ISMG Studio

Infosecurity® Europe

Highlights & Insights

Video Interviews, News, Photos and More From the ISMG Team

Infosecurity Europe 2026: Security in the Age of AI

Mathew Schwartz
Executive Editor, DataBreachToday and Europe,
ISMG

Once again, Infosecurity Europe brought together cybersecurity, technology, legal and business leaders from across the United Kingdom, Europe and beyond. This year's conversations were largely shaped by this rapidly evolving reality: Artificial intelligence has become both one of the most powerful tools for cyber defenders as well as one of the most potent weapons in the hands of adversaries.

As a media partner of this year's event, ISMG staffed a video studio on the Infosecurity Europe 2026 expo hall floor, gathering insights from CEOs, CISOs, government officials, researchers and innovators. Experts explored advances in AI-driven threat detection, autonomous security operations and emerging technologies, including the use of Anthropic's Mythos large language model to find vulnerabilities. They also warned of the growing sophistication of AI-powered and AI-assisted attacks, the continuing threat posed by ransomware groups and the challenge of attempting to secure today's increasingly complex IT ecosystems. One message resonated throughout the event: The human element remains at the heart of effective cybersecurity. The demand for skilled practitioners, critical thinking and fostering a strong security culture has never been greater.

The interviews in this Infosecurity Europe Compendium, created by ISMG.Studio, our unparalleled platform for cybersecurity and technology leaders hosted at major events worldwide, feature across our news sites. In these pages, enjoy the in-depth discussions conducted by our editorial team as they explore how organizations are navigating a future in which human expertise and AI must combine forces to confront an increasingly complex cybersecurity landscape filled with threats, challenges, as well as opportunities.

TABLE OF CONTENTS

Video Interviews

Why UK Cyber Law Struggles to Keep Pace With AI

James Morris of CSBR on Balancing AI Opportunity With Cyber Resilience

The U.K.'s Cyber Security and Resilience Bill is midway through Parliament, but a fast-moving AI landscape is testing its limits. James Morris of CSBR explains why sovereignty concerns and AI governance gaps must be addressed before the bill becomes law.

In this video interview with ISMG at Infosecurity Europe 2026, Morris also discussed:

- How the U.K.'s pro-growth AI policy differs from the European Union's risk mitigation approach;
- Why the National Health Service represents the clearest near-term opportunity for AI adoption in public services;
- The role of political instability in undermining long-term cybersecurity and resilience planning.

Watch Now

> **"One of the issues around that bill is that if you think about what's happened in the landscape for security and resilience over the last 15 months, there's been a huge amount of change."**
>
> - James Morris

Why PKI Visibility Gaps Put Business Resilience at Risk

Paul Holt of DigiCert on Closing Certificate Visibility Gap Before It's Too Late

Most organizations lack visibility into their own certificates, yet certificate failures now threaten business continuity and regulatory compliance. DigiCert's Paul Holt lays out why discovery is the critical first step toward crypto agility.

Watch Now

Faster Patching Is the Wrong Answer to AI Threats

watchTowr's **Benjamin Harris** on Why Edge Mitigation Beats the Patch Race

AI-assisted vulnerability discovery has compressed exploitation timelines from hours to minutes, leaving security teams unable to patch fast enough. Mitigation at the edge is the practical answer, said Benjamin Harris, founder and CEO at watchTowr.

Watch Now

Why Security Teams Need Non-Security Thinkers

CIISec's **Amanda Finch** on Building a Workforce Beyond Technical Talent

The cybersecurity talent shortage isn't just a numbers problem. It's a sourcing problem, says Amanda Finch, CEO at CIISec. She discusses why organizations need to recruit from varied backgrounds and build teams with communication, analytical and problem-solving skills alongside technical expertise.

Watch Now

Why Vulnerability Patch Windows Are Now Zero or Negative

Dataminr's **Joseph Slowik** on Using Agentic Workflows to Outpace AI-Enabled Threats

Attackers are moving from initial access to impact in hours, and vulnerability exploitation is outpacing disclosure. AI agents and large language model-assisted workflows are the practical answer for cyber defenders, says Joseph Slowik of Dataminr.

Watch Now

“You’ve got to have people that are very good at technical stuff. You’ve got to have people that are very good at problem solving when things go wrong. You also need people that are good at communicating, so they can talk to people about how to stop things from happening.”

