iSMG Studio

at Infosecurity Europe 2025

Infosecurity Europe 2025: Securing an Uncertain World

Once again, Infosecurity Europe hosted cybersecurity, technology, legal and other leaders from the U.K., Europe and around the world, but this year the world's security posture was a little more uncertain.

As a media partner of this year's event, Information Security Media Group staffed a video studio on the Infosecurity Europe 2025 expo hall floor, gathering insights from CEOs, CISOs, government leaders, researchers and more. While experts discussed the latest technology innovations in artificial intelligence, data protection and cyber defense, they also warned that ransomware attacks are becoming more disruptive and geopolitical tensions are triggering new threats.

The many interviews we produced at the event capture all of these insights and more. These videos, created by ISMG.Studio, our unparalleled platform for cybersecurity and technology leaders hosted at major events worldwide, are featured across our news sites. We also captured insightful discussions with members of ISMG's lively CyberEdBoard community. In these pages, enjoy the in-depth interviews conducted by our seasoned editorial team about how cybersecurity teams are safeguarding this fast-changing world.

Mathew Schwartz

Mathew Schwartz
Executive Editor, DataBreachToday and Europe
Information Security Media Group

Visit us online for more ISMG at Infosecurity Europe coverage

ISMG.Studio

Video Interviews

Security by Design, Not by Retrofit

Acumen Cyber's **Kevin Robertson** on Cloud Security During Digital Transformation

Many organizations embrace digital transformation without embedding security early on. Kevin Robertson, CTO and co-founder of Acumen Cyber, shares insights on why retrofitting controls after cloud migration rarely works and the often-misunderstood shared responsibility model.

WATCH ONLINE

Why AI Needs Stronger Laws, Not Just Smarter Tech

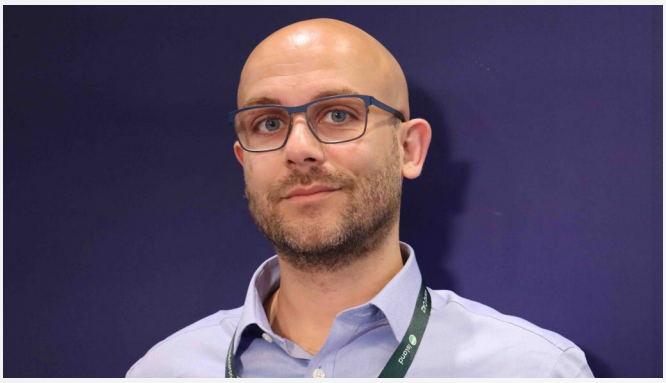
Andrea Isoni of AI Technologies on Certifications, Deepfakes and ISO 42001

AI misuse - from deepfakes to cyber incidents - continues to outpace regulation. Andrea Isoni, chief AI officer at AI Technologies, shares why stronger cyber laws, certification frameworks like ISO 42001 and risk-based prioritization are necessary to manage AI risks safely and compliantly.

WATCH ONLINE

Behavior Data Now Key to Cyber Risk Posture

Frost & Sullivan's **Stahnke** on How Human Risk Insights Drive Better Threat Response



Legacy cybersecurity training often fails because users skip the content or treat it as a compliance task. Forward-looking organizations now recognize that human behavior is a critical piece of their security posture, said Claudio Stahnke, industry analyst at Frost & Sullivan.

WATCH ONLINE

Law Firms Face New Supply Chain Risk Pressures From FIs

Pinsent Masons' **Mike Seeney** Says Financial Services Clients Demand More Resilience

Financial services clients are pushing law firms harder on third-party resilience, backup and disaster recovery capabilities. Legal services providers must balance client demands with their operational realities, said Mike Seeney, head of information supply chain risk at Pinsent Masons.

WATCH ONLINE

Ransomware Resilience, Identity-Based Threats and Data Visibility Gaps

Rubrik's **Kev Johnson** on the State of Data Security

Most organizations manage data across SaaS, cloud and on-premises systems - and nearly as many operate in multiple cloud environments. This fragmentation leaves critical visibility gaps that attackers exploit, said Kev Johnson, staff technical marketing manager at Rubrik.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, Johnson also discussed:

- How data visibility gaps leave organizations vulnerable;
- Why ransomware resilience requires more than prevention;
- Why identity-based threats demand behavioral monitoring.

