11th Annual IT Hacking Conference – Presenters

Roger Grimes
KnowBe4

Presentation:
Talking Cyber Risk Quantification to your Board
How AI Impacts Patch Management

Last year, we had over 48,000 publicly announced vulnerabilities. That's over 132 a day, day after-day, and each year the number of vulnerabilities just keeps going up. AI is going to cause the number of vulnerabilities found and exploited to soar! Attend this session to learn:

- How AI will impact vulnerabilities
- The reality of hackbots
- How AI will impact patch management

Bio:
Roger A. Grimes, CPA, CISSP, CEH, MCSE, CISA, CISM, CNE, yada, yada, CISO Advisor for KnowBe4, Inc., is the author of 16 books and over 1600 articles on computer security, specializing in host security and preventing hacker and malware attacks. Roger is a frequent speaker at national computer security conferences and was the weekly security columnist at InfoWorld and CSO magazines between 2005 - 2019. He has worked at some of the world's largest computer security companies, including, Foundstone, McAfee, and Microsoft. Roger is frequently interviewed and quoted in the media including Newsweek, CNN, NPR, and WSJ. His presentations are fast-paced and filled with useful facts and recommendations.

- Email: roger@banneretcs.com
- LinkedIn: https://www.linkedin.com/in/rogeragrimes/ (Top 2% industry influencer)
- X/Twitter: @rogeragrimes
- Reddit: r/rogeragrimes (top 1% poster)
- YouTube: @CyberSecWTFRants
- TikTok: https://www.tiktok.com/@rogeragrimescswtf
- Instagram: https://www.instagram.com/rogeragrimes/

11th Annual IT Hacking Conference – Presenters

Ryan Rene R.

Presentation:

<u>You Can't Audit What You Don't Understand: AI Risk & the OWASP Top 10 (Don't Avoid It, Embrace It)</u>

This session is a practical, plain language walkthrough of the most critical risks emerging from modern AI systems—especially LLMs and agentic AI—using the OWASP Top 10 for LLM Applications (2025) and the OWASP Top 10 for Agentic Applications (2026) as your roadmap. We'll translate each risk category into what it actually looks like in real environments in LLM systems and with agentic AI—where systems don't just "generate," they act.

You'll leave with a pragmatic approach to protecting data in AI workflows—what to require, what to test, and what to monitor—so you can move from AI anxiety to AI assurance. The audience will leave with practical insight into what to assess in AI systems, how to apply existing security and control frameworks, and why AI risk remains a human problem one that requires judgment, oversight, and defensible evidence (aka AI won't take your job).

At the end of the campaign, you will learn (takeaways):

- What the OWASP AI Top 10 is and why it's relevant
- Where AI introduces material security and data risks
- What leaders should secure and audit in AI deployments

Bio:

Ryan René Rosado is a dynamic emerging leader and respected voice in the cybersecurity community, with 15 years of experience across public, private, and academic sectors. She is a Teaching Assistant at Harvard Extension School and Advisor to Ally Security. With roots as a US Air Force Cyber Intelligence Analyst, Ryan went on to strengthen the security posture of leading organizations such as EY, Accenture, and Optiv. She's enrolled in the cyber graduate program at NYU Tandon and holds dual BS degrees in Cybersecurity (Utica College) and Disaster Management (SUNY Empire State College). She was named an AFCEA Emerging Leader in 2018. She has presented at multiple conferences and on many podcasts. Ryan is passionate about mentorship, leadership, emerging tech, and building community.

11th Annual IT Hacking Conference – Presenters

Andrew Belsick
BDO

Kelly Austin
BDO

Presentation:

Strike First, Audit Hard: No Mercy for AI Risk

AI isn't magic—it's another technology with threats, risks, and controls. The difference is that these risks can emerge quickly and in unexpected ways, sometimes sweeping the leg before you're ready. This session breaks down how to audit AI with those risks in mind, focusing on issues like bias, hallucination, data governance/integrity, and misuse. Auditors will leave knowing what questions to ask and how to go beyond the compliance checkbox to truly safeguard their organizations.

Remember: In the world of AI, strike first, strike hard, no mercy.