Amanda Finch
CEO, Chartered Institute of Information Security

Agentic AI's Blind Spot Is Control, Not Trust

Cloudflare's **Christian Reilly** on Securing AI Agents Before They Scale

Many organizations don't know how many AI agents are running on their networks or what those agents are doing. Christian Reilly, field CTO at Cloudflare, says visibility, identity and control must come before trust.

In this video interview with ISMG at Infosecurity Europe 2026, Reilly also discussed:

- The risks of shadow agents and unmanaged Model Context Protocol deployments;
- Why prompt and response controls are critical for customer-facing AI applications;
- How regulated industries can apply human-in-the-loop accountability to agent workflows.

Watch Now

> **"My biggest fear is that there's lots of agents running around that the security parts of organizations have absolutely zero visibility into, and therefore not really sure about the risk of those agents in operation."**
>
> - Christian Reilly

Why Identity Security Needs a Rethink

Patricia Titus of Abnormal AI on Identity Risks and Keeping Humans in the Loop

AI-powered attacks have transformed phishing and identity security, making threats harder to detect and easier to scale. Patricia Titus, field CISO at Abnormal AI, argues that the answer isn't fully automated defense - it's a companionship model where AI handles scale and humans handle judgment.

In this video interview with ISMG at Infosecurity Europe 2026, Titus also discussed:

- The importance of maintaining human oversight as AI becomes embedded in security operations;
- How telemetry surfaces threat actors living off the land;
- Why third- and fourth-party relationships expand the infiltration risk.

Watch Now

> **"What we don't want to do is fully rely on AI without some sort of a checkpoint or a checking in, because then we run the risk of catastrophic failure of our systems."**
>
> - Patricia Titus

When the Threat Wears a Human Face

Eset's **Jake Moore** on Deepfakes, Quantum Risk and AI-Enabled Crime

Criminals are using artificial intelligence where it helps most, said Jake Moore, global cybersecurity advisor at Eset. Phishing, social engineering and as-a-service criminal ecosystems are getting better thanks to AI, but he warns that quantum computing is the bigger sleeper threat.

Watch Now

Why AI Defenses Fail Without Data and Identity Fundamentals

RPC's **Spencer Scott** on Why Security Basics Must Come Before Agentic AI Adoption

Organizations are racing toward agentic artificial intelligence defenses, but without clean data, identity and asset management in place, those defenses will fall short. Security fundamentals must come first, said Spencer Scott, head of information security at RPC.

Watch Now

AI Agents Need Governance Before Scale

1Password's **Dave Lewis** on Unchecked Privilege and Security Debt

Organizations are rushing to deploy artificial intelligence agents without understanding their access, identities or risks. Dave Lewis, global advisory CISO at 1Password, says the security debt that's accumulating now will only grow harder to address over time.

Watch Now

Boards, Security Teams and the Cyber Fluency Gap

Cybersecurity Leader **Purvi Kay** on Leadership, Trust, Closing Cyber Strategic Gaps

Cybersecurity's biggest gaps aren't technical - they're strategic. Purvi Kay, cybersecurity leader, TEDx speaker and diversity advocate, discusses why closing them demands stronger leadership, smarter boardrooms and a workforce built on cognitive diversity.

Watch Now

“Businesses will knowingly release vulnerable code. This is nothing new because there’s always going to be a bit of business and the risk associated with that.”

Richard Meeus
Senior Director, Security Technology and Strategy - EMEA, Akamai

Ransomware Thrives by Adapting Faster Than Defenders

Rapid7's **Thom Langford** on Vulnerability Exploitation and Cybercrime

Ransomware groups are simplifying operations, embracing service-based business models and increasingly exploiting vulnerabilities instead of relying on phishing. Thom Langford of Rapid7 explains why organizations must improve vulnerability prioritization before AI-driven flood of new flaws arrives.

Watch Now

Cyber Resilience Starts With People, Not Technology

PPRO's **Bronwyn Boyle** on Burnout, AI and Building High-Performing Teams

Cybersecurity teams face growing pressure as AI accelerates the pace of technological change, threat activity and business expectations. Bronwyn Boyle, CISO at PPRO, argues that investing in psychological resilience is essential to building high-performing security teams.

Watch Now

Human Cyber Risk Demands a Psychology Makeover

CybSafe Science and Research Director **Jason Nurse** on Cyber Fear in AI Era

People feel intimidated by cybersecurity - a reaction that breeds learned helplessness and erodes the very behaviors organizations depend on for their defense, said Jason Nurse, director, science and research, CybSafe, and associate professor for cybersecurity at the University of Kent.

