



RSAConferenceTM2024

Highlights & Insights

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

COMPENDIUM

RSA Conference 2024: The Art of the Possible



What happens when you bring thousands of cybersecurity professionals to San Francisco for four days?

New ideas, collaborative thinking, industry vision and the "Art of the Possible" – the theme of RSA Conference 2024. The industry is at a pivot point: Cybercrime and nation-state attacks are worse than ever before but at the same time, emerging technologies such as generative AI, large language models and automation are changing the game for defenders. Yes, ransomware groups are using AI and other tools and tactics to scale their attacks, but the cybersecurity community is coming together to defeat them through law enforcement action, information sharing and good cyber defense.

As the event's largest media sponsor, we again staffed two video studios at the conference, and we produced nearly 150 interviews. CEOs, CISOs, government leaders, investors, researchers and attorneys all were represented in our interviews and are featured here. This event also showcased the latest developments at ISMG. We debuted ISMG.Studio, an unparalleled platform for leaders in the cybersecurity and technology sectors hosted at major events worldwide. And to help our readers focus on what's important, many of this year's RSA Conference interviews are featured on AIToday.io, OT.today and CIO.inc – major news sites we've recently launched. You'll also see insightful panel discussions and Profiles in Leadership interviews featuring CyberEdBoard members.

We brought our largest-ever ISMG team from around the world to RSA Conference 2024. In these pages, you'll find insightful interviews by our seasoned editorial team – an in-depth view of the latest information and thought leadership from RSA Conference and a glimpse of the Art of the Possible.

Enjoy,

Best,



Tom Field
SVP, Editorial
Information Security Media Group
tfield@ismg.io

Visit us online for more ISMG at RSAC coverage:

ismg.studio



RSAConference™2024

By the numbers

4

Days

2

Studios

150

Interviews

CEOs, CISOs, CIOs, Experts, Investors,
Analysts and More



CISO/CIO

Alexander Antukh, AboitizPower 6

Kris Burkhardt, Accenture 6

Rajeev Batra, The Times Group..... 7

Vaughn Hazen, CN
(Canadian National Railway)..... 7

Brian Spanswick, Cohesity 7

Tom Gillis, Cisco..... 7

Phil Venables, Google Cloud 7

Subra Kumaraswamy, Visa..... 9

Tiauna N. Ross, Stryker..... 10

Sam Curry, Zscaler 11

Marene Allison, Johnson & Johnson..... 12

Rick Doten, Centene Corp and
Carolina Complete Health 12

GOVERNMENT OFFICIALS

Alaina Clark, CISA 13

Vinayak Godse, Data Security
Council of India 13

Floor Jansen, Dutch National
Police Agency 15

Erin West, Santa Clara County,
Office of the District Attorney 15

Robert Tripp, FBI 15

ANALYSTS/ASSOCIATIONS

Daniel Kennedy, 451 Research 17

Diana Burley, American University 17

Clarence Worrell, CERT Division of
Carnegie Mellon University 18

Joseph Blankenship, Forrester..... 18

Philip Reiting, Global Cyber Alliance ... 18

Clar Rosso, ISC2 18

Joe Sullivan, Ukraine Friends 19

Brian Essex, JP Morgan 20

Grant Schneider, Venable 21

Jerry Cochran, PNNL..... 21

Tiauna Ross, Stryker 21

J.C. Raby, Stryker 22

INVESTORS

Bob Ackerman, AllegisCyber 23

Alberto Yépez, ForgePoint Capital 23

Andrew Almeida, Thoma Bravo..... 24

Piyush Malik, Veridic Solutions 24

Harnath Babu, KPMG India 25

Sarfraz Nawaz, Mighty Capital..... 25

Hamza Fodderwala, Morgan Stanley..... 26

Dave DeWalt, NightDragon 26

Jay Leek, SYN Ventures 27

Alex Doll, Ten Eleven Ventures 27

Rama Sekhar, Menlo Ventures..... 28

Yoav Leitersdorf, YL Ventures 28

Ryan Perme, SYN Ventures..... 29

Christian Schnedler, WestCap..... 2

Technology and Services Experts

AI & MACHINE LEARNING

Herain Oberoi, Microsoft..... 27

Sheetal Venkatesh, Cohesity 27

Steve Grossenbacher, Zscaler..... 27

Kevin Skapinetz, IBM..... 28

JC Raby, JP Morgan Investment
Banking..... 28

Heather West, Venable..... 28

Lior Div, Seven AI 28

Jeetu Patel, Cisco..... 29

Aaron Shilts, NetSPI..... 31

Greg Touhill, Carnegie Mellon
University..... 31

Datta Junnarkar, Boeing..... 31

Technology and Services Experts

APPLICATION SECURITY

Rupesh Chokshi, Akamai 32

Pieter Danhieux, Secure
Code Warrior 32

Chris Wysopal, Veracode..... 33

Dror Davidof, Aqua Security..... 33

Technology and Services Experts

CLOUD SECURITY

Mark Ryland, Amazon 34

Rahul Kashyap, Arista Networks 34

Lou Fiorello, ServiceNow 36

Shlomo Kramer, Cato Networks 37

Alicja Cade, Google..... 37

Vamsi Koduru, Normalyze..... 37

Rich Campagna, Palo Alto Networks 37

Sid Shibiraj, Google Cloud 37

Sumedh Thakar, Qualys..... 39

Sébastien Cano, Thales..... 39

Raaz Herzberg, Wiz 39

Monica Shokrai, Google Cloud..... 39

Jay Chaudhry, Zscaler..... 40

Technology and Services Experts

DATA PRIVACY & PROTECTION

Chris Pierson, BlackCloak..... 41

Seemant Sehgal, BreachLock..... 41

Casey Ellis, Bugcrowd..... 42

Sanjay Mirchandani, Commvault..... 42

Video Interviews

TABLE OF CONTENTS

Tamar Bar-Ilan, Cyera.....	42	Wendy Nather, Cisco.....	57	Sunil Patel, Accenture.....	66
Amit Sinha, DigiCert.....	42	Dave Merkel, Expel.....	58	Matt Girdharry, AWS.....	66
Rohit Ghai, RSA.....	43	Lieuwe Jan Koning, ON2IT.....	58	Mark McClain, SailPoint.....	67
Mike Nichols, Elastic.....	44	Dharshan Shanthamurthy, SISA.....	58	Christophe Van de Weyer, Telesign.....	68
Manny Ravelo, Forcepoint.....	44			Maurice Côté, Devolutions.....	68
Amir Ben-Efraim, Menlo Security.....	44	Technology and Services Experts		David Batty, iboss.....	68
Mickey Bresman, Semperis.....	44	RISK MANAGEMENT			
Bipul Sinha, Rubrik.....	46	Thom Dekens, At-Bay Security.....	59	Technology and Services Experts	
J.J. Guy, Sevco Security.....	47	Marten Mickos, HackerOne.....	59	SECURITY OPERATIONS	
Bob VanKirk, SonicWall.....	47	Jason Passwaters, Intel 471.....	60	Nayaki Nayyar, Securonix.....	69
Vivek Ramachandran, SquareX.....	47	Ashley Rose, Living Security.....	60	Anthony Pierce, Splunk.....	69
J. Trevor Hughes, IAPP.....	47	James Foster, ZeroFox.....	60	Bruce Johnson, TekStream.....	70
Barbara Cosgrove, Workday.....	47	Robert Booker, HITRUST.....	60	Mary Lou Prevost, Splunk.....	70
Brian Fox, Sonatype.....	48	Stu Sjouwerman, KnowBe4.....	61		
		Tony Pepper, Egress.....	61	Technology and Services Experts	
Technology and Services Experts		Niloofar Razi Howe, Pondurance.....	62	THREAT DETECTION & RESPONSE	
ENDPOINT SECURITY AND		Stu Solomon, HUMAN.....	62	Kyle Hanslovan, Huntress.....	71
EMAIL SECURITY		Alex Bazhaniuk, Eclipsium.....	62	Will Gragido, NetWitness.....	71
Bradon Rogers, Island.....	49	Joe Sullivan, Ukraine Friends.....	63	Phil Owens, Stamus Networks.....	72
Mike Fey, Island.....	49	Aravind Swaminathan, Orrick,		Alex Pinto, Verizon.....	72
Dan Streetman, Tanium.....	50	Herrington & Sutcliffe.....	63		
Elia Zaitsev, CrowdStrike.....	51			Technology and Services Experts	
Sumit Dhawan, CEO, Proofpoint.....	53	Technology and Services Experts		OT/IOT SECURITY	
John Shier, Sophos.....	54	SECURE ACCESS & IDENTITY		Edgard Capdevielle,	
J R Balaji, Dell Technologies.....	54	MANAGEMENT		Nozomi Networks.....	73
Mihir Maniar, Dell Technologies.....	54	Jeff Shiner, 1Password.....	64	Rick Kaun, Verve Industrial Protection,	
Masha Sedova, VP, Human Risk		Tom Gillis, Cisco.....	64	a Rockwell Automation Company.....	73
Strategy, Mimecast.....	54	Clay Rogers, CyberArk.....	65	Theresa Lanowitz, AT&T	
John Scimone, Dell Technologies.....	56	Amit Chhikara, Deloitte.....	65	Cybersecurity.....	74
		Charles Carmakal, Mandiant.....	65	Dawn Cappelli, Dragos.....	75
Technology and Services Experts		Danny Brickman, Oasis Security.....	65	Robert M. Lee, Dragos.....	76
MANAGED SERVICES		David Bradbury, Okta.....	65	Dr May Wang, Palo Alto Networks.....	78
Curt Aubley, Deepwatch.....	57	Brandon Traffanstedt, CyberArk.....	66	Brad Brooks, Censys.....	79
Edna Conway, EMC Advisors.....	57			Marc Witteman, Riscure.....	79
Behind the Scenes: ISMG at RSAC 2024.....					80



CISO/CIO

Technology and cybersecurity must work hand in hand in modern enterprises. Both CIOs and CISOs are navigating complex IT environments, constantly changing cyberthreats and high visibility on projects deemed crucial to the business. Today, technology and cybersecurity are on the agendas of the board of directors. We spoke with some of the leading CISOs and CIOs in the industry to find out what's keeping them up at night, what's on the horizon and how they plan to meet the challenges of this dynamically changing world.