Learning Objectives: Learn how to

1. Deconstruct AI into audible components
2. Identify AI risk scenarios
3. Evaluate AI governance and control effectiveness

Bios:

Andrew is a GRC, cybersecurity, privacy, and business resilience leader with over 20 years of experience across multiple industries, including financial services, retail, healthcare, and manufacturing. Andrew is a trusted advisor to his clients and leads efforts to identify risks and design effective mitigation strategies that enable business outcomes. Andrew has experience advising and delivering services in the areas of technology risk/compliance, third-party risk, security operations, incident response, vulnerability management, privacy risk/compliance,

and business resilience. Andrew has implemented technology risk assessment programs that enable both compliance and business strategy and provide data-driven insights that enhance business risk decisions. He has also developed generative artificial intelligence (GAI) guidance to responsibly leverage these technologies across business and technology stakeholders.

Andrew is a Certified Information Security Manager (CISM), Certified in Risk and Information System Control (CRISC), and a Certified Information Systems Auditor (CISA). Prior to joining BDO, Andrew most recently led the cybersecurity operations, vulnerability management, GRC, privacy, and business resilience functions at a Fortune 300 retailer; Nittany Lion graduate in Business Administration

Kelly is an Experienced Senior Associate in BDO's Privacy & Data Protection practice, where she leads and supports complex, multi-workstream privacy initiatives across global regulatory environments. She specializes in designing and operationalizing privacy programs, conducting Privacy Impact Assessments (PIAs) and AI-risk assessments, maturing data inventories, and developing policies, notices, and procedures. Kelly has driven large program implementations involving privacy frameworks, governance models, data review, privacy technology deployment, data subject request operations, cookie compliance, and assessment processes. Across her portfolio, Kelly excels in managing complex workstreams, coordinating cross-functional stakeholders, and delivering high-quality outputs. She has extensive experience supporting Data Protection Officer (DPO) functions, including handling individual rights requests, addressing privacy concerns, and engaging with regulatory authorities. Her work also spans comprehensive privacy assessments, regulatory compliance evaluations, and project-based advisory support across complex data use, regulatory readiness, and remediation initiatives.

11th Annual IT Hacking Conference – Presenters

Shannon Moran
Herzum

Presentation:

One Gate, One Way: Identity in the AI Age (Single Sign-On)

Don't let security slow down your AI ambitions. As organizations accelerate AI adoption, identity management and single sign-on have become both critical enablers and concentrated risk points. This session explores how to protect knowledge documentation and sensitive data while enabling AI-powered search across the enterprise—without weakening security or governance. Attendees will learn how stronger identity controls, access discipline, and governance frameworks can improve compliance, reduce AI-related risk, and ultimately allow the business to move faster with confidence.

Like karate, AI security isn't about brute force—it's about discipline, preparation, and knowing exactly who has access before the first move is made.

Learning Objectives: Learn how to

1. Protect knowledge documentation
2. Improve compliance and governance of your organization
3. Move faster by allowing AI search across your organization by having better security protections in place

Bio:

Shannon Moran, MCIS, is an accomplished sales manager with extensive experience in technology and consulting sectors. Currently serving as the Sales Manager at Herzum, an international consulting firm specializing in Agile & DevOps and Atlassian products, Shannon previously held significant roles including US East Coast Sales Director at Jscrambler, where leadership encompassed the Eastern half of Canada, and Regional Sales Manager at Splunk, managing enterprise negotiations with major clients. Previous experiences also include Enterprise Application Sales Manager at Oracle, National Sales Director at Comscore, and various sales positions at Adobe, CBS, and Verizon. Shannon holds a Bachelor's degree from Fordham University and a Master's degree in Computer Information Systems from Elmhurst University.

11th Annual IT Hacking Conference – Presenters

Rajath Srinvasa

Presentation:

Quantum Strike: Re-Thinking the Data Protection Horizon

As enterprises evolve their data protection controls to support AI at scale, quantum computing introduces a fundamental shift to the security and control environment. This session examines how quantum advancements will impact encryption, identity, and data protection architectures—and what that means for governance, compliance, and risk management. Attendees will gain practical insight into how data protection implementations will change and how daily business, security, and audit functions must adapt to remain resilient in a post-quantum world.

In the face of quantum disruption, mastery comes not from reacting fast—but from training early, maintaining balance, and strengthening defenses long before the match begins.

Learning Objectives:

1. Understand the impact of quantum computing on enterprises
2. Identify how data protection implementations will evolve
3. Anticipate how daily business and security functions will change

Bio:

Rajath is a cybersecurity expert specializing in cloud risk mitigation and data-centric threat defense. With more than six years of experience in Technology Risk consulting, Rajath has navigated the security landscapes of global financial institutions and tech giants, including his recent work developing security guardrails for AWS. He graduated with a Master's in Computer Science degree from Georgia State University. When he isn't securing cloud environments, Rajath spends his time diving into non-fiction literature and biographical documentaries.

