IIA / ISACA 2026 Hacker Conference
May 11-12 2026

Conference Theme:

Cobra Kai - Cyber Edition
Strike First, Strike Hard, No Mercy
vs
Defense over offense, protect others and inner peace

CISO Panel "Sensei Circle"
May 12, 2026 – 8:10 AM

Facilitator:
Christopher Pries, CPA, CIA, CRMA – Managing Director, Grosvenor Advisors LLC
Panelists:

- Glenn Kapentansky, CSO, Trexin
- Craig Youngberg, BISO, Abbvie
- Jeremy Mann, SVP Global Attack Surface Mgmt, Northern Trust Corporation

CISO Panel Abstract
Title: Attack vs. Defense: Navigating the 2026 Threat Multiverse
Information security leaders must choose their path: proactive aggression or balanced defense. This interactive "Sensei Circle" panel will explore critical domains of the 2026 threat landscape, including AI-driven exploits and third-party ecosystems — to determine how leadership styles impact audit outcomes and business resilience. Come for the drama of the "Sensei Circle," stay for the "Secret Scrolls" of advice on how auditors can effectively evaluate modern CISO programs in an era of constant disruption.

Learning Objectives

1. **Evaluate Contrasting Security Postures:** Attendees will be able to distinguish between "Offensive Defense" (Strike First) and "Strategic Resilience" (Miyagi-Do) methodologies, identifying how each approach impacts risk appetite and control effectiveness in a 2026 threat landscape.
2. **Assess the Impact of Agentic AI and Deepfakes on Identity Governance:** Participants will learn to identify the vulnerabilities created by autonomous AI agents and generative media, enabling them to design audit programs that verify identity beyond traditional multi-factor authentication (MFA).
3. **Analyze Third-Party Risk in Decentralized Ecosystems:** Attendees will be able to evaluate the limitations of traditional compliance artifacts (like SOC 2 reports) when overseeing "Shadow AI" and complex supply chain dependencies, shifting toward a model of continuous resilience verification.
4. **Translate Technical Cyber-Risk into Business-Centric Reporting:** Participants will gain strategies for auditing the "communication gap" between the CISO and the Board, learning how to quantify technical debt and security investments in terms of business continuity and strategic organizational value.

Method of Instruction: Interactive Panel Discussion with Case-Based Scenario Analysis
Recommended Knowledge Level: Intermediate
Prerequisites: None