WATCH ONLINE

> "Having visibility is the first step in being able to manage your sensitive data risk."
>
> - ***Kev Johnson***

AI Is Redefining Data Risk. What CISOs Need to Know About the Security Shift

Varonis Field CTO **Matt Lock** on Shadow AI, Managing Risks and Path to Safe Adoption

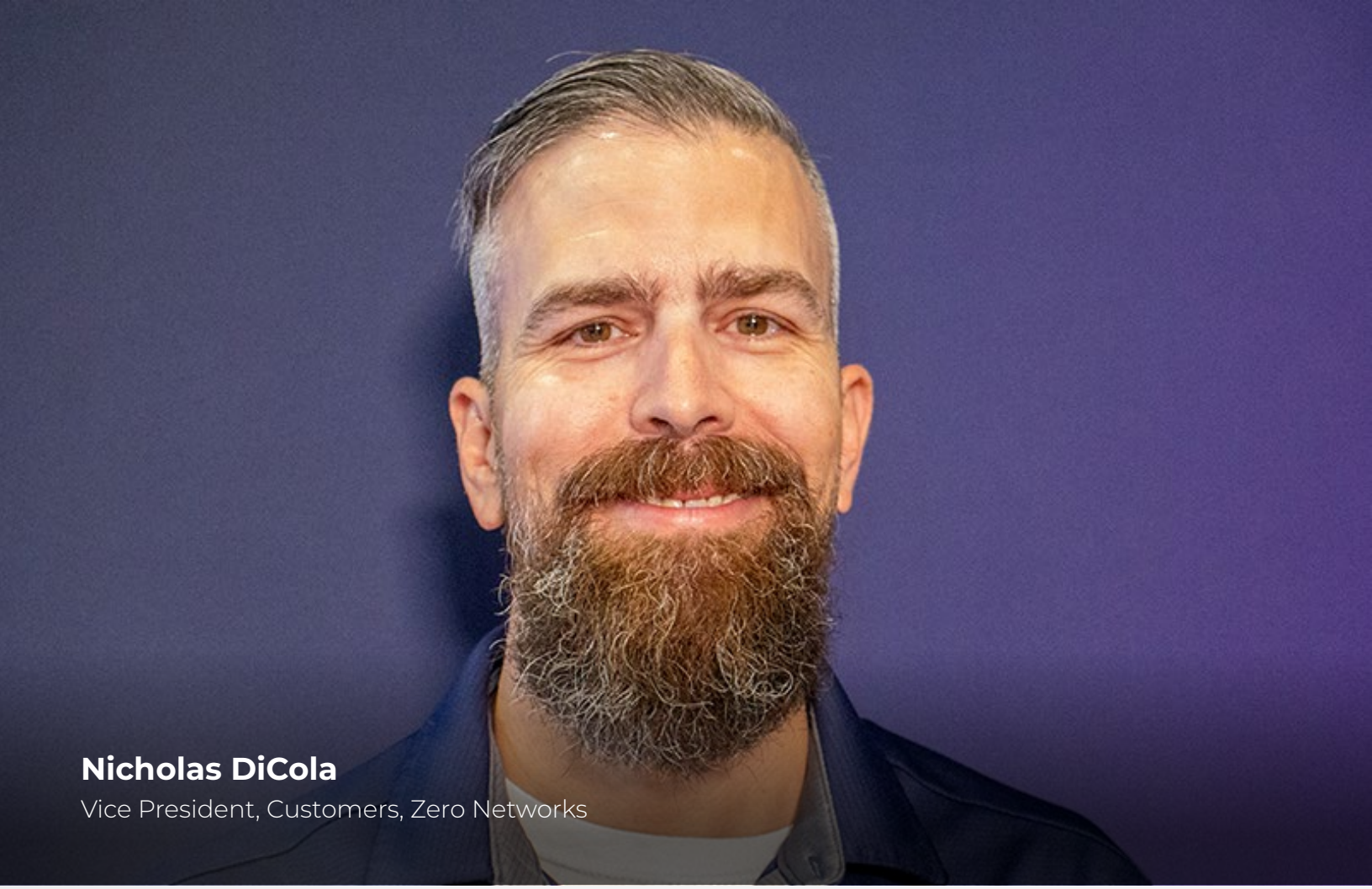
As AI adoption accelerates, traditional perimeter-based controls have failed to keep pace. The widespread reliance on internal trust and outdated protections leaves organizations vulnerable, said Matt Lock, field CTO for the EMEA region at Varonis.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, Lock also discussed:

- Why automation requires context, confidence and gradual implementation;
- The importance of data ownership;
- The need for policy-based access and stakeholder education to support safe AI use.

