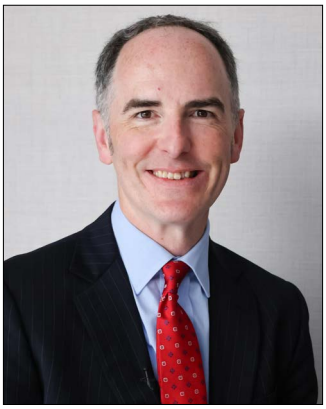
iSMG Studio

at Infosecurity Europe 2024

Infosecurity Europe 2024: Cybersecurity



This year's vibrant Infosecurity Europe 2024 at the London ExCeL convention centre featured a who's who of cybersecurity, technology, legal and other leaders from the U.K., Europe and beyond.

As a media sponsor of this year's event, Information Security Media Group staffed a video studio on the bustling expo hall floor, gathering insights from CEOs, CISOs, government leaders, researchers and more. Top themes at Infosecurity Europe 2024 included:

- **Generative AI:** Attendees discussed the targeting as well as business and defensive uses of AI – including how to secure the enterprise with AI and how to secure AI systems and data. Chatbots loomed large at the conference, and one expert urged CISOs to get to on board with their organisations' use of AI immediately.
- **Cybercrime:** Trends include rapid ransomware ecosystem innovation, ongoing use of social engineering and phishing, criminal interest in AI and the burgeoning use of zero-day exploits.
- **Supply chain attacks:** Multiple interviews referenced the devastating ransomware attack that hit a critical NHS pathology lab just days before the conference began, disrupting patient care across southeast London and highlighting the need for robust supply chain security practices.
- **Incident response and crisis management:** Incident responders and CISOs shared their hard-won advice for preparing, handling and surviving attacks.

The more than 30 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 captured many insightful discussions and Profiles in Leadership interviews featuring members of ISMG's lively CyberEdBoard community.

In these pages, enjoy the in-depth interviews conducted by our seasoned editorial team, which highlight the wisdom of front-line practitioners about all things cybersecurity, and please don't hesitate to share your advice and feedback with us.

Mathew Schwartz

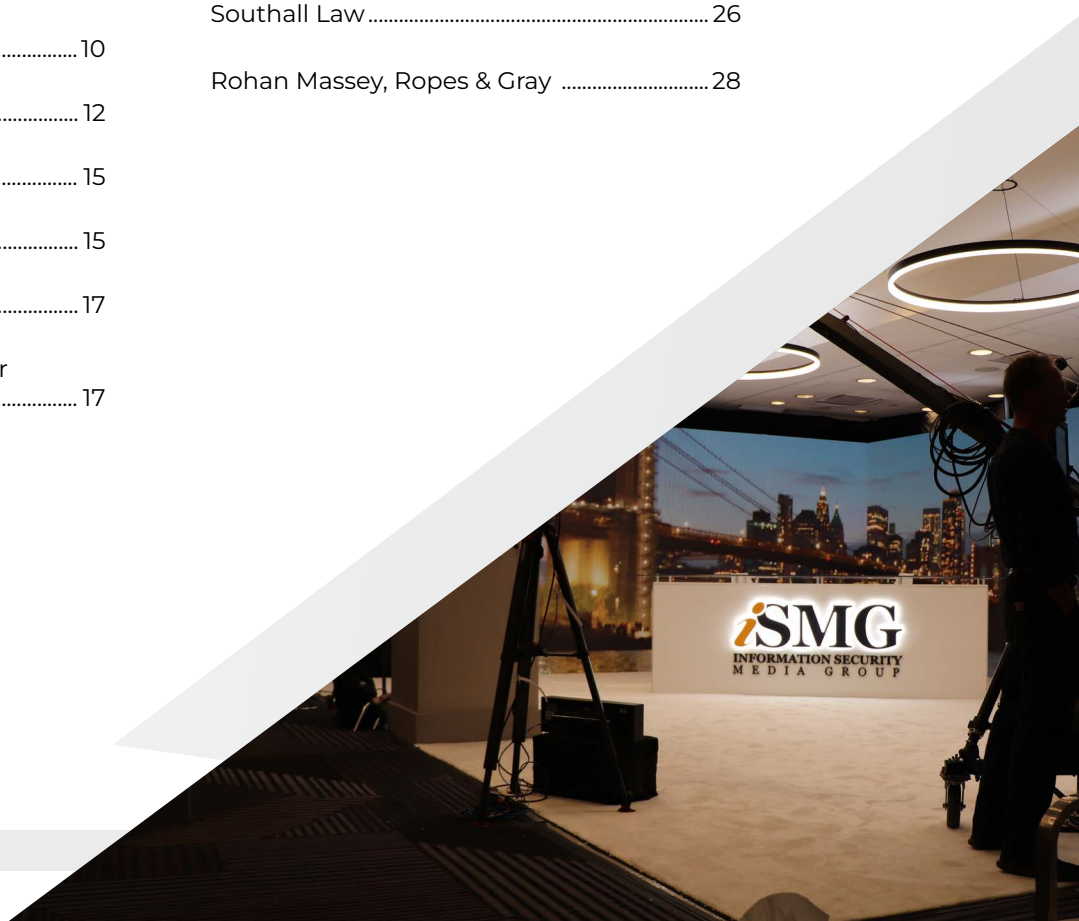
Executive Editor, DataBreachToday and Europe