CyberEdBoard Profiles in Leadership: Alexander Antukh

Antukh Discusses Cybersecurity Leadership and Critical Infrastructure Threats



From malware analyst and ethical hacker to CISO of AboitizPower, Alexander Antukh's cybersecurity journey has shaped his leadership style. It is crucial to allow leaders to understand technical intricacies while maintaining a broader perspective. This blend enables effective communication across diverse stakeholders, Antukh said.

WATCH ONLINE

CyberEdBoard | Member

AI and Passwordless Systems: The New Era in Cybersecurity

Accenture CISO **Kris Burkhardt** on Advancing Cybersecurity With Innovative Tech



As cyberthreats continue to evolve, organizations are increasingly turning to advanced technological solutions to mitigate risks. Replacing traditional passwords with biometrics and passwordless has become imperative for many organizations due to the inherent risks associated with passwords, according to Kris Burkhardt, CISO, Accenture.

WATCH ONLINE

How Generative AI Is Transforming Readers' Experiences

Rajeev Batra of Times Group on How Generative AI Enhances News Content Production



Print and digital media platforms are undergoing a transformation with a focus on improving reader experiences. Generative AI and LLMs can play a key role, but media houses must weigh the pros and cons of adopting AI, with an eye on ROI, said Rajeev Batra, CIO, Bennett, Coleman & Co., The Times Group.

[WATCH ONLINE](#)

CyberEdBoard Profiles in Leadership: Vaughn Hazen

CN Rail CISO Shares Tips for Organizations to Ramp Up Cybersecurity



Organizations with 24/7 operations such as hospitals, power plants and financial services must be hyper-vigilant about cybersecurity, particularly in complex hybrid IT environments. Legacy systems further complicate the process of implementing effective security and complying with regulations, said Vaughn Hazen, CISO, CN Rail.

[WATCH ONLINE](#)

CyberEdBoard | Member

Strengthening Cyber Resilience: Tackling Threats and Gaps

Industry Leaders Discuss Proactive Measures to Strengthen Cyber Resilience



It's time for organizations to focus on strengthening their cyber resilience. Industry leaders Brian Spanswick, CIO and CISO of Cohesity, and Tom Gillis, senior vice president and GM of Security Business Group, Cisco, shared insights into the evolving landscape of cyberattacks and defenses.

[WATCH ONLINE](#)

Supercharge Security With AI

Google Cloud CISO Phil Venables on Using Generative AI in Cybersecurity



AI has been the foundation of many Google products, and Phil Venables, vice president and CISO at Google Cloud, said AI can help streamline and enhance security operations. But to be successful, organizations need to treat AI risk as a data risk and ensure the integrity of the training data and test data.

[WATCH ONLINE](#)



“We use AI to defend billions of people every day, whether it's from malware, safe browsing or spam. Generative AI has demonstrated its worth in analyzing threats, supporting cybersecurity professionals and automating threat detection.”

Phil Venables

VP, CISO, Google Cloud



Subra Kumaraswamy

CISO, Visa

Defenders' Dilemma: Can AI Bolster Cyber Resilience?

Visa's **Subra Kumaraswamy** on Threat Detection, AI and Third-Party Supply Chain Risk

As the threat landscape evolves rapidly with sophisticated attack vectors and adversaries leveraging AI for malicious purposes, businesses must proactively harness AI to bolster their cyber resilience capabilities, said Subra Kumaraswamy, senior vice president and CISO at Visa.

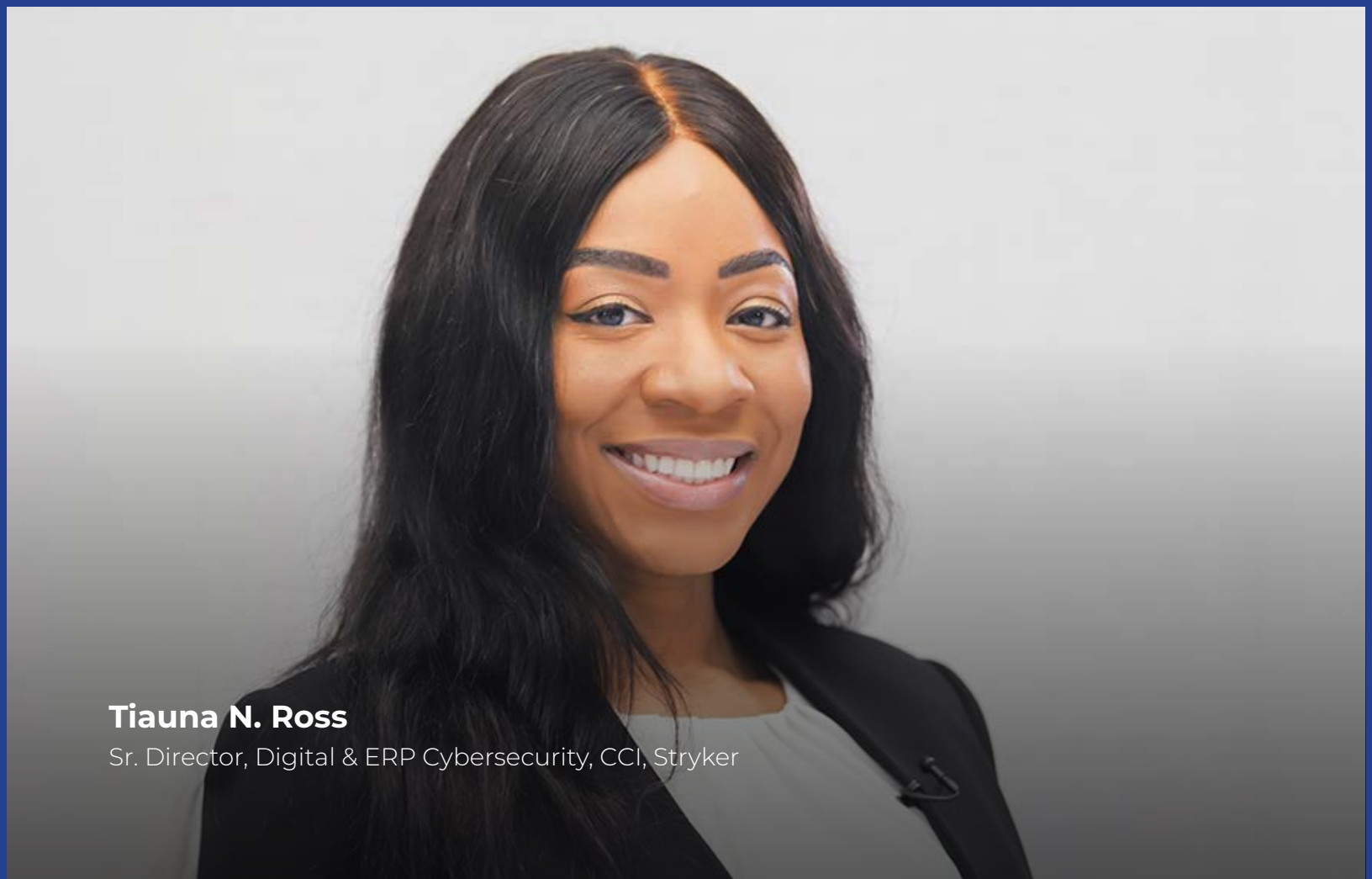
In this video interview with Information Security Media Group at RSA Conference 2024, Kumaraswamy also discussed:

- Visa's multipronged approach to addressing the cybersecurity skills gap through certification programs, apprenticeships and hiring military veterans;
- The importance of data governance to prevent misuse of AI;
- The need to extend supply chain risk assessments beyond third parties to fourth parties.

“We've been using AI for the last 30 years, and we've protected \$40 billion of fraud using AI technology.”

- **Subra Kumaraswamy**

WATCH ONLINE

A portrait of Tiauna N. Ross, a woman with long dark hair, smiling. She is wearing a black blazer over a light-colored top.

Tiauna N. Ross

Sr. Director, Digital & ERP Cybersecurity, CCI, Stryker

CyberEdBoard Profiles in Leadership: Tiauna Ross

Stryker's Ross Discusses Effective Leadership and Mentoring in Security

Since transitioning from CPA to cybersecurity professional in 2015, Tiauna Ross has brought a unique blend of skills and qualities to her leadership role. She attributed her success to adaptability, a passion for problem-solving and a keen understanding of technology's impact on business.

In this video interview with Information Security Media Group at RSA Conference 2024, part of the CyberEdBoard's ongoing Profiles in Leadership series, Ross also discussed:

- The importance of building a strong relationship with vendors in cybersecurity;
- Mentoring the next generation of cybersecurity professionals;
- Why developing business acumen is critical for cybersecurity leaders.

“Engineering and research and development are areas where innovation is a part of what is delivered,” Ross said. “In looking at adjacent fields and capabilities, agile methodology is one of my favorite things to implement.”

- *Tiauna Ross*

WATCH ONLINE

CyberEdBoard | Member



Sam Curry
CISO, Zscaler

Elevating Application Security With AI Insights

Sam Curry of Zscaler Explores AI's Role in Enhancing Security Protocols

"It's always better and cheaper to catch these issues earlier in the cycle," Curry said, advocating for the use of memory-safe programming languages and zero trust architecture.

In this video interview with Information Security Media Group at RSA Conference 2024, Curry also discussed:

- The importance of merging AI-driven models with traditional security to ensure comprehensive system protection;
- The ongoing need for conventional security measures, such as risk assessments and resource allocation, to safeguard AI-integrated systems;
- Challenges and strategies for protecting the integrity, availability and privacy of data within AI systems.

“It's always better and cheaper to catch these issues earlier in the cycle.”

- **Sam Curry**

WATCH ONLINE

CyberEdBoard | Member

The Convergence of Policy and Technology in Cybersecurity

Retired Johnson & Johnson CISO on Building the Next Generation of Security Leaders



Cybersecurity is a "team sport" requiring technology to align with robust policy frameworks to secure nations as well as organizations, said Marene Allison, CEO of Marene Allison Consulting. "All these pieces must come together - technology, government policy and corporate strategy."

[WATCH ONLINE](#)

AI Bias: The Emerging Threat to Sound Business Decisions

VP and CISO **Rick Doten** on Often Overlooked Risks of Relying on Generative AI



Bias lurks everywhere in generative AI: in the data, in the model, in the human interpreting the output of a model. That's why one of the biggest emerging security threats is relying on AI for important business decisions, said Rick Doten, VP of information security at Centene Corp. and CISO of Carolina Complete Health.

[WATCH ONLINE](#)



GOVERNMENT OFFICIALS

Government agencies have always been on the front lines of the war between threat actors and society. But the job of fighting cybercrime and nation-state groups has escalated beyond anyone's expectations. We interviewed some of the leading minds in government about how they're coping with attacks and how they're cementing new partnerships with public and private sector organizations to gain badly needed advantages over the cybercriminals.

CISA Wants Everyday Americans to Help 'Secure Our World'

CISA's **Clark** Discusses New Campaign to Bolster Individual, National Cybersecurity



CISA is calling on everyone from tech firms to ordinary Americans to take part in securing the nation's digital landscape with a new public service announcement titled "Secure Our World." The message is simple: Citizens, software developers and critical infrastructure sectors alike can all help bolster individual and national security, said Alaina Clark, assistant director, CISA.

[WATCH ONLINE](#)

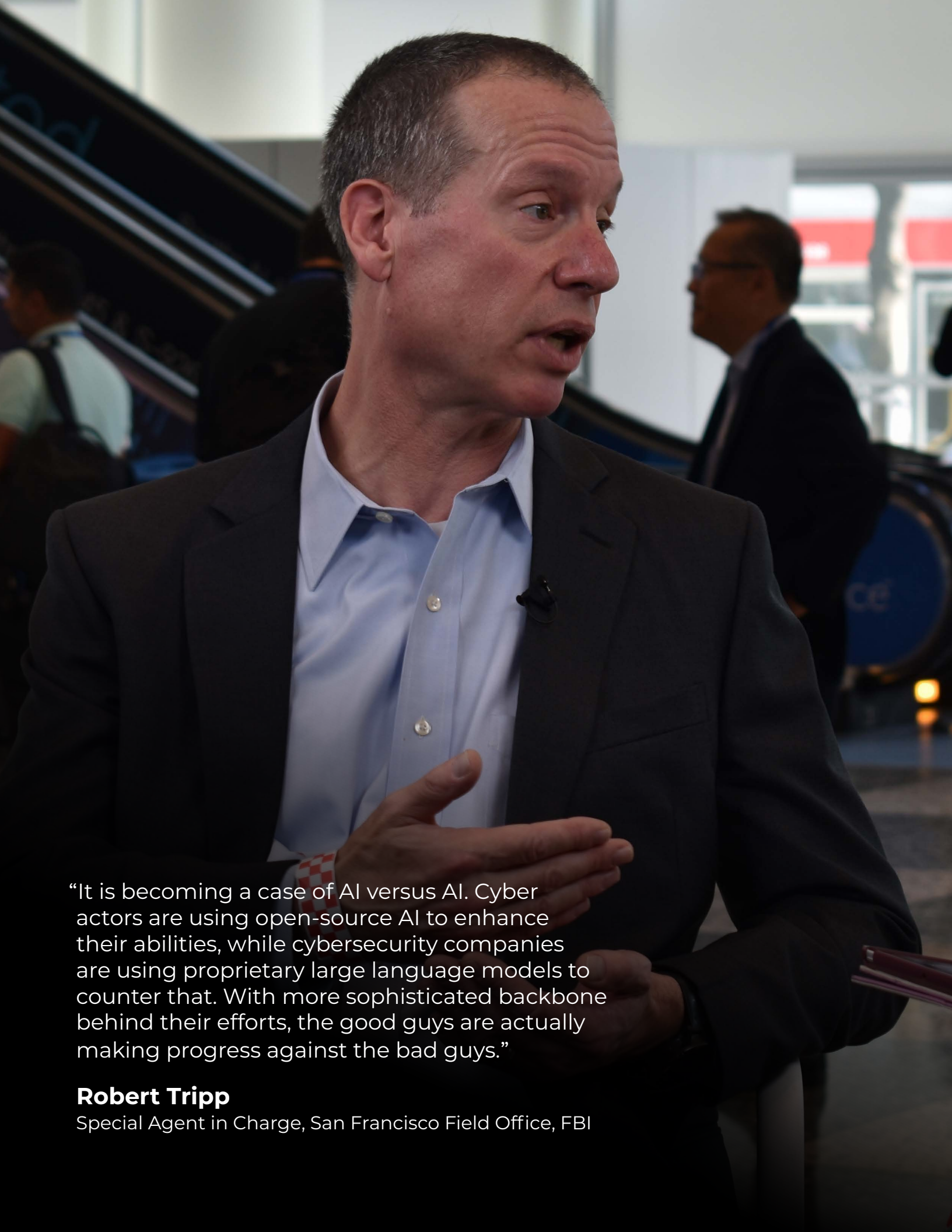
Driving Cybersecurity Innovation in India

DSCI CEO **Vinayak Godse** on India's Thriving Cybersecurity Ecosystem



The Data Security Council of India has been driving innovation in the cybersecurity ecosystem. With over 350 global and homegrown security firms, this environment has led to the development of security products, and many tech companies have established development and engineering operations in India, said Vinayak Godse, CEO, DSCI.

[WATCH ONLINE](#)

A medium shot of Robert Tripp, a man with short grey hair, wearing a dark grey suit jacket over a light blue button-down shirt. He is speaking and gesturing with his hands. The background is a blurred conference or exhibition space with other people and displays.

“It is becoming a case of AI versus AI. Cyber actors are using open-source AI to enhance their abilities, while cybersecurity companies are using proprietary large language models to counter that. With more sophisticated backbone behind their efforts, the good guys are actually making progress against the bad guys.”

Robert Tripp

Special Agent in Charge, San Francisco Field Office, FBI

Advanced Tech Drives Dutch Police's Cybercrime Crackdown

Floor Jansen on High-Tech Crime Unit's Shift From Reactive to Preemptive Practices



Combating the complexity and scale of modern cybercrime effectively is driving a global shift in law enforcement practices from a reactive to a preemptive approach, including innovative use of technologies such as AI and big data analytics.

WATCH ONLINE

Combating Pig-Butchering Scams With a Unified Approach

Deputy DA Erin West Discusses the Anatomy of the Scam and Mitigation Strategies



Pig-butchering scams - a combination of romance and investment scams - have left victims financially bankrupt. Erin West, a deputy district attorney in Santa Clara County, California, discusses the multifaceted nature of the scams, which start with phishing and lead to cryptocurrency fraud.

WATCH ONLINE

Cyber and Financial Crime, Through the FBI Lens

FBI Special Agent Robert Tripp Details Impact of AI, Mitigation Strategies



Artificial intelligence has quickly grown from a potential risk to a real threat that hits many victims. Robert Tripp, special agent in charge of the San Francisco Field Office of the FBI, discusses countermeasures to AI-based attacks, the future of fraud fighting and secure authentication methods.

WATCH ONLINE



“We have facilitated the productization of research, with currently over 12 research projects already in the commercialization process. DSCI is supporting startups that are emerging in critical areas such as quantum security, SCADA OT security and hardware security.”

Vinayak Godse

CEO, Data Security Council of India (DSCI)



ANALYSTS/ASSOCIATIONS

While hundreds of companies offer a variety of tools and services, a community of analysts and associations provides research and training to help security leaders make the right decisions and prepare for the future. We spoke to a variety of analysts and association representatives about the current state of cybersecurity technology and the best bets for the future.

Top CISO Gen AI Challenges: Employee Use, Red Team Testing

Daniel Kennedy of 451 Research Details Gen AI, MFA and Cyber Insurance Challenges



Dealing with generative artificial intelligence is increasingly challenging for CISOs on multiple security fronts, said Daniel Kennedy, principal research analyst for information security for quantitative research at 451 Research, a part of S&P Global Market Intelligence.

WATCH ONLINE

Preparing the Cyber Workforce of the Future

American University's **Diana Burley** on Why Cybersecurity Field Needs Diverse Skills



In the evolving field of cybersecurity, having a diverse workforce is a strategic necessity, said Diana Burley, vice provost of research and innovation at American University. The cybersecurity workforce should comprise "people from different backgrounds, different areas, from different perspectives all working together," she said.