WATCH ONLINE

> "PII and source codes are being uploaded into these AI tools to make them more effective ... it's inevitable that those models will start to use that sensitive information to train themselves and get better."
>
> - ***Matt Lock***



Automation Accelerates Microsegmentation for Security Teams

Zero Networks' **DiCola** on How Modern Segmentation Helps Limit Ransomware Movement

Microsegmentation is often delayed due to its complexity and resource demands. Nicholas DiCola, vice president, customers, at Zero Networks, shares how automation simplifies microsegmentation by replacing manual rule-building.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, DiCola also discussed:

- Automating connection analysis and rule creation for faster segmentation;
- Using just-in-time multifactor authentication to block privileged ports and prevent ransomware spread;
- Building a zero trust architecture through network, identity and remote access security.

WATCH ONLINE

> "With automation, we use a very deterministic engine to automate learning what's already involved in the environment, what's already connecting to each other, and build those rules for the customer so that they can do a light validation of those rules."
>
> – ***Nicholas DiCola***

“Organizations still have to respond to a rapidly evolving regulatory landscape - a topsy turvy landscape from a geopolitical and risk intelligence perspective.”

Paul McKay
Vice President, Principal Analyst, Forrester

Europe Is Elevating Cyber Resilience in Critical Infrastructure

Forrester's **McKay** and **van der Hout** on How Regulations Are Driving Cyber Resilience

Security leaders worldwide are elevating resilience in cyber strategies, where Europe emerges as a frontrunner globally in protecting critical infrastructure. Driven by regulation such as NIS2 and DORA, its cybersecurity posture reflects strong resilience planning amid increasing disruptions.

WATCH ONLINE

Help Desk Hoax: How Attackers Bypass Tech Defenses

Team Cymru's **Thomas** on Social Engineering, Insider Threats and Supplier Compromise

Social engineering attacks against major British retailers have exposed critical vulnerabilities in corporate cybersecurity defenses. The attacks typically begin with threat actors calling IT help desks to reset employee credentials, said Will Thomas of Team Cymru.

WATCH ONLINE

Under Pressure: The Hidden Cybersecurity Threat

Bronwyn Boyle of Cybermindz on Why Psychological Resilience Is Mission Critical

Cybersecurity burnout isn't just a well-being issue, it's a security vulnerability. "If we're optimizing our tech stack, we should optimize our psychology stack as well," says Bronwyn Boyle, CISO and U.K. board member at Cybermindz.

WATCH ONLINE

Shared Intel Helps Law Enforcement Disrupt Ransomware Groups

Coveware's **Magnus Jelen** on How Early Preparation Prevents Future Compromises

Cybercriminals are evolving their tactics under law enforcement pressure. Magnus Jelen, lead director of incident response at Coveware/Veeam, says organizations must prepare before ransomware strikes. Proactive communication can help authorities disrupt threats and prevent future compromises.

WATCH ONLINE

Robert Hann
Global Vice President, Technical Solutions, Entrust

Taming Cryptographic Sprawl in a Post-Quantum World

Entrust's **Hann** Says Visibility, Control Are Key to Managing Cryptographic Assets

Most organizations have created a tangled mess of keys, certificates and protocols, making it nearly impossible to manage their cryptographic estate effectively, said Robert Hann, global vice president of technical solutions at Entrust.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, Hann also discussed:

- How poor cryptographic visibility increases key theft and regulatory risk;
- Why post-quantum readiness requires streamlined cryptographic management;
- How centralized platforms enable better decisions, faster migrations and improved security.