Watch Now

Geopolitics Is Now a Cybersecurity Problem

UCL's **Melanie Garson** on Anti-Fragility, Supply Chain Risk and AI Adoption

Geopolitical exposure has quietly moved to the front of the security agenda, and most organizations are only now realizing how little they understand about where their risks originate, says Melanie Garson, associate professor of international security at UCL.

Watch Now

Why Tool Count Is the Wrong Security Metric

CybaVerse's **Oliver Spence** on Matching Tools to Business Outcomes

Mid-market organizations manage 30 to 40 security tools on average, yet many still struggle to define the outcomes these tools should deliver. Oliver Spence, CEO of CybaVerse, says the fix should start well before any procurement decision.

Watch Now

How to Keep Cyber Crisis Communications From Going Wrong

Brunswick's **Nicola Hudson** on Building a Response Plan Before Attack Hits

When a cyberattack strikes, poor communications can cause as much damage as the breach itself. Nicola Hudson, partner at Brunswick, outlines why organizations must plan their crisis response well before an incident occurs, and what gets it wrong when they don't.

Watch Now

Resilience Must Be Built Before Crisis Strikes

Security Expert **Ragna Sveinsdottir** on AI, Collaboration and Security by Design

Security leaders can't afford to treat resilience as a response to crisis. Security expert Ragna Sveinsdottir stresses that organizations must build resilience into services from the outset, while balancing AI adoption, supply chain risk and the growing need for collaboration across teams and industries.

Watch Now

The CISO Inbox Is Not a Sales Funnel

Inversion6 CISO **Ian Thornton-Trump** on What Cybersecurity Startups Get Wrong

CISOs are bombarded with more than 400 cold outreach attempts a month - ignoring nearly all of them. If vendors want to break through, they need to stop selling and start solving, said Ian Thornton-Trump, CISO at Inversion6.

Watch Now

"We keep telling the CISOs and the cyber leaders that you need to be able to translate cybersecurity into business language for the boardroom to make informed decisions. I say, and this is a challenge, board members, how about you meet us in between? How about you get cyber savvy as well."

Purvi Kay
Cybersecurity Leader, TEDx Speaker and Diversity Advocate

“Cybercriminals are mastering psychology. They know how we think. I’m championing that everyone within an organization, especially within a security role, needs to be thinking about how does psychology play a part in what we’re asking people to do.”

Jason Nurse
Director, Science and Research, CybSafe, and Associate Professor, Cybersecurity, University of Kent

Cyber Risk Contracts Have Become the Weakest Link

Attorney **Jonathan Armstrong** on AI, Vendor Consolidation and Personal Liability

As organizations outsource more crown jewels to third-party vendors and silently roll out AI, the old playbook of contracts and one-time due diligence is dangerously out of date, says Jonathan Armstrong, partner at Punter Southall Law.

Watch Now

Board Attention Doesn't Always Mean Understanding

Security Advisor **Barry Coatesworth** on Cyber Risk, Resilience and Accountability

Cybersecurity has earned a place on board agendas, but many organizations still struggle to translate technical risks into business decisions. Security advisor Barry Coatesworth explains why resilience depends on clear communication, accountability and continuous testing, not compliance alone.

Watch Now

Why Banks Must Align Stakeholders Before Scaling AI

Sandip Wadje of BNP Paribas on Consensus, Data Quality and Multi-Model Strategy

Scaling artificial intelligence in a large, regulated bank is less a technology challenge than a stakeholder alignment problem - one that demands shared definitions, clean data and process rigor, says Sandip Wadje of BNP Paribas.

Watch Now

When Burnout Becomes a Cybersecurity Control Failure

Peter Coroneos of Cybermindz on Stress, the Brain and Human Capability Risk

Cybersecurity burnout is no longer just a wellness concern. It's an operational risk that quietly degrades the capability of cyber defenders, says Peter Coroneos, founder and chairman of Cybermindz. Cyber burnout levels now exceed those of frontline healthcare workers.

Watch Now

SMEs Need Cyber Help That Speaks Their Language

Helen Barge of Howden on Scaling Practical Cyber Support for Small Businesses

Small and mid-sized businesses face unique cybersecurity barriers - from budget constraints to IT providers who fall short on basics - and need accessible, jargon-free guidance, said Helen Barge, principal and head of digital resilience services at global insurance group Howden.