Information Security Media Group

Visit us online for more ISMG at Infosecurity Europe coverage:

ismg.studio

Video Interviews



Rethinking Cybersecurity: The Role of MSSPs

Kevin Robertson of Acumen on Effective Cybersecurity Solutions Beyond Microsoft

Organisations often grapple with the question of whether relying solely on Microsoft for cybersecurity is enough. Kevin Robertson, chief operating officer and co-founder of Acumen, made the case for including best in breed security technology and services from specialised vendors.

In this video interview with Information Security Media Group at Infosecurity Europe 2024, Robertson also discussed:

- The importance of heterogeneity in security products;
- Tailoring security solutions to meet the unique needs of organisations, particularly in critical national infrastructure sectors;
- Fostering competition for innovation in cybersecurity.

WATCH ONLINE

> "The advice we give is: Use best in breed security technologies from security partners that specialise in it."
>
> ***- Kevin Robertson***

How Enterprise Browsers Enhance Security and Efficiency

Island President **Steve Tchejeyan** Says Enterprise Browsers Offer Significant ROI

Enterprise browsers offer corporations many advantages over traditional web browsers, from simplifying application delivery to protecting intellectual property.

WATCH ONLINE

CyberEdBoard Profiles in Leadership: Ian Thornton-Trump

The Cyjax CISO Discusses the Shift From Cyber Defence to Cyber Resilience

Ian Thornton-Trump, CISO of Cyjax, shared the importance of flexibility and continuous learning - key qualities that have shaped his career.

WATCH ONLINE CyberEdBoard | Member

Enhancing Security With a Fit-for-Purpose Enterprise Browser

Poornima DeBolle Discusses Menlo Security's Approach to Enterprise Browsers

Poornima DeBolle, co-founder and chief product officer, Menlo Security, discussed the features of a secure enterprise browser, highlighting its tailored functionality for enterprises and how it differs from consumer browsers. She explained why enterprises require a browser that prioritizes security.

WATCH ONLINE

CyberEdBoard Profiles in Leadership: Jez Reichmann

Channel 4's Deputy CISO on Balancing Technical and Managerial Skills

For Jez Reichmann, deputy CISO at Channel 4 Corp., leading cybersecurity and IT operations during the COVID-19 pandemic was challenging - and rewarding. He said focusing on the human element in keeping teams motivated, as well as securing the organisation, was key during that time of crisis.

WATCH ONLINE CyberEdBoard | Member

“We've got the ecosystem. We had businesses that were going commercial and bringing this technology to market.”

John Goodacre
Professor, The University of Manchester, and
Director, Digital Security by Design, UKRI

How CISSP Certification Helps CISOs Secure Digital Business

ISC2's **Jon France** on CISSP's 30-Year Mission to Build Skills, Competency and Ethics

Should CISOs have a seat at the executive table? Yes, if the world runs on data and digital technologies, said Jon France, CISO at ISC2. France highlighted the transition from a largely offline world to an interconnected digital environment and the growing need for CISOs to blend technical skills with business acumen.