WATCH ONLINE

> "Stealing cryptographic keys is very advantageous. You get far more than just stealing a password from a user. Once you have the key, you have the keys to the kingdom."
>
> - ***Robert Hann***

“I think it's probably easier than it's ever been to become a cybercriminal.”

William Lyne
Head, Cyber Intelligence, National Crime Agency

“It's important that we get that intelligence so it can be properly actioned and we can take immediate steps to protect critical national infrastructure.”

James Morris
Chief Executive, U.K.'s Centre for Cyber Security and Business Resilience

Ransomware 3.0: A Glimpse Into the Post-Trust Ecosystem

National Crime Agency's **William Lyne** on Fragmentation, Cartels and AI in Ransomware

"I think it's probably easier than it's ever been to become a cybercriminal," says William Lyne, head of cyber intelligence at the National Crime Agency, as he discusses how fragmentation, pure extortion and AI are redefining the ransomware threat landscape.

WATCH ONLINE

UK Prepping Legislation to Strengthen Cybersecurity Defenses

CSBR's **James Morris** Details Proposed Cyber Security and Resilience Bill

James Morris, CEO of the U.K.'s Centre for Cyber Security and Business Resilience, details how proposed cybersecurity legislation would expand regulators' powers, and expand the definition of critical infrastructure and incident reporting requirements, to bolster both national resilience and trust.

WATCH ONLINE

The Casino Approach: Why CISOs Should Play to Win

Rapid7's **Thom Langford** on Why CISOs Should Embrace Rather Than Avoid Risk

Security leaders have always viewed risk as something to eliminate, but they should adopt a “casino” mindset for risk management. It's extremely rare for a casino to go bankrupt because they understand and embrace risk rather than let things happen to them, says Thom Langford, EMEA CTO at Rapid7.

WATCH ONLINE

Legacy Systems and Policies Expose West to Cyber Disruption

Ciaran Martin Urges Increased Focus on Essential Service Continuity, Resilience

China's ability to monitor and disrupt Western infrastructure demands a major shift in cybersecurity thinking. Ciaran Martin, a professor at Oxford University, said avoiding fear-driven narratives and focusing instead on service continuity and resilience is of paramount importance.

WATCH ONLINE

“I hate hype in cybersecurity, it's really, really damaging.”

Ciaran Martin
Professor, Oxford University; Director, CISO Network, SANS Institute

Enterprise Browser Transforms App Delivery and Compliance

Steve Tchejeyan on How Island's Browser Platform Enables Secure Workflows

Island's enterprise browser optimizes app performance, enhances data controls and simplifies compliance - all while improving user productivity and reducing legacy IT burdens, says Island President Steve Tchejeyan.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, Tchejeyan also discussed:

- Application-specific controls at the browser's presentation layer;
- Regulatory compliance through real-time data boundary enforcement;
- VDI and VPN dependencies, improving the experience for employees and contractors.

WATCH ONLINE

> "Now finally, cyber can give a tool back with infrastructure to the end users, to the employees, but can actually insert ambient security in the workflow of their day-to-day function."
>
> - ***Steve Tchejeyan***

Vulnerability Databases Face Accuracy and Access Gaps

VulnCheck's **Garrity** on the Uncertainty of the CVE Ecosystem and EUVD's Limitations

Funding shortages and incomplete coverage in critical vulnerability databases are increasing the risk for defenders. Patrick Garrity, security researcher at VulnCheck, discusses how data gaps and scoring confusion hinder response strategies for potential cyberattacks.

WATCH ONLINE

CyberEdBoard Insights: Ian Thornton-Trump

Inversion6 CISO on Help Desk Gaps, IAM Failures and AI Detection

Recent attacks on Marks & Spencer and Co-op reveal critical gaps in identity and access management and help desk functions. Ian Thornton-Trump, CISO at Inversion6, explains why retail has become a prime target and why help desk resilience and identity governance must be rethought.