Watch Now

Security Leaders Must Stop Living by the Framework

Paul Watts of Keywords Studios on Business Alignment, AI Hype and Workforce Risk

Cybersecurity leaders who still operate through the lens of frameworks and risk registers could be irrelevant in a world where business moves without them, said Paul Watts, CISO at Keywords Studios. He recommends investing in both AI and people to sustain operations over the long haul, he said.

Watch Now

Fighting AI Threats Requires AI and Human Judgment

Adecco's **Alex Gomez** on Trust, Deepfakes and Email Fraud Defense

As AI-powered scams become more convincing, organizations must balance advanced detection technologies with human oversight. Alex Gomez of The Adecco Group explains why behavioral AI, security awareness and user trust are all essential to defending against evolving threats.

Watch Now

Why Cyber Recovery Is Not Disaster Recovery

Cohesity's **James Blake** on Restoring Trust, Not Just Data, After Cyberattacks

Backing up data is the easy part. But cyber recovery demands something far harder, says James Blake, vice president of global cyber resiliency strategy, response and consulting at Cohesity. It demands restoring trust in every layer of the environment before a single system goes back into production.

Watch Now

“It’s not like a fire that is put out and contained, and then you’re dealing with the impact. You have a threat actor in your system looking to do you harm minute after minute after minute.”

Nicola Hudson
Partner, Global Cyber Practice Co-Lead, Brunswick

Femtech Can't Afford to Get AI Trust Wrong

Laure Lydon of Flo Health on Securing AI Without Compromising Trust

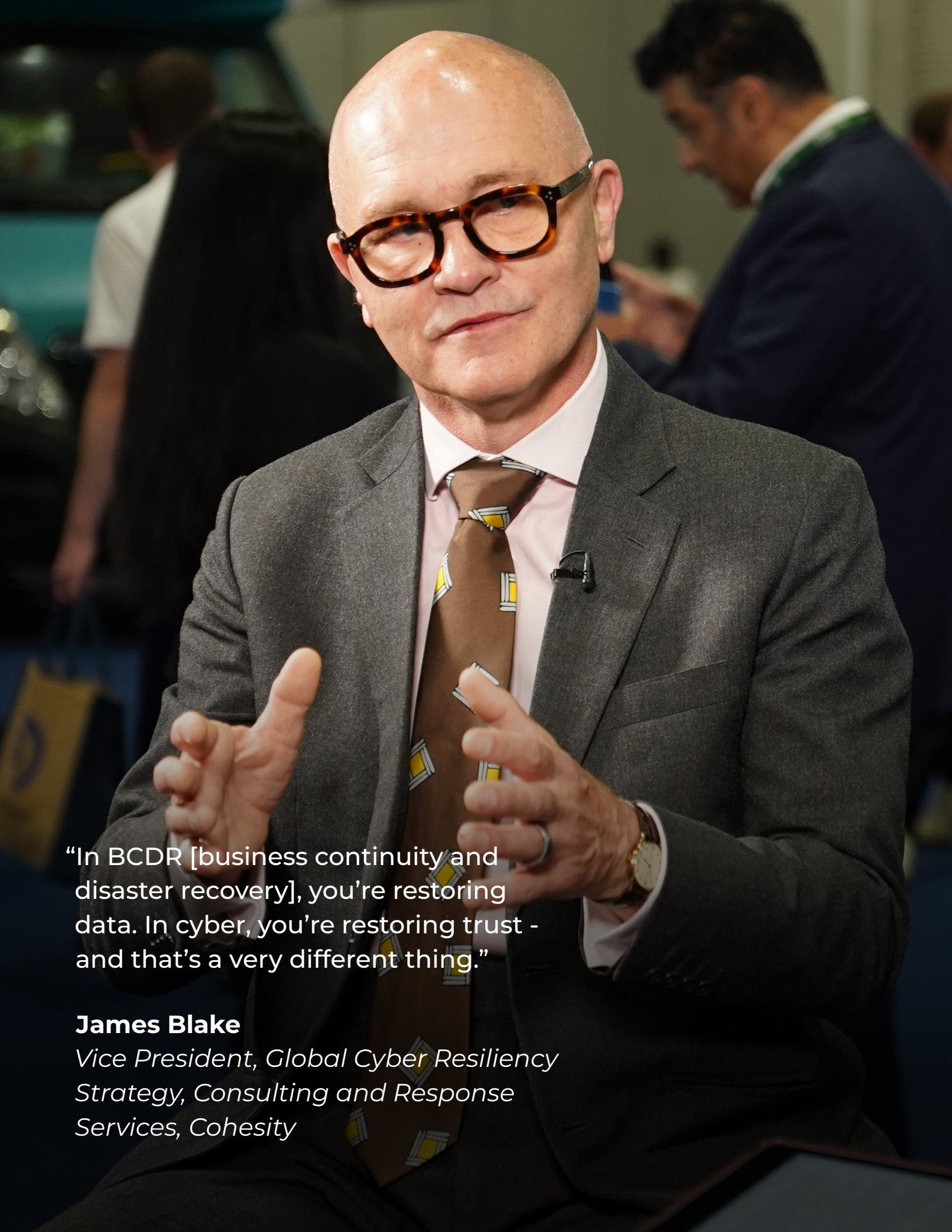
Trust in femtech isn't a feature. It's the foundation. Laure Lydon, vice president of security at Flo Health, makes the case for embedding privacy and security into AI development from day one, not as an afterthought. Firms must evaluate potential risks before systems are built, she said.

