LUMU Technologies
10:15 AM–10:45 AM	Refreshment Break
10:45 AM–11:30 AM	Part II: Security Basics, continued
@10:45 AM	The Many Shades of MFA Multi-Factor Authentication (MFA) is one of the most effective security controls for preventing unauthorized access, but not all MFA is created equal. This session explores the different types of MFA—including phishing-resistant methods, human-to-machine and machine-to-machine authentication—and explains how proper implementation strengthens identity security and significantly reduces cyber risk. Speaker: Jamie Tolles, IDX
@11:00 AM	Immutable Cloud Backups and Storage Immutable backups are one of the most effective defenses against ransomware, ensuring critical data cannot be altered or deleted—even if attackers gain access to an environment. This session explains how immutable storage works, compares leading backup approaches, and explores how organizations can select the right solution to strengthen cyber resilience and accelerate recovery. Speaker: Anna Sarnek, Terra
@11:15 AM	Employee Security Awareness Training Technology alone cannot stop cyberattacks—employees are often the first line of defense. This session explores how effective security awareness training, phishing simulations, and practical security habits help reduce human error, strengthen an organization's security culture, and prevent many of today's most common cyber incidents. Speaker: Shelly Giesbrecht, CrowdStrike
11:30 AM–12:15 PM	Part III: Claims & Losses
@11:30 AM	Cyber Claims & Losses Gain insight into today's cyber claims landscape by examining the most common causes of loss, emerging claims trends, and real-world incident examples. We'll explore how claims data helps insurance professionals understand cyber risk, evaluate policyholders, and identify the security controls that have the greatest impact on reducing losses. Speakers: Alyssa Farruggia, Ascot Group; Mark Giacopelli, Nationwide; Kyle Ulscht, Old Republic Cyber

12:15 PM–1:30 PM	Lunch
1:30 PM–3:00 PM	Part IV: Breach Response
@1:30 PM	Digital Forensics & Incident Response (DFIR) Digital Forensics and Incident Response (DFIR) plays a critical role in helping organizations contain cyber incidents, determine what happened, and recover quickly while preserving key evidence. This session provides an overview of the DFIR process and highlights best practices for minimizing the impact of cyberattacks. Speaker: Rich Servillas, RSM US LLP
@1:45 PM	Ransomware Negotiation & Payments Our professional ransomware extortion negotiator will lead us through a hacker negotiation, provide firsthand insight, and discuss how to successfully navigate the extortion payment process and stay on the right side of OFAC. Speaker: Don Wyper, Chaintrax Cyber
@2:00 PM	From Breach to Notification: Reducing Cost, Delay, and Complexity in Breach Response Sensitive data review is often the most complex and costly phase of breach response. Learn how AI-powered data mining and workflow automation are helping breach response teams improve accuracy, accelerate notification decisions, and deliver more efficient, defensible outcomes. Speaker: Hannah Woodruff, Relativity
@2:15 PM	Mechanics of Mandatory Notification, Call Center & Credit Monitoring for Affected Parties Once impacted individuals have been identified after a breach, a well-coordinated notification process is essential to meeting legal obligations and maintaining trust. See how breach response partners manage notification requirements, call center operations, and credit monitoring services to help deliver a timely, compliant, and effective response. Speaker: Allen Burzen, CyEx
@2:30 PM	Restoration and Remediation Recovering from a cyber incident requires more than restoring systems—it requires a coordinated strategy to resume operations, strengthen security, and minimize long-term business impact. This session explores technical recovery, legal considerations, and best practices for reducing business interruption and building cyber resilience. Speaker: Luke Green, Lyra Recovery
@2:45 PM	Crisis Communications: To notify or not to notify? Communicating after a cyber incident requires balancing legal obligations, operational realities, and reputational risk. This session examines the key factors that influence disclosure decisions, including notification timing, stakeholder communications, and the potential consequences of notifying too early, too late, or more broadly than necessary. Speaker: Alex Rostron, FTI Consulting
3:00 PM–3:30 PM	Refreshment Break
3:30 PM–4:45 PM	Part V: Legal & Regulatory
@3:30 PM	Reporting to and Notifying Regulators So many rules and so many regulators! Hear from our State Attorney General representative about complying with incident notification requirements and how it impacts regulatory and legal exposure. Speaker: Kashif Chand, New Jersey Division of Law, Department of Law and Public Safety
@3:45 PM	Privacy & Cyber Regulation: What You Need to Know Our legal panelists will discuss what has been the focus of global data privacy legislation and regulation over the last year and how it impacts legal exposure and cyber insurance coverage. The discussion will include various updates and trends with a spotlight on privacy legislation. Speakers: Ian Birdsey, Clyde & Co LLP; Daniel Marvin, Kennedys
@4:15 PM	Current Trends in Class Action Cases within the Cyber Insurance Sphere Hear about the latest trends in class action filings, certifications & settlements. This panel discussion will delve into the growing occurrence of class action cases within the cyber insurance sphere, as well as tactics for anticipating and addressing potential surges in litigation, with a particular focus on recent cases such as Metapixel and BIPA. Speakers: Kamran Salour, Lewis Brisbois; Melissa Siebert, Cozen O'Connor
4:45 PM–6:30 PM	Reception

The Career Pathways Program is made possible by our sponsor:

