Jim West Delivers Two Talks at ISACA GRC 2026 in San Diego

In both sessions, West challenges GRC professionals to move beyond awareness and into taking action now.

Jim West, CEO and Founder of TopCyberPro.com, presenting at the 2026 ISACA GRC Conference in San Diego.

SAN DIEGO, CA, UNITED STATES, August 19, 2026 /EINPresswire.com/ -- Award-winning cybersecurity expert, author, and TopCyberPro.com founder Jim West is speaking this week at the 13th annual Governance, Risk, and Control Conference, jointly presented by ISACA and The Institute of Internal Auditors (IIA), taking place August 17–19, 2026, in San Diego and virtually. The conference brings together governance, risk, control, audit, and cybersecurity professionals for world-class content, practical guidance, and forward-looking insight into today's most complex risk environment.

West is presenting one of his most requested sessions, "The Encryption Endgame: Beating the Quantum Clock," a timely and urgent presentation focused on the governance, risk, and operational impact of quantum computing on modern cryptography. First created and delivered by West in 2017, the talk has evolved alongside the quantum threat landscape and remains one of his most requested and longest-running sessions. The session examines harvest-now/decrypt-later risk, the exposure of sensitive long-life data, the weakening of legacy public-key cryptography, and the need for organizations to begin building quantum-readiness roadmaps now.

> Boards, risk leaders, auditors, CISOs, and system owners must stop treating quantum security as a distant issue and treat it as a resilience, disaster recovery, and trust-infrastructure issue.”
>
> *Jim West*

Drawing on the session's core content, West offers three pieces of guidance he considers non-negotiable for organizations navigating the post-quantum transition. First, because adversaries can capture encrypted data today and decrypt it once sufficiently powerful quantum computers

exist, organizations must secure sensitive communications now rather than waiting for a formal Q-Day announcement. Second, he urges organizations to build a complete cryptographic inventory and prioritize remediation based on how long specific data must remain protected, rather than migrating systems in an ad hoc order. Third, he recommends layering defenses using NSA's Commercial Solutions for Classified (CSfC) framework — built on the "rule of two," or two independent layers of cryptography — alongside Zero Trust architecture, giving organizations a defensible, field-tested bridge strategy while formal post-quantum cryptography standards continue to mature.

"Q-Day is not just a technology problem; it is a governance failure waiting to happen if organizations do not act," said West. "The encrypted traffic being captured today may become readable in the future. That means boards, risk leaders, auditors, CISOs, and system owners must stop treating quantum security as a distant science project and start treating it as a resilience, disaster recovery, and trust-infrastructure issue."

On the first day of the conference, West spoke on "The Art of War in Cybersecurity: Cybersecurity Strategy in an Ever-Changing Threat Landscape," highlighting how the approximately 2,500-year-old guidance is applicable today. Attendees interested in the strategic framework behind the session can find further detail in West's book, The Art of War in Cybersecurity, which expands on the themes covered in the presentation.

West brings an unusually broad perspective to the post-quantum discussion. With more than 35 years in cybersecurity, more than 100 professional certifications — including CISSP with all three ISC2 advanced concentrations (ISSAP, ISSEP, ISSMP), C-CISO, GPEN, CTIA, ECES, and CHFI — and thousands of continuing education hours across cryptography, governance, risk management, systems engineering, cloud, AI, Zero Trust, NSA security engineering, RMF, NIST, COBIT, ISO, CSfC, MBSE, and related frameworks, West approaches quantum security as an enterprise architecture and risk management challenge—not simply a cryptographic algorithm change. He currently serves as a Senior Cybersecurity Advisor supporting U.S. defense operations in EMEA (Europe, the Middle East, and Africa), and completes approximately 400–600 continuing education hours annually to stay current with technology changes.

West's recent thought leadership reinforces that message. In ISACA Journal, he authored "Commercial Cybersecurity in the Post-Quantum Era: Applying NSA CSfC Principles," published April 29, 2026, focused on adapting Commercial Solutions for Classified principles to improve cryptographic resilience. In GRC Outlook, his article "Q-Day and Disaster Recovery: Building a Quantum-Ready Resilience Playbook," reframed Q-Day as a disaster recovery and trust-restoration problem, emphasizing crypto inventory, crypto-agility, hybrid migration approaches, certificate reissuance, key rotation, and third-party readiness.

West was also recently profiled by CP Magazine in "The Man Who Could Save Cybersecurity," which highlighted his multi-domain approach across cybersecurity, engineering, architecture, governance, risk management, and emerging technologies. The profile noted his long-running

warnings about harvest-now/decrypt-later attacks, his advocacy for crypto-agility and layered security architectures, and his ability to integrate multiple frameworks into a unified method for solving complex cybersecurity problems.

Through both sessions at ISACA GRC 2026, West challenges GRC professionals to move beyond awareness and into action — whether the threat is quantum decryption or the broader, ever-shifting cybersecurity landscape. His core message is direct: the clock is already ticking, and the organizations that inventory, prioritize, engineer, and govern their dependencies today, with strategy as sharp as their adversaries', will be the ones best positioned to withstand what's next.

Michelle Kaldenberg
TopCyberPro.com
+1 832-303-4593
email us here
Visit us on social media:
LinkedIn