In this video interview with Information Security Media Group at Infosecurity Europe 2024, France also discussed:

- The evolution of cybersecurity certifications;
- The shift in CISO responsibilities from technical to business risk management;
- The importance of integrating security into business processes and strategies.

> "CISSP is built on competency and ethics. If you have that certification, it's not only a piece of knowledge; it's also competency."
>
> ***- Jon France***

WATCH ONLINE

The Future of Digital Security by Design

Professor **John Goodacre** on Cybersecurity by Design vs. Cybersecurity by Default

Two key concepts are shaping how organisations protect their digital assets: cybersecurity by default and cybersecurity by design. Professor John Goodacre, director, Digital Security by Design, UKRI, discussed the need to design technology that inherently protects against vulnerabilities.

WATCH ONLINE

Safeguarding Election Integrity in the Digital Age

Javvad Malik of KnowBe4 Advises Vigilance, Critical Thinking During 2024 Elections

Javvad Malik, lead security awareness advocate at KnowBe4, emphasised the increasing risk posed by threat actors during election cycles - exploiting social media, posting deepfake content and disseminating misinformation.

WATCH ONLINE

What Makes Healthcare a Prime Target for Ransomware?

Rubrik's **Steve Stone** on Reducing Data-Related Vulnerabilities in Healthcare

Healthcare organisations are particularly vulnerable to ransomware, risking significant data loss. Steve Stone, head of Rubrik's Zero Labs, outlined why healthcare faces higher risks and how organisations can strengthen their defences against these disruptive threats.

WATCH ONLINE

Cybersecurity Lessons Learnt From Latest NHS Hospital Hits

Focus on Cyber Hygiene and Crisis Management, Says Acacium's **Andrew Cooke**

The latest ransomware attack that led to pathology service outages at multiple London hospitals underscores the need for more robust healthcare sector security and resilience measures, including threat hunting, said Andrew Cooke, director of information security services at Acacium Group.

WATCH ONLINE

Taking a Closer Look at AI Governance and Cybersecurity

Philip Morris International's **Ray Ellis** Shares Strategies for Secure AI Integration

Ray Ellis, head of AI security at Philip Morris International, emphasised the necessity of capturing requirements for securing AI capabilities, protecting privacy, understanding legal implications and ensuring enterprise architecture that prevents shadow AI.

In this video interview with Information Security Media Group at Infosecurity Europe 2024, Ellis also discussed:

- Essential elements of AI governance in cybersecurity;
- Challenges and solutions in integrating AI securely;
- Future cybersecurity trends and implications for defenders.

> "From a security point of view, we're looking at: Where is your data, and what is the classification of data?"
>
> ***- Ray Ellis***

WATCH ONLINE

Beyond the Cost Centre: Building Cyber Risk Management

Trend Micro's **Jon Clay** on Adversarial AI, Misinformation Campaigns, CISO Challenges

Cybercriminal campaigns aided by generative AI and political misinformation campaigns by nation-states are just two of the latest risks organisations are facing. That's why cyber risk management has become a focal point for CISOs, said Jon Clay, vice president of threat intelligence, Trend Micro.

WATCH ONLINE

Implementing GRC in a Complex Global Organisation

Purvi Kay of BAE Systems on Unifying GRC and Building Diverse Cyber Talent

Implementing governance, risk and compliance in a global organisation comes with challenges. The complexity increases with sophisticated cyberthreats and an evolving geopolitical landscape.

WATCH ONLINE

Zero-Day Exploits and Ransomware Trends for 2024

Rapid7's **Christiaan Beek** Addresses the Surge in Zero-Day Exploits

Christiaan Beek of Rapid7 revealed alarming trends in zero-day exploits, especially against network appliances. He said the financial rewards of ransomware are enabling threat actors to buy zero-days. He urged firms to enhance detection and patching strategies.

WATCH ONLINE

CyberEdBoard Profiles in Leadership: Aman Sood

Elsevier Cybersecurity VP Shares His Leadership Journey and Challenges

Aman Sood began his career in cybersecurity as a help desk analyst, handling tasks such as resetting user passwords and providing technical support. He shared his journey from analyst to cybersecurity vice president, discussed the challenges and offered advice to aspiring security professionals.