WATCH ONLINE

Securing Attack Surfaces With Cyber-Aware Machine Learning

Carnegie Mellon CERT's **Clarence Worrell** on the Role of Machine Learning in Security



As industries embrace digital transformation, machine learning is emerging in many ways across the whole threat detection process, enhancing both speed and accuracy. Clarence Worrell, senior data scientist, CERT Division of Carnegie Mellon University's Software Engineering Institute, highlighted ML's practical applications and emerging challenges in cybersecurity.

[WATCH ONLINE](#)

Insider Risk in the Generative AI Era

Forrester's **Joseph Blankenship** Says Human Beings Are Fallible



In today's digital landscape as AI adoption increases, insider threats have evolved and now pose significant challenges to enterprises. Joseph Blankenship, Forrester vice president and research director, discussed the impact of generative AI on insider risks and highlighted concerns about accidental data loss and malicious exploitation.

[WATCH ONLINE](#)

Safeguarding the Internet With 'Common Good Cyber' Initiative

Global Cyber Alliance CEO **Philip Reitinger** on the Initiative's Goals and Strategies



The internet plays a key role in virtually every aspect of life, from commerce and communication to governance and personal connectivity. Unlike traditional infrastructure, the internet depends on a whole variety of small organizations, nonprofits and volunteers, said Philip Reitinger, CEO, Global Cyber Alliance.

[WATCH ONLINE](#)

CEO/Founder

Women in Cybersecurity: Light at the End of the Tunnel?

ISC2 CEO **Clar Rosso** Discusses Trends and Challenges for Women in Cybersecurity



For years, the percentage of women in the cybersecurity field has been stagnant at 20% to 25%, but a recent study shows a promising trend: More women are taking cybersecurity leadership roles, and they are staying in those roles, said Clar Rosso, CEO of ISC2.

[WATCH ONLINE](#)

CEO/Founder



Joe Sullivan
CEO, Ukraine Friends

CyberEdBoard Profiles in Leadership: Joe Sullivan

Former Uber CSO Discusses Emerging Digital Risks and Security Leadership Roles

Leaders of digital security risk in the near future will have more influence within their organizations and executive ranks, but they won't necessarily be today's CISOs, said Joe Sullivan, CEO of Ukraine Friends and former CSO of Uber.

In a video interview with Information Security Media Group as part of the CyberEdBoard's ongoing Profiles in Leadership series, recorded at RSA Conference 2024, Sullivan also discussed:

- Why CISOs who think AI is not yet being used within their companies have their "heads in the sand";
- How CISOs must "step up" to assert their security concerns about the enterprise;
- Reflections on his federal sentencing related to a 2016 breach at Uber.

“If we go five years into the future, security will be 100% part of the executive team. But the real question is whether it's going to be the person that is in that CISO role now or if that person is going to get leveled and there will be a different digital risk leader above the CISO.”

- Joe Sullivan

WATCH ONLINE CyberEdBoard | Member



Brian Essex

Executive Director, U.S. Software
Equity Research, J.P. Morgan

Platform or Point Solutions? AI May Be Tipping the Scales

JP Morgan Equity Research Analyst **Brian Essex**
Details AI's Impact, Emerging Threats

To platform or not to platform? That is the question facing many CISOs when it comes to managing cybersecurity vendors. Point solutions often provide the best defense against cutting-edge problems, but they also create vendor management and integration challenges. Platforms built by a single vendor can be simple and handle it all, but they may not do as well for emerging problems.

In this video interview with Information Security Media Group at RSA Conference 2024, Essex also discussed:

- Why ransomware attacks are becoming more sophisticated;
- Why AI is a "civilization-changing technology";
- The three layers of AI that enterprises must secure to ensure that sensitive AI doesn't leak.

[WATCH ONLINE](#)

“There's always been this debate across the industry. For the first time, we're starting to see segments of the industry emerge where platforms can actually give you better visibility and better protections as they leverage the efficiency of their platforms in this new generation of software.”

- **Brian Essex**



Grant Schneider, Senior Director of Cybersecurity Services, Venable

Tiauna Ross, Senior Director of Digital & ERP Cybersecurity, Stryker

Jerry Cochran, Deputy CIO - Cybersecurity & DigitalOps, Pacific Northwest National Laboratory

CyberEdBoard Talks: Implementing Federal Cyber Mandates

Panel Discusses How Organizations Can Navigate New Mandates From the White House

Here's the text you can replace on the left: The White House has released a wave of security guidelines and mandates for critical infrastructure sectors and private industry following U.S. President Joe Biden's 2021 executive order on cybersecurity. Is the industry ready to respond?

In this video interview with Information Security Media Group at RSA Conference 2024, Essex also discussed:

- New federal cybersecurity guidance affecting private sector organizations and critical infrastructure sectors;
- The role of public-private sector collaboration in combating emerging cyberthreats;
- Strategies for enhancing cyber posture and complying with federal regulations.

“There are resource challenges across the board, both from the way the government is funded but also from the way that some of the critical infrastructure entities who are regulated and don't have the opportunity to raise rates and necessarily make the investments that are really needed.”

- **Grant Schneider**

WATCH ONLINE

CyberEdBoard | Member



JC Raby

Managing Director,
JP Morgan Investment Banking

Outrunning the Bear: Cybersecurity in the AI Era

Cybersecurity Expert **JC Raby** on Shifts
in the Field and What Lies Ahead

The hype cycle for AI is much more accelerated than other emerging technologies. But the swift pace of application development and the drive to capture market opportunities are outpacing security. "It's a quantum leap over where the market is trying to catch up from a security perspective," said J.C. Raby, managing director and head of emerging technology at J.P. Morgan Investment Banking.

In this video interview with Information Security Media Group at RSA Conference 2024, Raby also discussed:

- The continuous transformation of cybersecurity tools;
- Emerging trends and key areas of investment for venture capitalists;
- The role of mergers and acquisitions in shaping the future of data security.

"You know the analogy 'outrunning the bear versus your friend'? It's not easy. The bear can get him and get you at the same time."

- **J.C. Raby**

WATCH ONLINE



INVESTORS

The past year posed both challenges and opportunities for cybersecurity firms and the venture capitalists and investors who take huge risks to create and nurture startup companies. But a wide range of investors we spoke with at RSA Conference are optimistic about the future – and emerging AI technologies that could transform the way security organizations operate.

The Dual Role of AI in Cybersecurity

Bob Ackerman Discusses How AI Shapes Offensive, Defensive Cybersecurity Strategies



Advancements in AI have "redefined the table stakes in cybersecurity," said Bob Ackerman, managing director at AllegisCyber. AI is helping enhance defensive mechanisms, making it easier for analysts to differentiate relevant data from background noise, thereby boosting productivity.

WATCH ONLINE

Next-Generation Identity Platforms to See Sizeable Adoption

Alberto Yépez of ForgePoint Capital on the State of the Cybersecurity Marketplace



With so much data being generated and processed, the market is going to experience a proliferation of next-generation identity platforms, said Alberto Yépez, co-founder and managing director, ForgePoint Capital.

WATCH ONLINE

AI in Cybersecurity Investing: Opportunities and Risks

Thoma Bravo's **Andrew Almeida** on AI Integration, Portfolio Growth and Acquisitions



Artificial intelligence plays a crucial role when evaluating potential investment targets. Thoma Bravo, a key player in cybersecurity investments, recognizes AI's pivotal role in enhancing cybersecurity measures and ensuring business resilience, said Andrew Almeida, partner, Thoma Bravo.

WATCH ONLINE

CEO/Founder

Scripting Winning AI Strategies

Panelists Discuss Artificial Intelligence Implementation and Use Cases



Piyush Malik of Veridic Solutions, Harnath Babu of KPMG India, and Sarfraz Nawaz of Mighty Capital discuss the evolving nature of AI projects and the need for strategic approaches that bridge the gap between experimentation and full-scale production.

WATCH ONLINE

Growing Influence of Hyperscalers in Cybersecurity Markets

Morgan Stanley's **Hamza Fodderwala** on Cybersecurity Market Trends and Opportunities



Hyperscalers such as Microsoft, AWS and Google are enhancing cybersecurity acquisitions and investments to better secure their cloud environments and to build robust partner ecosystems, said Hamza Fodderwala, executive director, U.S. Software Equity Research, Morgan Stanley.

WATCH ONLINE

AI, Disinformation and Vendor Consolidation

Dave DeWalt, CEO, NightDragon, Says the State of Cybersecurity Is Vibrant



Generative AI has ushered in a new era of cybersecurity, presenting opportunities for innovation while also posing significant threats to AI models. "It's a curse and a blessing," and the state of cybersecurity is "vibrant" and experiencing a "golden age," said Dave DeWalt, founder and CEO, NightDragon.

WATCH ONLINE

CEO/Founder



“We have been doing this with natural language processing for some years - making our software platforms more conversational with users. If a CEO wants to know something about their business, they can just go to a platform and type that in - whether it's their HR system or their finance system - to see how their revenue is doing.”

Andrew Almeida

Partner, Thoma Bravo

The Role of Automation, Mini Platforms and Cyber Investments

Jay Leek of SYN Ventures Calls for Prevention-First Approach to Combat Cyberthreats



The shortage of skilled cybersecurity professionals poses a formidable challenge for organizations striving to defend against evolving threats. Leek stressed the importance of technology in combating cyberthreats. With the rapid evolution of the threat landscape, human response times cannot match the speed of the adversaries as they exploit vulnerabilities, he said.