11th Annual IT Hacking Conference – Presenters

Santosh Vasudevan

Sessions:

1) Know Your Enemy: AI Fraud Detection

Fraud is evolving faster than traditional rule-based controls and periodic audits can adapt. This session explores how modern AI techniques can help organizations detect emerging fraud risks earlier and with greater confidence. Attendees will see how structured data signals and unstructured evidence can be combined to generate explainable, audit-ready insights rather than opaque model scores. The session focuses on practical implementation patterns, governance considerations, and real-world lessons from deploying AI systems in enterprise environments. Participants will leave with a clear framework for building scalable, evidence-driven fraud detection capabilities that augment human judgment rather than replace it.

Participants will learn how to:

- Understand core AI techniques used in fraud detection and anomaly identification
- Combine structured transaction signals with unstructured evidence to enable explainable investigations
- Design governed AI workflows that support auditability, transparency, and regulatory review

2) Breakout Session - Fraud Detection Case Study

This interactive break-out sessions presents participants with a realistic fraud scenario and invites them to design an end-to-end investigation workflow using the methods and tools they currently rely on. Through guided discussion, attendees will identify the data sources they would review, the steps they would take to validate concerns, and the challenges they commonly face in manual investigations. The session then explores how artificial intelligence and data-driven tools can be applied to accelerate evidence gathering, improve consistency, and support clearer documentation, while preserving professional judgment and governance requirements. Participants will leave with a practical understanding of where AI can enhance existing workflows rather than replace them.

Participants will learn how to:

11th Annual IT Hacking Conference – Presenters

- Outline a structured, end-to-end fraud investigation workflow using current practices
- Identify common bottlenecks and risks in manual review and documentation processes
- Recognize practical opportunities where AI and data tools can augment speed, consistency, and decision support while maintaining human oversight and accountability

Bio:

Santosh Vasudevan is a Data Scientist specializing in building AI-driven anomaly detection and continuous monitoring solutions for large enterprise data environments. He brings close to a decade of experience designing scalable machine learning systems, automated data pipelines, and business intelligence products across financial services, retail, and engineering domains. Santosh began his career as a Control Systems Engineer before pivoting into data science, bringing a strong foundation in engineering and systems thinking to his work. He holds a bachelor's degree in Instrumentation Engineering from RV College of Engineering (Bangalore, India) and master's degrees in Business Analytics and Project Management from the University of Connecticut. Santosh actively contributes to professional and research communities focused on the practical and responsible adoption of AI and machine learning. Outside of work, he enjoys CrossFit, distance running, yoga, stand-up comedy, concerts, and live sporting events.

11th Annual IT Hacking Conference – Presenters

Valerie Nielsen
Inside Edge Risk Advisors

Sessions:

The Risk of Inaction

In the rapidly evolving landscape of cybersecurity, the choice to act or not can have profound implications for organizational security, reputation, and financial health. While there is an inherent risk in acting regarding implementing new technologies, following protocols, or addressing emerging threats; there is a far greater and more underestimated risk in failing to act when action is needed. The goal is to spark conversation about the invisible yet potent danger of hesitation. The presentation will delve into the nuances of risk assessment, showcasing how we can balance the scales between action and inaction. It will illustrate real-world scenarios where inaction led to catastrophic breaches or prolonged vulnerabilities. Conversely, it will also examine cases where taking calculated risks proved transformative in mitigating threats and enhancing resilience.

Learning Objectives:

1. Understand the risks associated with inaction in cybersecurity, including the potential for breaches, reputation damage, and financial loss.
2. Assess risks when deciding whether to act or not to ensure informed decision-making across leadership stakeholder groups.
3. Discover tools and strategies to build a proactive culture within organizations that prioritize calculated action over avoidance or stagnation.

Bio:

Valerie is a Risk Executive with expertise across Incident Response, Fraud Investigations, Compliance, Governance, Third Party Assurance, Information Security Awareness, and Geopolitics. She has been recognized by LinkedIn as a Top Voice and influencer.
She has created and led risk management for $2B and $5B revenue business units at Aon.

11th Annual IT Hacking Conference – Presenters

Russell Safirstein
NexAI Cyber

Presentation:

Can AI Bridge the Security Gap

Most security programs will fail in the next three years—not because they lack budget or tools, but because they still rely on humans to reason through machine-speed chaos. Attackers are already using AI to automate reconnaissance, exploit paths, social engineering, and real-time adaptation. Meanwhile, defenders are overwhelmed by alerts, dashboards, and compliance checklists. The imbalance is structural—and growing.