WATCH ONLINE CyberEdBoard | Member

“How do you prevent or limit ransomware in the cloud and SaaS? It has to start and end with identity.”

Steve Stone
Head of Zero Labs, Rubrik

Ransomware Actors Focusing on More Opportunistic Targeting

Martin Zugec of Bitdefender on the Shifting Tactics of Cybercriminals

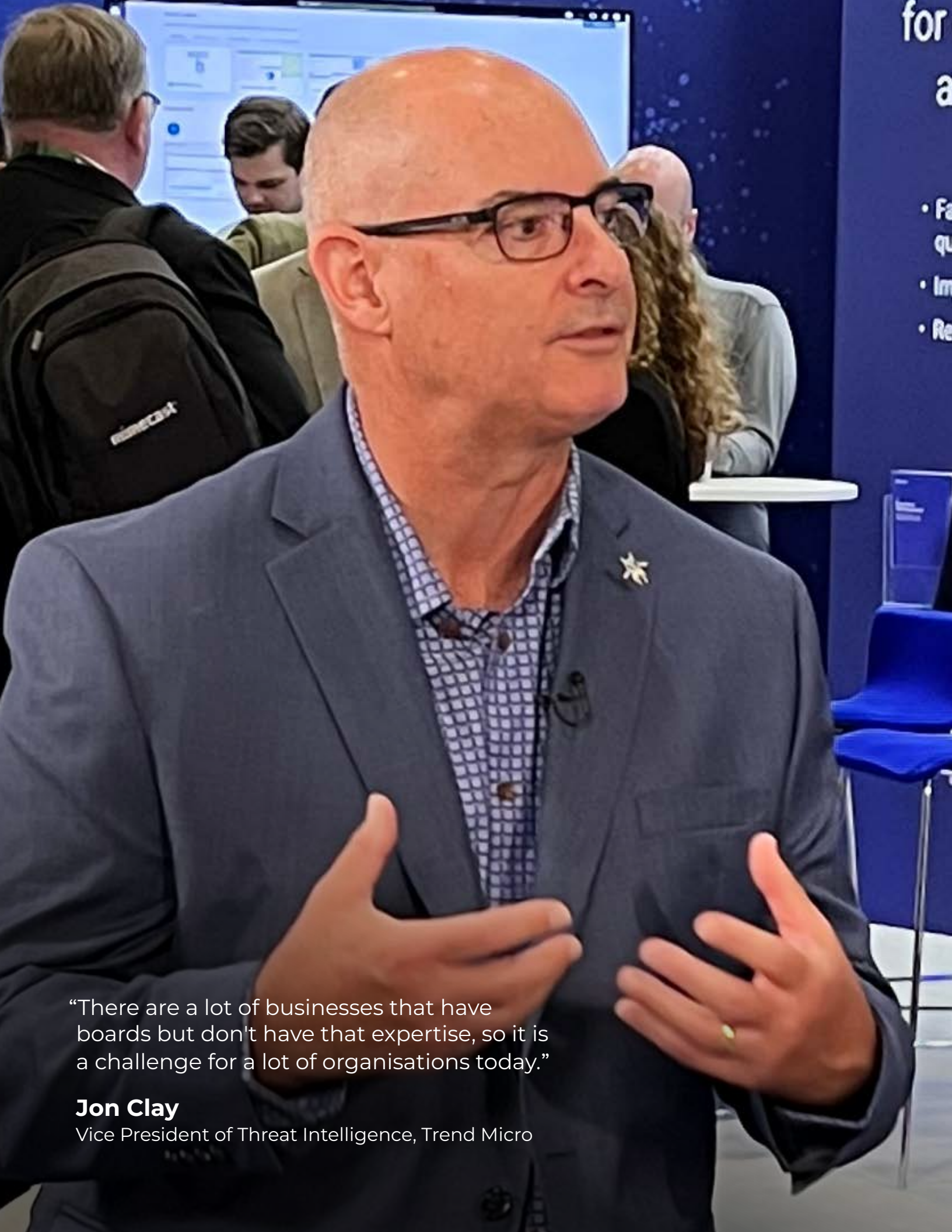
Ransomware tactics have shifted. Martin Zugec, technical solutions director at Bitdefender, discussed the evolution of ransomware threats. He pointed out that attackers have moved to opportunistic targeting and detailed the rise of automation in initial compromises.