WATCH ONLINE

CyberEdBoard

Predicting CVE Threats Beyond Conventional Scores

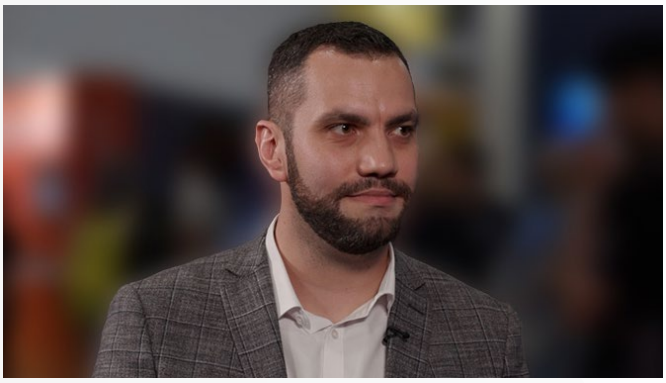
runZero's **Tod Beardsley** Outlines Flaws in Conventional Vulnerability Scoring Systems

Security teams are overwhelmed with CVEs, often struggling to prioritize the critical ones. To address this challenge, Tod Beardsley, vice president of security research at runZero, outlines how prediction systems can help identify vulnerabilities with serious risk.

WATCH ONLINE

Ransomware Response: Real-World Lessons From the Frontlines

Kivu's **Saunders** on Threat Actor Tactics, Negotiations and Intelligence Gathering



Ransomware negotiations aren't just about paying criminals, they're about gathering intelligence. "There's a misconception around threat actor negotiation that if you're going to speak to a threat actor, you're ultimately going to go and pay them," said Kivu's Daniel Saunders.

WATCH ONLINE

Boards Leave CISOs Exposed to Legal Risks

Attorney **Jonathan Armstrong** Says Board Diversity Must Include Cybersecurity Skills

Many boards lack cybersecurity expertise, leaving CISOs exposed to legal risks. New fraud laws and AI regulations compound the challenge as security leaders struggle for boardroom support, said Jonathan Armstrong, partner at Punter Southall Law.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, Armstrong also discussed:

- The importance of rehearsing data breach responses with key team members missing;
- How CISOs need enhanced vendor due diligence capabilities under new fraud laws;
- The growing use of subject access requests as litigation tools post breach.

WATCH ONLINE

> "Boards have vacuums, and regulators, prosecutors, litigants concentrate on the CISO because the board's asleep at the wheel in some cases."
>
> - ***Jonathan Armstrong***

AI's Black Box Problem: When Security Fixes Fall Short

Cobalt CTO **Gunter Ollmann** on Why Organizations Struggle With AI Vulnerabilities

Organizations can fix only 21% of generative AI vulnerabilities, according to Cobalt's State of Pentesting Report 2025, creating a dangerous security gap as AI adoption accelerates. Gunter Ollmann, CTO at Cobalt, discusses why traditional defenses lag behind in AI technology.

WATCH ONLINE

Inclusive Security Demands Strategic, Human-Centric Design

Resilionix's **Heather Lowrie** on Embedding Civic Values Into Cybersecurity

Cybersecurity must be treated as a public good that protects more than systems and data. Heather Lowrie, founder of Resilionix, says security should defend civic integrity and democratic resilience. Systems should be built with inclusion, accessibility and privacy in mind, she says.

WATCH ONLINE

Why Cybersecurity Must Be Part of What You Live and Breathe

4FOX Security CEO **McPherson** on Why Trust Is Essential for Vendor Risk Resilience

Hazel McPherson, founder and CEO of 4FOX Security, outlines a pragmatic approach to third-party resilience, emphasizing risk prioritization, cultural alignment and trust-driven relationships across supply chains.

WATCH ONLINE

Quantum-Resilient Cryptography: Why Migration Matters

Lastwall CEO **Karl Holmqvist** Says Q-Day May Arrive Without Warning

Quantum computing poses a serious risk to current encryption systems. Karl Holmqvist, founder and CEO of Lastwall, said Q-Day may arrive without warning, which means firms need to start migrating to post-quantum cryptography.

WATCH ONLINE

UK Cyber Sector Grows Amid Fragmentation Challenges

Plexal's **Saj Huq** on Regulation, AI Resilience and Scaling Innovation

The U.K. cyber sector continues to grow in double digits and is one of the world's top cyber economies, valued at £13.2 billion - $17.9 billion. Yet, venture capital investment has declined over the past year, and extreme market fragmentation persists, said Saj Huq, chief commercial officer at Plexal.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, Huq also discussed:

- Why AI adoption is being constrained by cybersecurity, privacy and regulatory compliance concerns;
- Why U.K. cyber startups must scale beyond the "long tail";
- How cross-functional board conversations are evolving to integrate cyber risk with business strategy.