The real question is no longer, "Do we have the right tools?"
It is, "Can we think and act faster than automated adversaries?"

This session challenges the traditional security operating model and introduces an emerging approach combining biomimetic digital twins, chaos modeling, and agentic AI to rethink how cyber risk is understood and managed. Rather than adding headcount or another platform, the focus is on re-architecting security for speed, adaptability, and resilience.

Learning Objectives:

1. Learn how to diagnose the Cybersecurity Execution Gap,
2. Apply Advanced biomimetic digital twins, chaos modeling and agentic AI to security operations, and
3. Examine how audit and risk management can move from static compliance checklists to dynamic, continuously simulated risk environments.

Bio:

Russell Safirstein is a board member, executive advisor, and innovative thinker known for delivering non-traditional solutions to complex business challenges. By integrating technology, audit, accounting, risk, and compliance, he has driven growth, resilience, and transformation across multiple industries. Russell has delivered more than 40 keynotes and presentations at leading organizations, including the Harvard Club, American Bar Association, NYSSCPA, and the Institute of Internal Auditors.

He currently serves as CEO of NexAI Cyber, a cybersecurity risk and AI services firm, and is Co-Founder and COO of RYLTI, a cognitive AI-as-a-service company focused on complex data and business opportunity. Russell previously served as a Partner at two global accounting firms, held multiple CAE roles, and is a licensed CPA.

11th Annual IT Hacking Conference – Presenters

Stewart Deken
RubinBrown

Presentation:

Tales from Forensics Investigations

The modern business landscape is fraught with danger, and when something happens, whether internal or external, a good forensic investigation is often the difference between knowing what happened and how to prevent future occurrences and just guessing. We'll discuss some real-world scenarios and lessons learned to help give you an edge in responding to a variety of unexpected occurrences. This will keep you safe and make sure you have a plan in place if/when something happens. Also, catching or stopping bad guys is fun.

Learning Objectives:

- Name the four goals of a BEC response
- Apply some simple preventive techniques
- Determine when you may need outside assistance

Bio:

Stu Deken is the Digital Investigations Manager at RubinBrown and assists clients with a wide variety of cyber security and computer forensic engagements. Prior to joining the firm, Stu spent twenty years as a police officer in the St. Louis metro area and served on a cybercrime task force for five years. He has assisted federal, state, and local investigators and prosecutors with forensic investigations and analysis and served as an FBI Task Force Officer. Stu has testified in both state and federal court as an expert witness and attended training with the secret service and the FBI. Stu has a Master's Degree in Cyber Security and holds several forensic and cyber certifications including the CFCE and the CISSP. When he's not boring everyone by talking about forensics, he enjoys reading, watching movies, and spending time with his family in Minneapolis.

11th Annual IT Hacking Conference – Presenters

Jason Torres
Memorial Sloan Kettering Cancer

Presentation:

Making Threat Intelligence Operational

As threat intelligence data volumes continue to accelerate and security teams face growing pressure to reduce detection times and prevent breaches, organizations struggle with a critical operational challenge: translating abundant threat data into timely, automated defensive action. The rapid proliferation of threat feeds has blurred the boundaries between awareness and operationalization. This talk examines how organizations can reshape threat intelligence strategies and shift intelligence from passive awareness into active defense.

As Mr. Miyagi would say, ""Know the threat. Shape the response. Act with purpose."

Participants will share perspectives on:

- Defining Operational Intelligence
- Prioritizing Intelligence Data Sources
- Security Tool Stack Integration
- Measuring Effectiveness

Bio:

Jason is a seasoned cybersecurity and risk management leader with over 20 years of experience developing and leading security programs in complex healthcare and academic environments. As Associate Director of Security Threat & Incident Management at Memorial Sloan Kettering Cancer Center, he oversees SOC, Incident Response, Threat Intelligence, and Enterprise Security operations. Known for his collaborative leadership and strategic approach, Jason builds trusted teams that align technical excellence with business priorities. Outside of work, he enjoys traveling with his family to all 50 states, golfing, and cheering on the Chicago Bears.

11th Annual IT Hacking Conference – Presenters

Velu Natarajan

Krishnakumar K. Mohanram

Presentation:

Auditing AI in the Lakehouse: Centralized Catalog Controls for LLMs on Sensitive Data

This session introduces an approach that uses the enterprise data and AI catalog as the primary enforcement point for governing how LLMs access regulated datasets. By integrating identity, metadata, data classification, and model governance into a single control plane, organizations can safely enable AI innovation while maintaining auditability, compliance, and regulatory defensibility.