[WATCH ONLINE](#)

How AI Is Reshaping the Startup Landscape in Cybersecurity

Venture Capitalist: Tackling AI's Unsolved Problems Creates Startup Opportunities



Enterprise-level ChatGPT has been a game changer. The interface and LLMs created a decade's worth of AI awareness in a year, even though one-third of cybersecurity companies were already using AI. The difference today is scale, as cloud allows massive datasets of all kinds, increasing from 700 variables to millions of data points.

[WATCH ONLINE](#)

CEO/Founder

How AI Is Transforming Cybersecurity Models and Practices

Exploring the Future of AI in Cybersecurity With Menlo Ventures' Rama Sekhar



The introduction of artificial intelligence has transformed cybersecurity, presenting organizations with both new challenges and innovative solutions. AI is not just a tool but a pivotal element in redefining security strategies, said Rama Sekhar, partner with Menlo Ventures.

[WATCH ONLINE](#)

Revamping Cybersecurity: Innovative Approaches by Startups

Yoav Leitersdorf on Startup Potential for the Future of Cybersecurity



Yoav Leitersdorf, managing partner at venture capital firm YL Ventures, discusses how technology startups are spearheading transformative initiatives. As organizations face evolving threats, the need for innovative approaches has never been more pressing, he said.

[WATCH ONLINE](#)

CEO/Founder

How Investors Boost Cybersecurity Across Portfolio Companies

WestCap's **Christian Schnedler** on Why Vetting Portfolio Security Posture Is Crucial



Investors are increasingly involving themselves in the cybersecurity posture of their portfolio companies. Christian Schnedler, managing director and cyber practice lead at WestCap, attributes the increased involvement to the intertwining of businesses with digital platforms.

[WATCH ONLINE](#)

Cybersecurity Startup Ecosystem: A VC's Perspective

Ryan Permech of SYN Ventures on Finding Novelty, TAM in Startups



SYN Ventures outlined three critical factors to consider when evaluating startups: the team, technology and Total Addressable Market, or TAM. Startups must understand the problems they are solving and create a unique position in the market.

[WATCH ONLINE](#)

CEO/Founder



TECHNOLOGY AND SERVICES EXPERTS

AI & MACHINE LEARNING

Addressing CISOs' Concerns About Generative AI Security

Microsoft's **Oberoi** on Executive Awareness, Governance Challenges in AI Security



As conversations around the intersection of artificial intelligence and cybersecurity continue to intensify, CISOs are increasingly voicing their top concerns regarding the use of generative AI, data protection and regulatory governance, said Herain Oberoi, general manager, Microsoft Security.

WATCH ONLINE

Fighting Back Against Double Extortion and Data Exfiltration

Cohesity's **Venkatesh** and Zscaler's **Grossenbacher** on Distributed Data Management



Sheetal Venkatesh, senior director, product management, Cohesity, and Steve Grossenbacher, director, product marketing, Zscaler, discuss double-extortion ransomware, Cohesity and Zscaler's collaboration, and the power of AI-driven solutions for sensitive data protection.

WATCH ONLINE

82% Leaders Find It Essential to Secure AI; Only 24% Do It

IBM Security's **Kevin Skapinetz** on Embedding Security in AI Development



AI adoption has transformed how security teams work. According to Kevin Skapinetz, vice president of strategy, IBM Security, AI can augment security professionals by enabling them to tackle complex tasks more efficiently and generate security content through generative AI.

WATCH ONLINE

Outrunning the Bear: Cybersecurity in the AI Era

Cybersecurity Expert **JC Raby** on Shifts in the Field and What Lies Ahead



JC Raby, managing director, head of emerging technology, JP Morgan Investment Banking, shares his insights on how historical trends inform current practices and future innovations in the dynamic field of cybersecurity - from early penetration testing to advanced AI solutions.

WATCH ONLINE

Integrating AI Into Cybersecurity Systems

Venable's **Heather West** on the Types of Attacks on AI and Securing AI Models



"We need to be integrating AI into cybersecurity systems," said Heather West, senior director, cybersecurity and privacy services, Venable. While AI models are "not yet standardized enough at attack," the rest of the system can be targeted. She discussed key traditional cybersecurity best practices.

WATCH ONLINE

CyberEdBoard | Member

The AI Standoff: Attackers Versus Defenders

Lior Div, Former CEO and Co-Founder, Cybereason, on the Pros and Cons of AI



Lior Div, former CEO of Cybereason and co-founder and CEO of Seven AI, discusses how hackers use AI to become smarter and more effective. He also emphasizes that cybersecurity defenders need to harness the power of AI more than ever to stay ahead of attackers.

WATCH ONLINE



Jeetu Patel

EVP & GM, Security & Collaboration, Cisco

The Need to Embed AI in Cybersecurity Frameworks

Cisco's **Jeetu Patel** on Industrywide Collaboration to Boost AI Defenses

Integrating generative AI into cybersecurity strategies is a pivotal shift in how organizations safeguard their assets. If AI is not embedded within cybersecurity frameworks, the adversaries will be far ahead, said Jeetu Patel, executive vice and general manager, security and collaboration, Cisco.

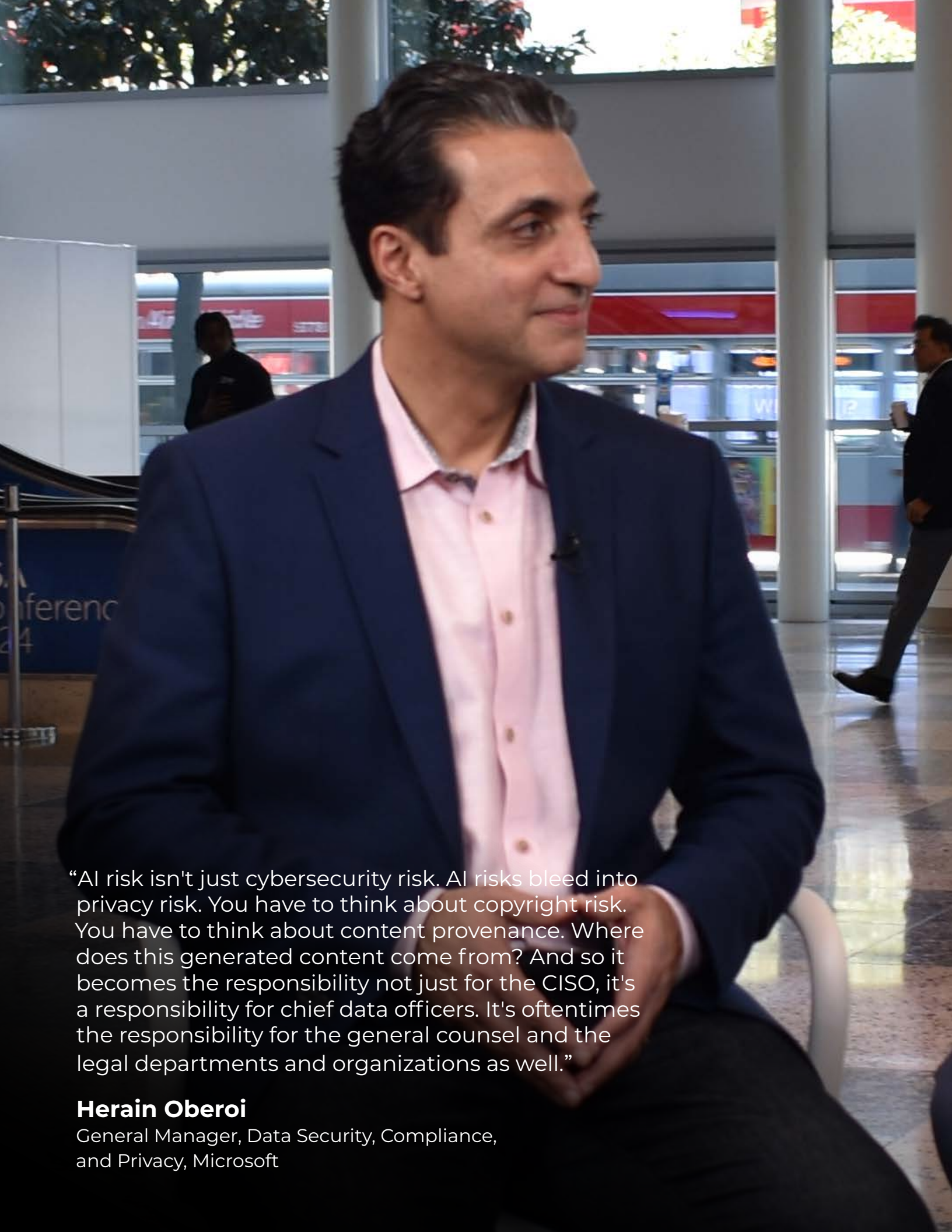
In this video interview with Information Security Media Group at RSA Conference 2024, Patel also discussed:

- Proactively integrating AI into cybersecurity strategies;
- The challenges security practitioners face due to widespread adoption of AI tools;
- Cisco's commitment to investing in AI.

WATCH ONLINE

“In the short term, people overestimate its impact. And in the long term, they grossly underestimate its impact,” Patel said. “If we don't have AI built natively in the defenses, we're going to have the adversary take the advantage.”

- **Jeetu Patel**



“AI risk isn't just cybersecurity risk. AI risks bleed into privacy risk. You have to think about copyright risk. You have to think about content provenance. Where does this generated content come from? And so it becomes the responsibility not just for the CISO, it's a responsibility for chief data officers. It's oftentimes the responsibility for the general counsel and the legal departments and organizations as well.”

Herain Oberoi

General Manager, Data Security, Compliance, and Privacy, Microsoft

The Shift to Continuous AI Model Security and Pen Testing

Aaron Shilts of NetSPI on Security Challenges, Threats of AI Models



The challenges of securing proprietary data within AI models and the paradigm shift in enterprise security are brought about by the widespread adoption of AI models. Aaron Shilts, president and CEO, NetSPI, discusses the risks posed by AI and the importance of continuous security assessments.