WATCH ONLINE

> "About 20% of the U.K. cyber sector is comprised of large and mid-sized firms, but they earn over 90% of all revenue effectively. Seventy-five percent of all companies are small and medium size, and they share less than 10% of revenue."
>
> – ***Saj Huq***

CyberEdBoard Insights: Don Gibson

Kinly CISO on Culture, Communication and Real Cyber Risk

Ransomware attacks targeting high-profile retailers are forcing organizations to reassess their cyber readiness. Despite having mature defenses, companies continue to fall victim to attacks rooted in social engineering, said Don Gibson, CISO at Kinly.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, Gibson also discussed:

- Social engineering attacks underscore the importance of workforce training;
- Mature cyber defenses mean little without cultural alignment;
- Board trust grows when CISOs show how risk connects with business goals.

> "You need to make sure that either they're [boards] making the correct decisions, or if they're not, you are doing absolutely everything possible to close the doors behind you."
>
> – ***Don Gibson***

WATCH ONLINE CyberEdBoard

Governments Embrace Secure by Design to Curb Cyberthreats

NextJenSecurity Founder Calls for Global Policy Shifts to Reduce Vulnerabilities

Governments worldwide are shifting from reactive responses to preventive strategies to tackle ransomware attacks. Jen Ellis, founder of NextJenSecurity, stresses the need for vulnerability accountability and secure-by-design policies to tackle systemic cybersecurity flaws.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, Ellis also discussed:

- The Pall Mall Process and global controls on commercial cyber intrusion tools;
- Challenges of securing small and medium businesses in ransomware resilience efforts;
- The Ransomware Task Force's evolving focus toward critical infrastructure security.

WATCH ONLINE

> "We have the 'Known Exploited Vulnerabilities Catalog' from CISA, which helps prioritize patching. But for organizations, it is difficult to keep up with it, which is part of the reason that secure by design has become such a critical movement."
>
> – ***Jen Ellis***

Offline Backup and Encryption Are Crucial to Data Resilience

Apricorn's **Jon Fielding** on Recovery Testing, USB Encryption, Automated Backups

While more than 90% of organizations have a backup strategy, nearly one-third fail to recover all data during a breach. To combat ransomware, defenders need encrypted offline backups, automated backup strategies and consistent recovery testing, said Apricorn's Jon Fielding.

WATCH ONLINE

AI Gives Predictable Answers, But With Unpredictable Results

Associate Professor **Michael Pound**: LLMs Are Probabilistic - and That Poses Risks

Generative AI predicts words, not truth. Michael Pound, associate professor at the University of Nottingham, warns that when large language models generate malicious content, it's not due to confusion or logic flaws - it's simply probability at work.

WATCH ONLINE

Why a Business-First Incident Response Approach Works Best

Semperis' **Hodgkinson** and **Rachman** on Tabletop Exercises and Continuity Plans

Cyber incidents aren't just technical problems, they're business crises that require comprehensive preparation, said Semperis' Strategic Advisor Simon Hodgkinson and Director of Security Research Yossi Rachman. Cyber incident simulations must focus on business impact, not just tech.

WATCH ONLINE

Stop Anthropomorphizing AI and Secure It Like Software

Mindgard CEO **Peter Garraghan** on AI Security Gaps and Safer Adoption

AI may talk like humans, but it's still software that is vulnerable to cyberattacks. Peter Garraghan, professor at Lancaster University and CEO of Mindgard, discusses why security is always a cat-and-mouse game and why treating AI as "just software" is crucial to securing it.

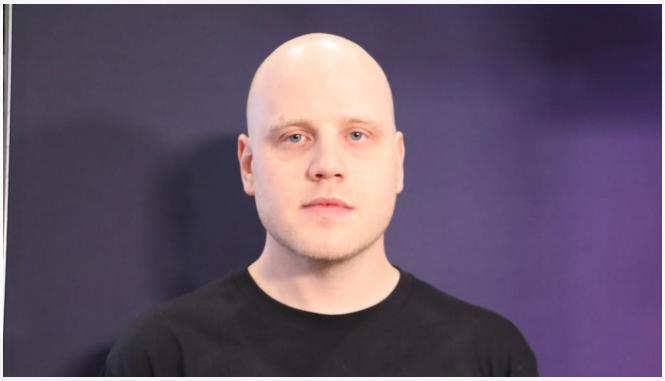
WATCH ONLINE

“If I said, I download a piece of software with no testing, no controls, no compliance … why is AI any different?”