Learning Objectives:

- Learn policy-driven LLM access based on data classification and identity
- Build End-to-end lineage from source tables to AI outputs
- Continuous population-level testing of AI data usage

Bio:

Velu Natarajan is a data architecture leader with 20+ years of experience designing and modernizing scalable, secure, high-performance data platforms. As a leader within his organization's Cloud Center of Excellence, he drives cloud modernization programs to build AI-ready data cloud platforms. His work strengthens governed data access, enables scalable analytics, and accelerates adoption of LLM and advanced AI workloads across enterprise environments.

Velu emphasizes cross-functional collaboration, self-service enablement, and measurable guardrails for performance, security, and cost as AI expands access to shared, interoperable data across platforms. Velu is also an author, technical reviewer, and conference speaker. Velu currently serves as a Principal Data Engineer at GoodRx. Outside of work, he enjoys watching epic films and playing soccer with his kids.

LinkedIn Me: **https://www.linkedin.com/in/velunatarajan/**

11th Annual IT Hacking Conference – Presenters

Krishnakumar Kunka Mohanram is a cloud security and assurance specialist focused on Oracle Cloud Infrastructure (OCI) security, auditability, and control automation. He enables audit-ready OCI environments through centralized logging, audit trails, network security change monitoring, and evidence-driven compliance using cloud telemetry. He designs practical cloud security guardrails that strengthen identity, network, and workload protections while supporting scalable governance. His work bridges internal audit expectations with cloud engineering practices by turning real-time operational signals into repeatable audit artifacts and continuous control monitoring. Krishnakumar is also an author, technical reviewer, and frequent speaker.

Krishnakumar currently serves as a Principal Cloud Architect at Infolob Global. Beyond his professional work, he is actively involved in community initiatives and enjoys playing cricket.

LinkedIn Me: **https://www.linkedin.com/in/krishnakumar-mohanram/**

11th Annual IT Hacking Conference – Presenters

Vinita Apte
Circle

Presentation:
Building and Auditing an AI-Driven Third-Party Security Program
AI is rapidly reshaping third-party risk management, transforming how organizations assess vendors, monitor risk, and make security decisions. Drawing on 15 years of experience in vendor security and third-party risk, this session provides a practical, real-world guide to building and auditing an AI-driven third-party security program.

The first half walks through a step-by-step approach to integrating AI into vendor security assessments, including intake, due diligence, risk scoring, continuous monitoring, and workflow automation. The second half shifts to the auditor's perspective, exploring how to evaluate consistency, accuracy, and governance.

In third-party risk, AI brings speed—but harmony comes when human judgment shapes how intelligence is applied, governed, and acted upon.

Attendees will leave with implementation lessons, and audit-ready practices to ensure that AI strengthens — rather than complicates — third-party security and risk management efforts.

Bio:
Vinita is a cybersecurity leader with a passion for building strong security programs and tackling complex security challenges. With a background in engineering, she's worked across third party security, Blockchain security, data loss prevention and AI-driven security automation. Currently, as Director of Security at Circle, Vinita ensures vendors, blockchains, and partners meet top-tier security standards.

Beyond work, Vinita calls Chicago home, where she lives with her husband and two kids. She enjoys hiking, art, and photography.

11th Annual IT Hacking Conference – Presenters

Ryan Ferran
BPM

Presentation:

How Read Teams Break Into Buildings and How You Can Stop Us

Learn all about physical security in the modern landscape and how it is actually a layer of cybersecurity. For organizations of all size/types, understand the nuances of protecting your networks and computers from physical attacks. Hear the details of how to examine your own physical security posture.

Learning Objectives:

1) Evolution of door and lock security of both the analogue (physical) and electronic varieties
2) Physically protecting computer networks
3) Protecting critical infrastructure

Bio:

Ryan holds degrees in Mathematics and Computer Science, which has provided the basis for his career in multiple technical fields, including over 10 years in IT system administration. After moving to offensive security in 2017 Ryan has completed over 200 highly technical penetration tests across a wide variety of industries. He leads the physical security team and performs in-person social engineering testing and rigorous physical security audits. Ryan has a personal and professional passion for Operational Technology (OT) assessments, and he has spent years mastering a thorough and delicate methodology to safely test organizations with OT considerations such as power companies, water treatment facilities, and industrial manufacturing. These areas of specialization are his passion, helping to secure critical infrastructure that supports the everyday lives of all people provides the largest impact for the skills he has developed throughout his career.