In this video interview with Information Security Media Group at Infosecurity Europe 2024, Zugec also discussed:

- Why post-initial compromise activities rely on manual operations and custom tools;
- The importance of timely vulnerability patching to prevent compromises;
- Steps that organisations can take to defend against evolving threats.

WATCH ONLINE

> "There is more opportunistic targeting, and bad actors are not picking up the victims and going after them. They are preying on vulnerabilities."
>
> ***- Martin Zugec***

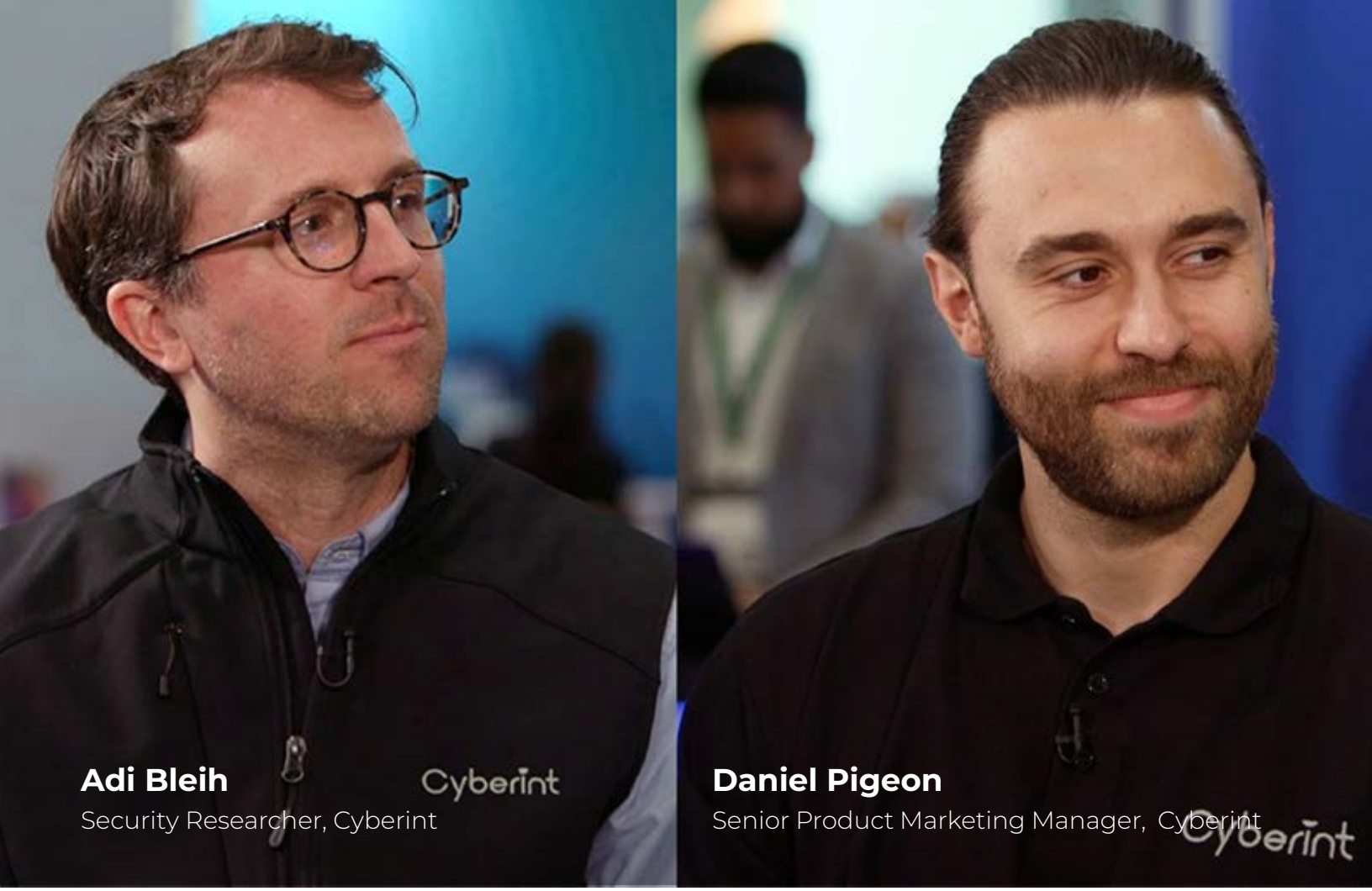


“There are a lot of businesses that have boards but don't have that expertise, so it is a challenge for a lot of organisations today.”

Jon Clay
Vice President of Threat Intelligence, Trend Micro

“We don't want our organisations doing two different things, so we're trying to bring it all together and have one consistent approach that provides for all our customers.”

Purvi Kay
Head of Cyber Security, Governance, Risk & Compliance, BAE Systems PLC



Is Cyber Becoming a Primary Domain of Warfare?

Adi Bleih and **Daniel Pigeon** on Evolving Cyberthreats in Modern Conflicts

Adi Bleih and Daniel Pigeon of Cyberint discused the evolution of cyber operations in recent conflicts, the rise of hacktivist groups, the targeting of critical infrastructure and supply chains and the need for new defence strategies.

In this video interview with Information Security Media Group at Infosecurity Europe 2024, Bleih and Pigeon also discussed:

- The increased targeting of essential services and the challenges of defending these sectors;
- Takeaways from a modern cyberwarfare analysis conducted by Cyberint;
- The psychological component to cyberattacks in a conflict.

WATCH ONLINE

> "Even if the attack is not successful, sometimes the fear and the operation itself may harm the public safety psychologically."
>
> ***- Adi Bleih***

"There is a lot more scrutiny coming to the technology providers of frontier large language models that have to be transparent."

Troy Leach