Peter Garraghan
Professor, Lancaster University, and CEO, Mindgard

Proactive Security Crucial Amid Faster Exploits

watchTowr's **Benjamin Harris** on Visibility and Speed to Counter Threats in Hours



The gap between disclosure and exploitation is shrinking. Benjamin Harris, founder and CEO of watchTowr, said companies need visibility, validation and fast triage to act before threat actors exploit common vulnerabilities and exposures - often within four hours.

WATCH ONLINE

IoT Security Failures: Same Mistakes, Different Devices

Ken Munro of Pen Test Partners on Why IoT Security Still Lags and What Must Change

IoT manufacturers continue making the same security mistakes due to rushed development and poor disclosure practices, said Ken Munro, CEO of Pen Test Partners. "You need to think about cybersecurity from day one," he said, because retrofitting security is both difficult and expensive.

WATCH ONLINE

Security Basics Are Still Being Missed Amid Market Hype

Information Security Forum's **Paul Watts** on Prioritizing IAM Over Flashy Tech

Despite rising cybersecurity investments, organizations are neglecting core security functions. Paul Watts, distinguished analyst at Information Security Forum, warns that skipping basic security functions such as IAM creates critical vulnerabilities that advanced technologies can't fix.

WATCH ONLINE

Cybersecurity Strategy Shifts Amid Global Political Tensions

NCC Group's **Katharina Sommer** on Why Nations Are Turning Inward on Cyber Defense

Geopolitical shifts are reshaping how countries approach cyber resilience. Katharina Sommer, group head of government affairs and analyst relations at NCC Group, explains why governments are turning inward and focusing on sovereign cybersecurity strategies.

WATCH ONLINE

“There is a real focus on sovereign solutions, what countries can do for themselves, how they can big up their own cybersecurity industry.”

Katharina Sommer
Group Head, Government Affairs and Analyst Relations, NCC Group

CyberEdBoard Insights: Ian Thornton-Trump and Martyn Booth

Inversion6 CISO Thornton-Trump and dunnhumby CISO Booth on Strategic AI Deployment

With every vendor claiming AI superiority, how do security leaders cut through the noise? Ian Thornton-Trump, CISO at Inversion6, and Martyn Booth, CISO at dunnhumby, discuss how to identify where AI delivers genuine value versus marketing hype in cybersecurity operations.

In this video interview with Information Security Media Group at Infosecurity Europe 2025, Thornton-Trump and Booth also discussed:

- How AI use in pen testing is reforming execution and reporting processes;
- The hidden benefits of AI-powered MSSPs in improving team retention;
- The need for governance frameworks to address transparency and bias issues in AI decision-making.

WATCH ONLINE CyberEdBoard

> "It's probably been a facet of shoehorning AI to everything, as opposed to working out what works and then buying it where it makes sense."
>
> - ***Martyn Booth***

ISMG Studio

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
info@ismg.io

Sales & Marketing

North America: +1-609-356-1499
APAC: +91-22-7101 1500
EMEA: + 44 (0) 203 769 5562 x 216

BANK INFO SECURITY · CAREERS INFO SECURITY · HEALTHCARE INFO SECURITY · GOV INFO SECURITY · infoRisk TODAY
CU Just for Credit Unions INFO SECURITY · Data Breach TODAY · AIToday.io · OT.today · PaymentSecurity.io · FraudToday.io · DeviceSecurity.io
CIO.inc · CyberEd.io · CyberEdBoard · CXO ADVISOR · CYBER THEORY · Xtra mile LIFECYCLE MARKETING · ATHENA
QC MEDIA · SUMMIT · custom events · roundtables · NULLCON · hardwear.io Hardware Security Conference and Training · ISMG Studio

iSMG

902 Carnegie Center · Princeton, NJ · 08540 · ismg.studio