WATCH ONLINE

CEO/Founder

AI, AI, AI: Opportunities, Implementations and an AISIRT

Greg Touhill Details AI Attacks and Necessary Guardrails



Greg Touhill, director of the Carnegie Mellon University Software Engineering Institute's CERT Division, detailed the creation of the AISIRT to address the increase in vulnerabilities in materials, products and services, including in software that is used to create machine learning models.

WATCH ONLINE

AI on the Agenda for CIOs

Datta Junnarkar, CIO, Maritime, on How Boeing Is Driving Generative AI Adoption



As generative AI races into boardrooms, Datta Junnarkar, CIO of Maritime at Boeing, champions training and harnessing employee innovation to master rapid technological advances. "We wanted to listen to what our employees are trying to do," Junnarkar said.

WATCH ONLINE



TECHNOLOGY AND SERVICES EXPERTS

APPLICATION SECURITY

Securing APIs: Akamai's Acquisition Strategy

Akamai's **Rupesh Chokshi** on API Trends and Noname's Integration Road Map



API security is a critical concern in today's interconnected world as APIs are prime target for attackers. Rupesh Chokshi, senior vice president and general manager, application security, Akamai, shared insights into the recent acquisition of Noname Security driven by the increasing adoption of APIs in the digital economy.

[WATCH ONLINE](#)

Enhancing Code Security With the Developer Trust Score

Pieter Danhieux on the Benefits of Trust Score for CISOs and Developers



Secure code has been a hot topic among cybersecurity practitioners. Even today, developers are struggling to produce fast and secure code - a problem that's been around for 20 to 25 years, said Pieter Danhieux, co-founder, chairman and CEO of Secure Code Warrior. The Developer Trust Score may just be the solution.

[WATCH ONLINE](#) **CEO/Founder**

The Role of AI in Cloud Application Security

Dror Davidoff of Aqua Security on Trends and Techniques of AI in Cloud Security



Among its many use cases, AI technologies are now being integrated into cloud environments to bolster security. With AI, organizations can automate the detection of code generated by machine learning models, enhancing the security posture without the traditional reliance on extensive manual oversight, said Dror Davidoff, co-founder and CEO of Aqua Security.

[WATCH ONLINE](#)

CEO/Founder

The Crossroads of AI and Application Security

Veracode's **Chris Wysopal** on Navigating AI's Risks and Rewards in App Security



AI has been in cybersecurity for a long time, but generative AI is the new thing, said Chris Wysopal of Veracode. With its ability to analyze and generate code, generative AI presents both challenges and solutions - the yin and the yang - reshaping how developers and security professionals approach software development and maintenance.

[WATCH ONLINE](#)

CEO/Founder



The Rise of Memory-Safe Languages in Secure Development

Amazon's **Mark Ryland** on Rust and the Importance of Improving Open-Source Security



Secure development and memory-safe languages are becoming increasingly critical for addressing long-standing security issues such as buffer overruns and remote code execution vulnerabilities. Mark Ryland, director of Amazon Security, Amazon, emphasized the shift toward using Rust, a high-performance language designed to eliminate such bugs.

[WATCH ONLINE](#)

Network Security in the Era of Cloud and AI

Rahul Kashyap of Arista Networks on the Evolution and Complexity of Networks



As CISO at Arista Networks, Rahul Kashyap oversees cybersecurity operations and incubates business initiatives. If you look back to 10 years ago, enterprise network were monolithic, Kashyap said, but they have been evolving.

[WATCH ONLINE](#)



“If you are not taking a view of what is the overall risk that is created by cyber infrastructure to your business, then you don't know where to focus, what to fix first and what to prioritize.”

Sumedh Thakar

President & CEO, Qualys



Lou Fiorello

VP & GM, Security Products, ServiceNow

Companies Adopting Automation See 95% Boost in Some Metrics

ServiceNow's **Lou Fiorello** on Upleveling Security Operations With Automation

Automation and AI are transforming security operations by significantly reducing response times and improving overall efficiency. Companies that have leaned in on automation aspects can see upward of 90% to 95% improvement in some metrics, said Lou Fiorello, vice president and general manager, security products, ServiceNow.

In this video interview with Information Security Media Group at RSA Conference 2024, Fiorello also discussed:

- ServiceNow's new tools to enhance vulnerability management and threat intelligence integration;
- The role of generative AI in boosting productivity and insight generation in security operations;
- Automation in operational technology environments.

[WATCH ONLINE](#)

“It's not just the security team, but it's security and the rest of the organization driving improved security posture. That, plus automation, is the journey.”

- **Lou Fiorello**

How Integrated Security Platforms Are Redefining Defense

Cato Networks' CEO **Shlomo Kramer** on the Benefits of Integrated Security Platforms



As threats become more sophisticated, the demand for integrated security platforms is at an all-time high. This demand is driven by the operational inefficiencies of traditional security models, said Shlomo Kramer, co-founder and CEO, Cato Networks.

WATCH ONLINE

CEO/Founder

Adapting Data Security for the Modern Cloud Era

Vamsi Koduru of Normalyze Explores the Evolution of Data Security Challenges



Data security products have been available for decades, but as enterprises shift from on-premises data centers to cloud-based environments, traditional solutions fall short in meeting this change in the landscape. "They're no longer meeting business needs," said Vamsi Koduru, director of product management at Normalyze.

WATCH ONLINE

Don't Silo Cyber Risk to CISOs, Says Former Financial CISO

Google's **Alicja Cade** Says 'Cyber' Isn't Just for CISOs



Tossing the word "cyber" onto something doesn't automatically mean it should belong to the chief information security officer. Cyber risk belongs to everyone in an organization - the users and the business divisions that make decisions about what kind of risks are acceptable. Chief information and technology officers also own it.

WATCH ONLINE

Security With Google Cloud NGFW Enterprise - Powered by Palo Alto Networks

Palo Alto Networks and Google Cloud Execs on Power of Security Solution Partnership



The move to cloud offers numerous benefits, but cloud apps and multi-cloud environments add complexity to defending IT environments. Palo Alto Networks and Google Cloud just renewed a multiyear, multibillion-dollar partnership to give customers end-to-end protection and secure infrastructure.

WATCH ONLINE



“Good AI starts with data. While there's a lot of general purpose data sitting out there for ChatGPT and the world, for cyber you need customer-specific data to see if a customer is being targeted, attacked or if reconnaissance is being done.”

Jay Chaudhry

Founder, Chairman & CEO, Zscaler

Enterprise Cyber Risk: Overcoming the Issue of Siloed Tools

Sumedh Thakar, Qualys, on Enhancing Cybersecurity Through Strategic Risk Management



Cybersecurity is evolving beyond tool deployment toward the strategic management of threats. While companies deploy numerous tools to address security incidents, this siloed strategy may obscure the bigger picture - understanding the comprehensive cyber risk to the business.

WATCH ONLINE

CEO/Founder

Thales' Strategic Move to Enhance Data Security

Sébastien Cano on Building Security Capabilities With Imperva Acquisition



The data security market today is characterized by a heightened emphasis on consolidation and platform solutions in response to challenges such as vendor fatigue. While data security is not a new industry, it continues to evolve significantly, according to Sébastien Cano, senior vice president for cloud protection and licensing at Thales.

WATCH ONLINE

From CNAPP to CDR: The Cybersecurity Road Ahead

Wiz's **Raaz Herzberg** on Market Consolidation and Securing Cloud Environments



Wiz, a cloud security company, has recently announced \$1 billion funding with a total valuation of around \$12 billion. Shedding light on Wiz's recent developments, Raaz Herzberg, the company's chief marketing officer and vice president of product strategy, said Wiz plans to invest in talent acquisition, product innovation and potential expansions through acquisitions.

WATCH ONLINE

Cyber Insurers Embrace Cloud Metrics, Prepare for AI Impact

Google Cloud's **Monica Shokrai** on How AI Is Disrupting the Cyber Insurance Market



While still an immature market, cyber insurance has progressed quickly in understanding risk assessment. Insurers have moved beyond relying solely on questionnaires filed by CISOs to incorporate external security scanning and cloud metrics aligned with an organization's internal security posture, said Monica Shokrai, head of business risk and insurance at Google Cloud.

WATCH ONLINE



Jay Chaudhry

Founder, Chairman & CEO, Zscaler

Going All-In With AI at Zscaler to Raise the Bar in Cyber

Jay Chaudhry, CEO of Zscaler, on Company's AI Commitment, Solutions

Zscaler is going all-in in its investment in AI to bolster its customers' ability to stay ahead of threat actors, including the company's recent purchase of Avalor and its hiring of a chief AI officer, said Jay Chaudhry, the company's founder, chairman and CEO.

In this video interview with Information Security Media Group at RSA Conference 2024, Chaudhry also discussed:

- Why VPNs and firewalls "need to be retired";
- How the Biden administration's policies and requirements have changed the perception of zero trust;
- Protecting the Department of Defense and other major federal government agencies.

“We have that data because of a large number of customers, which includes over 40% of Fortune 500 companies.”

- Jay Chaudhry

WATCH ONLINE

CEO/Founder



TECHNOLOGY AND SERVICES EXPERTS

DATA PRIVACY & PROTECTION

The Blurring Personal-Professional Executive Risks of a CISO

BlackCloak CEO **Pierson** Discusses Leadership, AI Threats, Regulatory Landscape



Nearly half of more than 500 CISOs reported cyberattacks on the personal lives of their executives, indicating the growing prevalence of hackers targeting individual employees - and skirting the strong protections of large enterprises, according to a study commissioned by Digital Executive Protection company BlackCloak.

