7:00 – 8:30 AM PT | 9:00 – 10:30 AM CT | 10:00 – 11:30 AM ET

Opening Keynote: Cybersecurity, Data Privacy & New Frontiers

Pablos Holman
Founder
Deep Future

Computers have infiltrated every area of our lives and our companies. These computers have given us intoxicating knowledge, powers, and capabilities. We've also inherited a cosmos of complications and consequences that we are only beginning to comprehend. Built with layers upon layers of technical components, the systems we use are vulnerable to all kinds of misuse. Opportunity lies here for innovators, some of whom have created entire new industries, some of whom have found ways to wreak havoc on nearly all of us. Pablos is a hacker with a deep understanding of these issues. He will show how the mind of a hacker works and how it can be deployed for the right reasons or wrong reasons. You'll learn that nothing is secure, that maintaining privacy and security in the modern world is a war of escalation. You will never win, but you can learn to mitigate your risk and lose less severely.

Pablos Holman is a hacker, inventor, and technology futurist with a unique ability to distill complex technology into practical tools. Always building the future, and a member of the most prolific team of inventors in the United States, he holds 70+ patents and has contributed to visions for the future of urban transportation, entertainment, education, energy, manufacturing, health care, food delivery, sensor networks, payment systems, and cloud computing. Holman has spoken at Singularity University, Stanford, the United Nations, the World Economic Forum at Davos, the Microsoft CEO Summit, the CIA, Google Zeitgeist, The Milken Global Conference, and to many of the world's top tech companies and conferences. His TED Talks have over 20 million views. Currently, Holman is working to rearchitect industries with the superpowers of automation, robotics, and machine learning.

NASBA: Specialty Knowledge | Learning Level: Basic | CPE Credit: 1.8

8:40 – 9:40 AM PT | 10:40 – 11:40 AM CT | 11:40 AM – 12:40 PM ET

Session 1: A Cyber Insurance Primer

Nicole Lazarz Graham
Risk Consultant
Aon Insurance Services

This presentation will provide insights into why CPA firms are prime targets for a data breach, in addition to examining the current cyber claim environment and coverage options available to help transfer that risk.

In this session, participants will:

- Learn how cyber incidents are impacting the accounting profession.
- Gain a basic understanding of cyber coverage available to help transfer cyber risk.

Nicole Lazarz Graham serves on a team within Aon Affinity's Accountants Risk Transfer and Risk Mitigation Division. She delivers risk management consulting services to Aon's CPA firm clients to assist them with mitigating professional liability risks, as well as provides risk advice regarding cyber, employment practices, management liability, and other related exposures. Previously, as general counsel at a media company, Graham provided advice on risk management and labor and employment matters, maintained accreditation compliance, drafted and negotiated commercial contracts and M&A transactions, and performed due diligence for investment opportunities. Prior, she served for 10+ years as a litigator, defending accountants and other professionals against professional liability claims.

NASBA: Auditing | Learning Level: Intermediate | CPE Credit: 1.2

9:50 – 10:50 AM PT | 11:50 AM – 12:50 PM CT | 12:50 – 1:50 PM ET

Session 2: Multiplying Internal Audit's Effectiveness in Mitigating Cyber Risks

Grant Ostler
Director of Product Marketing
Workiva

This session will investigate the apparent disconnect between internal audit's assessment of cyber and other IT risks and the level of resources allocated by audit to those risks. It will then explain opportunities for internal audit to increase its effectiveness in both validating cyber risks and providing assurance regarding the effectiveness of cyber controls intended to mitigate them.

In this session, participants will:

- Become familiar with how the Three Lines are intended to function together to mitigate cyber and other IT risks effectively.
- Explore regulations related to cybersecurity and their potential impact on the organization.
- Discover options internal audit has to increase its impact on understanding and mitigating cyber and other IT risks.
- Examine how the internal audit function can improve communications with internal IT stakeholders regarding security risks.

Grant Ostler is an Industry Principal of Integrated Risk at Workiva with 30+ years of experience emphasizing the disciplines of auditing, enterprise risk management, and process improvement. He served as chief audit executive for almost two decades for entities ranging from Fortune 500 companies to a pre-IPO technology company, including building internal audit functions from scratch and leading the implementation of SOX 404 compliance programs for three companies. An active member of The IIA's Twin Cities Chapter, Ostler has held numerous leadership positions, including Chapter President, over the past two decades.

NASBA: Auditing | Learning Level: Basic | CPE Credit: 1.2

11:20 AM – 12:20 PM PT | 1:20 – 2:20 PM CT | 2:20 – 3:20 PM ET

Session 3: Emerging Cyber and Cyber Regulatory Risks - from NIST Information Classification to Specific Industry Examples

Timothy Hediger, CIA, CCSA, CRMA, CISSP, CISA, ITIL
Director
MorganFranklin

The goal of this session is to discuss and highlight Q3 and Q4 2022 cyber emerging risks and their impact on internal audit organizations. The session will look at best practices, governmental, states' Attorneys General, and case law that internal audit departments should keep in mind for CY 2023 audit planning. More importantly, this discussion will provide specific cyber risk examples for attendees and their enterprises, including cryptocurrency, mergers and acquisitions, the US False Claims Act, and new NIST pronouncements.

In this session, participants will:

- Learn about cyber and cyber emerging risks, with a specific Q3 and Q4 2022 focus.
- Think a second time about CY 2023 cyber audit risk.
- Bring new guidance from NIST and other best practices to their organization, thus adding true value to their enterprise and internal audit brand.

Timothy Hediger is a well-rounded and trusted manager in IT security, cloud security, and GRC strategy (including FEDRAMP, AICPA SOC II reporting, ISO 18000/27000/31000 series, DISA, FIPS 140-2 (encryption), COVID/CARES Act, PCI, HIPAA, GDPR, CoBIT, NIST, and CA Senate Bill 1386). With two decades of leadership experience at EY, Deloitte, Costco Wholesale, GM Financial, and PRIDE Industries, Hediger has guided teams through multiple ERP, SIEM, IAM, ServiceNow CMDB, and GRC system implementations as well as cloud integrations. He has significant experience with both offshore (India and the Philippines) and US resources, along with client onsite resources. Hediger is also a well-regarded speaker.

NASBA: Auditing | Learning Level: Intermediate | CPE Credit: 1.2

12:30 – 1:30 PM PT | 2:30 – 3:30 PM CT | 3:30 – 4:30 PM ET

Session 4: Lessons Learned

Lisa Young, CISA, CISM, CISSP
Senior Metrics Engineer
Netflix

Cyber risk is business risk. In the face of a dynamic risk landscape, organizations continue to invest in independent activities for preparedness: incident response, information security, IT disaster recovery, business continuity, and the latest technologies. Given the complexity of today's business processes, cybersecurity benefits from a team approach. Hear lessons learned from cyber incidents and ransomware attacks and how taking a risk-based approach can improve security outcomes and minimize impacts to the business from realized risk.

In this session, participants will:

- Gain insights into how a risk-based approach differs from a controls-based approach in planning for incidents.
- Learn why capturing areas of concern across the organization can improve risk identification.
- Examine key cyber security capabilities that contribute to improved risk and incident management.

Lisa Young is an operational risk and security metrics professional with a passion for solving problems with data. She is a prominent cybersecurity veteran, having worked in government, military, industry, and academia. As a Security Metrics Engineer at Netflix, Young works across InfoSec to demonstrate the business value of GRC and enterprise resilience. She also serves on the board of directors at ISC2.org.

NASBA: Auditing | Learning Level: Intermediate | CPE Credit: 1.2