In this video interview with ISMG at Infosecurity Europe 2026, Lydon also discussed:

- Why user choice and data control are critical to building trust in digital health;
- How anonymous mode gives users control without personal or technical identifiers;
- How agent-human hybrid ecosystems can operate at machine speed.

Watch Now

> **"The question never was, can we [innovate with AI]? It was, how can we? How can we do this in a safe and secure way? How can we do this in a way that our users will continue to trust our app?"**
>
> - Laure Lydon



“In BCDR [business continuity and disaster recovery], you’re restoring data. In cyber, you’re restoring trust - and that’s a very different thing.”

James Blake
Vice President, Global Cyber Resiliency Strategy, Consulting and Response Services, Cohesity

How Virtual Patching Buys Time Against Rising Threats

Akamai's **Richard Meeus** on Using Virtual Patching and AI to Close Security Gaps

Vulnerability volumes are rising faster than teams can patch, and AI is accelerating discovery. Richard Meeus of Akamai says virtual patching and microsegmentation give organizations a practical path to managing exposure before patches can be deployed.

Watch Now

Data Extortion Remains Retail's Biggest Cyberthreat

RH-ISAC's **Lee Clark** on Why Low-Tech Attacks Still Outperform AI-Powered Threats

While organizations and bad actors experiment with AI, the most damaging incidents continue to stem from social engineering schemes. Lee Clark of Retail and Hospitality ISAC said data extortion campaigns, often launched through help desk impersonation and MFA reset scams, remain the dominant threat.

Watch Now

Why Cyber Resilience Must Start With People

Milos Pesic of Accelleron on Building Security Around Empowerment, Not Just Tools

Cyber resilience fails when it's built on tools alone. Accelleron CISO Milos Pesic argues that empowering people, aligning with regulations and treating cybersecurity as a business enabler are what make resilience programs adapt to new cyberthreats.

Watch Now

“We’re having all sorts of silent rollouts - AI being one - and that whole landscape has changed, but the legal answers haven’t changed that much.”

Jonathan Armstrong
Partner, Punter Southall Law

"You need to account for something going wrong, and then having tested and knowing what it looks like to recover."

Ragna Sveinsdottir
Senior Vice President and Advisory Council Member, Infosecurity Europe

Why AI Is Making Malware Harder to Detect

Ray Canzanese of Netskope Threat Labs on AI-Generated Threats and Supply Chain Risk

Attackers are using multi-model artificial intelligence harnesses to generate malware on the fly, with no malicious code ever shipped to a victim's machine. Ray Canzanese of Netskope Threat Labs breaks down why defenders must now inspect AI traffic, not just block it.

In this video interview with ISMG at Infosecurity Europe 2026, Canzanese also discussed:

- The surge in malicious PyPI and npm packages and why AI-generated code raises supply chain risk;
- The return of fake installers and the growing threat of ClickFix attacks;
- Why staying vendor-agnostic and version-pinning dependencies are essential defenses today.