Chief Strategy Officer, Cloud Security Alliance

AI and Adaptive Cybersecurity for SMBs

Troy Leach of Cloud Security Alliance on Adopting AI Solutions With Caution

Small and medium-sized businesses face mounting cybersecurity threats from AI-generated malware. Troy Leach, chief strategy officer at the Cloud Security Alliance, advised SMBs to implement continuous monitoring and automation to effectively mitigate risks.

WATCH ONLINE

Why Resilience Is More Than Just Cybersecurity

Paul Peters on Strengthening Cybersecurity for SMEs and Micro-Businesses

Paul Peters, detective superintendent and managing director at The Cyber Resilience Center for Wales, outlined strategies to enhance cyber resilience, particularly for SMBs and micro-businesses.

WATCH ONLINE

AI in Cybercrime: Lowering the Barrier for Bad Actors

ReliaQuest Field CISO **Rick Holland** on How Cybercriminals Are Exploiting AI Tools

Like security practitioners, cybercriminals want AI too. But in the AI-versus-AI cyber battle, the barrier for malicious actors "keeps getting lower and lower, while the barrier for defenders is getting more complex and more difficult," Holland said.

WATCH ONLINE

Transparency, Not Reticence: CISOs' Key to Crisis Aversion

Seymour of Virgin Media O2 Says Crisis Management Begins With Proactive Planning

Crisis management is a crucial skill for organisations and CISOs. It starts with understanding the business and tailoring plans to its needs, according to Stuart Seymour, group CISO and CSO, Virgin Media O2. He recommended rehearsing plans with leadership and regularly updating them.

WATCH ONLINE

Don Gibson
CISO, Kinly

CyberEdBoard Profiles in Leadership: Don Gibson

Kinly's **Don Gibson** Advises CISOs to Reevaluate Strategies Amid Economic Downturn

In the current economic climate, CISOs must shift priorities to ensure company survival. Don Gibson, CISO at Kinly, advised security leaders to reevaluate their strategies, optimise resource allocation and leverage existing tools to increase their return on investment.