WATCH ONLINE **CEO/Founder**

Offensive Security: Lose That Loser's Mindset

BreachLock's **Seemant Sehgal** on Proactively Finding Out Where Your Defense Will Fail



Offensive security in the past five years has moved from traditional pen testing to a platform-based strategy. BreachLock CEO Seemant Sehgal discussed why offensive security is more important than ever and how to convince the board to increase the budget for it.

WATCH ONLINE **CEO/Founder**

Outsmarting Adversaries: Using AI for Security

Bugcrowd Founder **Casey Ellis** on the Challenges of Integrating AI Into Security



Hackers are using generative AI to boost their malicious activities and are making progress toward autonomous, AI-driven internet exploitation. Casey Ellis, founder of Bugcrowd, highlights that while bias is a key AI concern, integrating AI safely into existing processes is a bigger challenge.

WATCH ONLINE

CEO/Founder

How to Increase Cyber Resilience With Continuous Testing, AI

Commvault's **Mirchandani** on Cyberthreat Response, Ensuring Operational Continuity



Commvault President and CEO Sanjay Mirchandani discussed how continuous testing and AI-enhanced recovery capabilities are crucial for businesses to swiftly respond to cyberthreats and ensure operational continuity. These capabilities will help "good AI to fight bad AI," he said.

WATCH ONLINE

CEO/Founder

Using AI at Scale Makes Data an Even More Critical Asset

Cyera's **Tamar Bar-Ilan**: AI Benefits Are Clear But Unintended Consequences Are Not



With the explosion of data, organizations need to understand what data they have, how it is being used, where it's going and how it is secured. Cyera's platform enables them to do just that, and the company has grown into a \$1.4 billion unicorn in just three years.

WATCH ONLINE

CEO/Founder

Post-Quantum Cryptography Key to Ensuring Digital Trust

DigiCert CEO **Amit Sinha** on Mitigating the Quantum Threat to Digital Communications



Quantum computing gives malicious actors the opportunity to break encryption algorithms and exploit the inherent trust that users place on legitimate applications and websites, and only post-quantum cryptography can defeat the threat and preserve the sanctity of digital communications, said Amit Sinha, CEO, DigiCert.

WATCH ONLINE

CEO/Founder



Rohit Ghai
CEO, RSA

NIST CSF 2.0 and the State of Cybersecurity

RSA CEO **Rohit Ghai** on Impact of New Regulations, Trends in Identity and AI

The federal government has expanded its regulations for cybersecurity best practices with the long-awaited NIST CSF 2.0 standards, and the new guidelines place more emphasis on governance and overall risk management, as well as the "outsized role of identity in the context of a zero trust security posture," said Rohit Ghai, CEO, RSA.

In this video interview with Information Security Media Group at RSA Conference 2024, Ghai also discussed:

- The state of the identity technology market and key trends including passwordless authentication;
- The implications artificial intelligence tools have for identity and why AI is a double-edged sword for our sector;
- Strategies for defending against a wide range of cybercriminals' tactics such as MFA bypass.

“2.0 broadens the scope of the document to beyond just critical infrastructure. Cybersecurity is now everybody's problem.”

- **Rohit Ghai**

WATCH ONLINE

CEO/Founder

How Elastic Is Changing the SIEM Game With AI Solutions

Mike Nichols on Enhancing SOC Workflows and Combating Analyst Burnout



The security information and event management landscape is constantly evolving, but "traditional SIEM has classically been stuck in the enterprises due to accessibility," according to Mike Nichols, vice president of product management for security at Elastic.

WATCH ONLINE

Future-Proofing Cybersecurity With Data-Centric Approaches

Manny Ravelo, CEO of Forcepoint, Discusses Next-Gen Data Security Strategies



As enterprises face growing complexities in data management, leaders seek innovative solutions to protect sensitive information. Manny Ravelo, CEO of Forcepoint, highlights the transition from traditional data loss prevention to more nuanced, AI-driven security models.

WATCH ONLINE

CEO/Founder

Securing the Enterprise Browser

Menlo Security's Ben-Efraim on Enhancing Existing Browsers With Additional Security



An enterprise browser offers control over browsing sessions and capabilities for enhanced security and connectivity, but enterprises need to disable browser synchronization to prevent security breaches, such as the inadvertent propagation of enterprise passwords, according to Amir Ben-Efraim, CEO, Menlo Security.

WATCH ONLINE

CEO/Founder

Identity Systems: Attackers' Keys to the Kingdom

Semperis' Mickey Bresman on Ransomware's New Frontier: Identity and Backup Systems



Ransomware attackers are increasingly targeting identity systems and backup files to gain control over organizational operations. Securing these systems has become critical to preventing cybercriminals from significantly disrupting operations and demanding ransom payments.

WATCH ONLINE

CEO/Founder



“We need to adopt newer standards that will allow us to have that foundational trust element by adopting algorithms that are safe from even quantum computers.”

Tamar Bar-Ilan

Co-Founder & CTO, Cyera



Bipul Sinha

Co-Founder, Chairman and CEO, Rubrik

The Challenges in Protecting Healthcare Data, Resiliency

Bipul Sinha, Co-Founder, Chairman and CEO, Rubrik, on Digital Transformation

As hospitals and other healthcare providers continue to digitize all kinds of very sensitive healthcare information, these organizations are becoming an increasingly attractive target for threat actors for a variety of reasons, said Bipul Sinha, co-founder, chairman and CEO, Rubrik.

In this video interview with Information Security Media Group at RSA Conference 2024, Sinha also discussed:

- The digital transformation of healthcare;
- The challenges of safeguarding health data in the cloud;
- The significance of Rubrik's purchase last August of data security posture management startup Laminar for \$104.9 million.

“Attackers are getting smart. They used to attack and encrypt files, now they're attacking at the virtual machine layer, which helps them escape detection.”

- **Bipul Sinha**

WATCH ONLINE

CEO/Founder

Solving the Fractured Data Problem in Exposure Management

Sevco Security's **J.J. Guy** on Aggregating and Prioritizing Vulnerabilities



Enterprises grapple with a deluge of vulnerabilities, misconfigurations and IT hygiene gaps. An automated exposure management program helps prioritize and remediate risks, fostering collaboration between security and IT teams, says J.J. Guy, CEO, Sevco Security.

WATCH ONLINE

CEO/Founder

Managed Security Service Provider Needs in the SMB Market

Bob VanKirk, President and CEO of SonicWall, on Latest MSSP Trends



Small and medium-sized businesses have a "resounding need" for SASE as part of managed security services, and that's why SonicWall has added SASE to its security stack, said Bob VanKirk, the company's president and CEO.

WATCH ONLINE

CEO/Founder

Can Browser-Native Security Stop Web Attacks?

Vivek Ramachandran of SquareX on Why the SASE/SSE Model Is Inadequate



Interest in SASE/SSE technologies is growing as organizations and vendors move toward consolidated networking and security platforms. But SASE has not been able to deliver on its promise of protecting enterprise users, according to Vivek Ramachandran, founder and CEO, SquareX.

WATCH ONLINE

CEO/Founder

Governance, Privacy and Ethics in the Age of AI

IAPP and Workday Executives Detail the Nuances of Dealing With the Impact of AI



Artificial intelligence, generative AI and machine learning have always been part of the broader privacy conversation, according to J. Trevor Hughes, CEO and president, IAPP. Workday Vice President and Chief Privacy Officer Barbara Cosgrove shares how she helped the company build an AI framework.

WATCH ONLINE

CEO/Founder



Brian Fox

Co-Founder & CTO, Sonatype

State of Software Security: Has It Moved Past Unacceptable?

Brian Fox Discusses Legislative Efforts and Challenges in Software Security

The state of software security is constantly evolving, and although awareness and conversation around it have increased, the industry is no closer to solving the problem, said Brian Fox, co-founder and chief technology officer, Sonatype.

In this video interview with Information Security Media Group at RSA Conference 2024, Fox also discussed:

- How companies are managing open-source software components after Log4j;
- How organizations should approach software composition analysis;
- How Sonatype is evolving to help customers meet their software security needs.

WATCH ONLINE

CEO/Founder

“We are in a world where we can’t trust any of our software anymore until we get better at understanding who the people behind it are, what their motivations are, and providing that level of transparency.”

- **Brian Fox**



TECHNOLOGY AND SERVICES EXPERTS

ENDPOINT SECURITY AND EMAIL DESURITY

Rethinking Browser Security: From Risk to Asset

Island's **Bradon Rogers** Discusses Transforming Browsers for Enterprise Security



The traditional browser was never built for the enterprise environment, yet it remains a central tool for application delivery and content consumption. Bradon Rogers, chief customer officer at Island, explained the inherent risks associated with conventional browsers and how Island's enterprise browser approach challenges the status quo.

[WATCH ONLINE](#)

How the Enterprise Browser Marries IT and Security

Island Co-Founder and CEO **Mike Fey** on Balancing Security and User Experience



Traditionally, CISOs initiate discussions about enterprise browsers due to their understanding of cybersecurity challenges in consumer browsers. But the involvement of CIOs is crucial as they oversee changes affecting end-user experience, according to Mike Fey, co-founder and CEO, Island.

[WATCH ONLINE](#)

CEO/Founder



Dan Streetman
CEO, Tanium

How AI and Real-Time Data Are Reshaping Endpoint Security

Tanium CEO **Dan Streetman** on Breaking Down Silos and Unified Endpoint Management

In today's digital business world, the separation of IT and security teams often hampers unified decision-making processes.