Watch Now

> **"The advice I give everybody right now is do not get too deep with any one vendor or model. We're going to be hot swapping for a long time."**
>
> - Ray Canzanese

Why the 30-Day Patch Cycle Is Dead

Cloud Security Alliance's **Troy Leach** on Mythos, Zero-Day Exploits and AI Governance

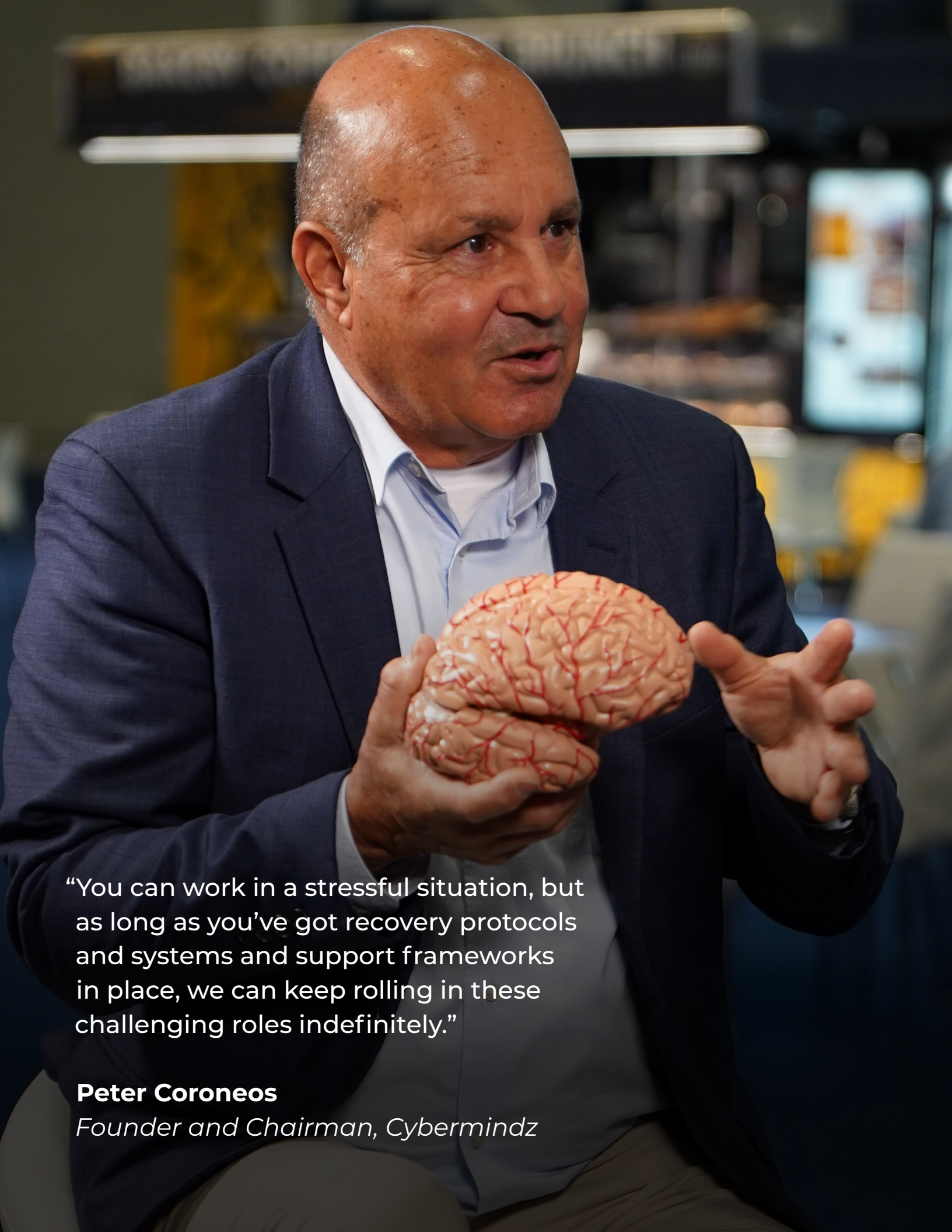
The window between vulnerability discovery and weaponized exploit has collapsed from roughly 70-plus days to under one. Troy Leach, chief strategy officer at the Cloud Security Alliance, says the 30-day patch cycle is already obsolete, and most boards don't know it yet.

In this video interview with ISMG at Infosecurity Europe 2026, Leach also discussed:

- How Anthropic's Mythos has accelerated the weaponization of zero-day vulnerabilities;
- Security risks emerging from AI agents, Model Context Protocol and toolchain attacks;
- Why best practices may advance faster than AI regulation in the coming years.

Watch Now

> **"We're at a point where security leaders are going to have to think about how do I respond and react to all these zero-day vulnerabilities, no longer relying on just security metrics that every 30 days we have a critical patch program."**
>
> - Troy Leach



“You can work in a stressful situation, but as long as you’ve got recovery protocols and systems and support frameworks in place, we can keep rolling in these challenging roles indefinitely.”

Peter Coroneos
Founder and Chairman, Cybermindz

ISMG Studio

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 ISMG Studio

ISMG

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