> "Investing in your team and your staff will give you a greater return on investment than going and buying the latest item."
>
> ***- Don Gibson***

In this video interview with Information Security Media Group at Infosecurity Europe 2024, conducted as part of the CyberEdBoard's ongoing Profiles in Leadership series, Gibson also discussed:

- Why CISOs must become storytellers to effectively communicate risks to the board;
- How automation and the effective use of existing tools can help CISOs manage resources better;
- Innovative ways to use cybersecurity budgets more effectively.

WATCH ONLINE CyberEdBoard | Member

“Criminals want their own Copilot, just like we have a Copilot for every security technology out there.”

Rick Holland
Field CISO, ReliaQuest

Addressing Security Gaps for Organisational Resilience

Closed Door Security CEO **William Wright** on Mitigating Common Security Risks

William Wright, CEO of Closed Door Security, shared the significance of enabling SMB signing to prevent NTLM relay attacks, a common vector exploited by ransomware groups. He also shared mitigation strategies identified during penetration testing with various organisations.

WATCH ONLINE

Balancing AI Innovation With Data Privacy and Security

Harmonic Security CEO **Alastair Paterson** on AI Adoption and Privacy Challenges

AI offers significant business benefits but also introduces data privacy risks. According to Harmonic Security's CEO Alastair Paterson, CISOs worry about sensitive data shared with third-party applications.

WATCH ONLINE

Ransomware Goes Pro, Warns Expert

WithSecure's **Tim West** on Ransomware Sophistication, Hacktivism and Role of AI

The ransomware industry has matured. Tim West, director of threat intelligence at WithSecure, warned about the modern ransomware ecosystem, which features an established marketplace of tools and services that can be used.

WATCH ONLINE

Advice to CISOs: Address AI Challenges Now!

Forrester's **Tope Olufon** on AI Deployment, Security Risks and Practical Solutions

Forrester senior analyst Tope Olufon discussed how CISOs face the challenge of shadow IT with generative AI. CISOs need to approach AI as they would any other technology, he said.

WATCH ONLINE

Latest Cyber Insurance Policy Takes Aim at Phishing Attacks

Generali Poland's Cyber Insurance Policies Come With YubiKey MFA and Education

Generali Poland's innovative approach to cyber insurance includes an anti-phishing initiative and market education efforts to enhance cyber resilience. Learn how these measures aim to support small and medium-sized businesses in Poland - and bridge the knowledge gap in cybersecurity.

In this video interview with Information Security Media Group at Infosecurity Europe 2024, Balwiński and Gajkowski also discussed:

- The benefits of educating SMBs and intermediaries to enhance cyber resilience through local events and training sessions;
- Why cyber insurance should complement a proactive cybersecurity approach;
- Generali Poland's collaborations with partners to offer enhanced security solutions and market education.

> "One of our pillar strategies is to be a lifetime partner ... to offer some prevention elements to our clients, to the policy itself."
>
> ***- Marcin Gajkowski***

WATCH ONLINE

“We are there to talk to all organisations and get them to put measures in place to improve their cyber resilience. And if you are a big organisation and have a mature cyber resilience posture, we're there to be signposted to your supply chain, which is an avenue of attacks.”

Paul Peters
Detective Superintendent/Managing Director,
The Cyber Resilience Center for Wales

Brian Honan
CEO, BH Consulting

Microsoft 365's Security Gaps: Logging and Beyond

BH Consulting's **Brian Honan** on Enabling Standard Security Features in Microsoft 365

Brian Honan, CEO of BH Consulting, discussed the need for robust logging capabilities in Microsoft 365 to prevent security breaches. He called for security features to be standard, highlighting issues from a recent intrusion and the risks associated with technologies such as Microsoft's Copilot.

In this video interview with Information Security Media Group at Infosecurity Europe 2024, Honan also discussed:

- The need for Microsoft to include essential security features as standard in all plans;
- The risks posed by new technologies such as Microsoft's Copilot;
- Why multifactor authentication is crucial for protecting sensitive data and preventing cyberattacks.

WATCH ONLINE

> "Microsoft has to look at their whole range of products - cloud and on-premises - with a view that security should not be an extra premium. It should be a core part of the product."
>
> ***- Brian Honan***

"A feature-rich browser has a lot of code. It has a lot of software. And within that software, there are zero-day exploits."

Poornima DeBolle
Co-Founder and CPO, Menlo Security

UK Cyber Sector Booms, But Challenges Remain

Plexal's **Saj Huq** on Why Collaboration Is Key for Cyber Innovation and Resilience

The U.K. cyber sector has grown significantly, but cyberattacks continue to increase. Fostering collaboration among industry, startups and academia is critical to drive cybersecurity innovation, develop skills and strengthen cyber resilience, said Saj Huq, chief commercial officer at Plexal.

WATCH ONLINE

The New Security Leader: Less Techy, More Business-Savvy

Paul Watts of Information Security Forum on Balancing Cyber Risk and Business Goals

Security leadership has evolved significantly in recent years, moving beyond technical expertise to strategic partnerships within organisations. Security professionals now articulate business value and align with organisational objectives, said Paul Watts of Information Security Forum.

WATCH ONLINE

Cloud Security Is a Big Challenge for CISOs - Here's Why

Kevin Kiley of Lacework on Using Data-Driven Solutions to Tackle Modern Threats

Cloud security is becoming a major challenge for security leaders. Kevin Kiley, chief revenue officer at Lacework, explained why traditional security methods fall short in cloud environments and how data-driven approaches offer better protection against new and complex threats.

WATCH ONLINE

Jonathan Armstrong
Partner, Punter Southall Law

Third-Party Oversight Is Needed to Stop Systemic Risk

Legal Expert **Jonathan Armstrong** on Breaches, Security Governance Issues

Third-party vendors should be supervised rigorously to prevent data breaches and ensure transparency across all organisational levels, according to Jonathan Armstrong, partner, Punter Southall Law.

In this video interview with Information Security Media Group at Infosecurity Europe 2024, Armstrong also discussed:

- The importance of third-party oversight;
- The need for enhancing transparency at all levels;
- Engaging the Gen Z workforce in security practices.

> "Many boards need to alter the composition to have a more diverse board in every sense of the word - not just ethnicity and gender, which are important, but diversity of skills as well."
>
> ***- Jonathan Armstrong***

WATCH ONLINE

“It's not all about: 'Everybody's got to do XYZ.' It's a case of working with people to understand the human element to everything that we do.”

Jez Reichmann
Deputy CISO, Channel 4 Corp.

Regulatory Changes Are on the Horizon. Are Companies Ready?

Ropes & Gray's **Rohan Massey** on Compliance Challenges and Strategic Prioritisation

The increasingly regulated landscape of cybersecurity is changing across Europe, America and Asia. Rohan Massey, partner at Ropes & Gray, spoke about the complexities organisations face and the importance of strategic prioritisation to comply with regulatory challenges effectively.

In this video interview with Information Security Media Group at Infosecurity Europe 2024, Massey also discussed:

- How the upcoming NIS2 Directive will affect EU companies and those working with the EU;
- How to build robust incident response plans and governance structures;
- How to ensure that third-party suppliers and partners comply with relevant regulations.

> "Look at your business and think how it applies. What are the risks based on what you do; what data you handle; and how you handle volume, size, sensitivity and location?"
>
> ***- Rohan Massey***

WATCH ONLINE

“Some of the biggest challenges are raising awareness and the profile of security. As security leaders, sometimes we're focused on the technical aspects. We can feel a bit overwhelmed with all of the domains that we have to manage, and we take our eye off the business side. But business engagement is key.”

Aman Sood
Vice President, Cybersecurity Business Engagement,
Elsevier, and CyberEdBoard Member

About ISMG

ISMG is the world's largest media organization devoted solely to cybersecurity and risk management. Each of its 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, AI, OT, and fraud. Its 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

CAREERS INFO SECURITY® · BANK INFO SECURITY® · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

CU Just for Credit Unions INFO SECURITY® · Data Breach. TODAY · infoRisk TODAY · AIToday.io · OT.today · CIO.inc

CyberEd.io · CyberEdBoard · DeviceSecurity.io · FraudToday.io · PaymentSecurity.io

CYBER THEORY · GREYHEAD AN ISMG COMPANY · Xtra mile LIFECYCLE MARKETING · QC MEDIA · ATHENA

ISMG

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io