In this video interview with Information Security Media Group at RSA Conference 2024, Streetman also discussed:

- How Tanium's partnership with Microsoft amplifies the impact of real-time data;
- The dangers of relying on outdated data for AI-driven decision-making;
- The role of AI in endpoint security.

WATCH ONLINE

CEO/Founder

“We can give them the insights. We call it a confidence score to make decisions on what to do next. That changes the paradigm.”

- **Dan Streetman**



Elia Zaitsev

Chief Technology Officer, CrowdStrike

Transform Traditional Security Models With AI-Integrated SOC

CrowdStrike CTO **Elia Zaitsev** on AI's Role in Overcoming Legacy SIEM Challenges

Legacy SIEM technology is deemed ineffective in modern security architecture. Traditional systems fail to integrate data from diverse sources, hindering effective incident response and leaving organizations vulnerable to evolving threats, according to Elia Zaitsev, chief technology officer at CrowdStrike.

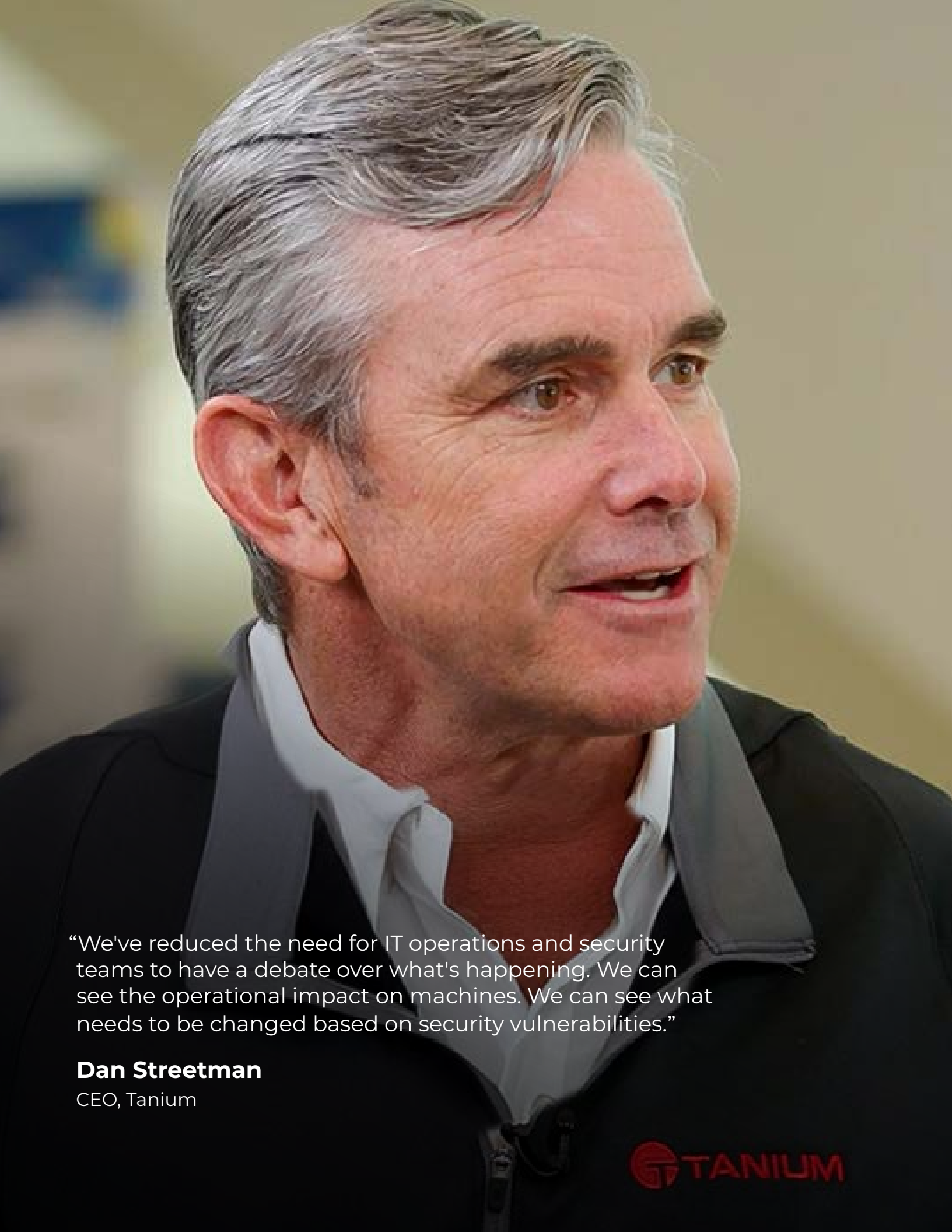
In this video interview with Information Security Media Group at RSA Conference 2024, Zaitsev also discussed:

- The challenges related to data proliferation;
- Why human oversight is crucial for creative problem-solving and decision-making in security operations;
- How AI is more effective in structured scenarios versus unpredictable, real-world situations.

[WATCH ONLINE](#)

“From a defensive standpoint, we're going to still want to bring in AI technologies to help deal with this larger and faster onslaught. But you still need the humans there - being creative, looking for that unknown unknown.”

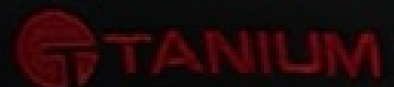
- *Elia Zaitsev*



“We've reduced the need for IT operations and security teams to have a debate over what's happening. We can see the operational impact on machines. We can see what needs to be changed based on security vulnerabilities.”

Dan Streetman

CEO, Tanium





Sumit Dhawan
CEO, Proofpoint

A Human-Centric Security Approach, Supported by AI

Protect People and Infrastructure Simultaneously: Proofpoint
CEO **Sumit Dhawan**

To address the cliché of people being the weakest link, cybersecurity company Proofpoint said it's putting humans at the center of its security.

In this video interview with Information Security Media Group at RSA Conference 2024, Dhawan also discussed:

- The challenges of protecting individual users within corporate security frameworks;
- How firms benefit from integrating infrastructure protection with human-centric security;
- Using generative AI to enhance predicting and mitigating security threats.

“You get EDR. You get SASE solutions that protect your infrastructure, endpoint and network. You take a very similar approach in protecting your people.”

- **Sumit Dhawan**

WATCH ONLINE

CEO/Founder

Ransomware Defense Strategies: Never Trust a Criminal

Sophos Field CTO **John Shier** on the Latest Annual Report on the State of Ransomware



Ransomware attacks have slightly declined in frequency but have grown more sophisticated and costly over the past five years. Sophos Field CTO John Shier shared insights from the latest annual report on the state of ransomware, revealing trends that challenge even the most fortified defenses.

[WATCH ONLINE](#)

The World's Most Secure PC and Holistic Security Services From Dell

J R Balaji and **Mihir Maniar** on Dell's Proactive Approach to Combating Cyberthreats



Dell Technologies, a leading PC manufacturer, claims to make the "world's most secure commercial PCs." J R Balaji and Mihir Maniar of Dell discuss the company's proactive security approach of anticipating emerging threats and providing end-to-end security services.

[WATCH ONLINE](#)

Human Risk Crisis: 8% of Employees Cause 80% of Incidents

Mimecast's **Masha Sedova** on Using a Metrics-Driven Approach to Mitigate Human Risk



More than two-thirds of breaches involve the human element. Traditional security awareness initiatives, often fixated on training participation and engagements, are inadequate in mitigating incidents triggered by employees' risky behaviors, said Mimecast's Masha Sedova.

[WATCH ONLINE](#)



“Customers tell us that 70% of the threats are actually coming in as social engineering attacks on their own people. People need to be protected from all these attacks.”

Sumit Dhawan

CEO, Proofpoint

A portrait of John Scimone, a man with short brown hair, wearing a grey suit jacket over a light-colored collared shirt. He is smiling slightly and looking directly at the camera.

John Scimone

President & Chief Security Officer, Dell Technologies

Securing AI's Role in Modern Business

John Scimone of Dell Technologies on AI Governance and Ethical Use

Artificial intelligence technology has become a major player in modern business security. John Scimone, president and chief security officer, Dell Technologies, emphasized AI's disruptive yet beneficial nature, highlighting three imperatives for security practitioners: managing new risks associated with AI adoption, preparing for criminal exploitation of AI and using AI to enhance security outcomes.

In this video interview with Information Security Media Group at RSA Conference 2024, Scimone also discussed:

- Upskilling the security workforce to adapt to the AI-driven landscape;
- The significance of understanding basic security principles before integrating AI into business operations;
- Dell's initiatives in promoting AI safety and security.

[WATCH ONLINE](#)

“You want to make sure that you're creating more good with the technology than potential harm. Both of those things need to be weighed - the potential business value and the organizational outcomes that you're going to achieve.”

- *John Scimone*



TECHNOLOGY AND SERVICES EXPERTS

MANAGED SERVICES

Organizations Hard-Pressed to Run Multiple Security Tools

Curt Aubley, COO, Deepwatch, on Maximizing Cybersecurity Tool Effectiveness



Organizations onboard multiple security solutions to meet their specific needs, such as securing cloud workloads or protecting identities, but many organizations lack the personnel or the training required to maximize the use of such tools, says Curt Aubley, COO and chief product officer, Deepwatch.

[WATCH ONLINE](#)

State of Security: Are We Moving Forward or Standing Still?

Edna Conway and **Wendy Nather** Discuss Cybersecurity's Past, Present and Future



Edna Conway, CEO, EMC Advisors, and Wendy Nather, director, strategic engagements, Cisco, discuss the persistent challenges and evolving dynamics in cybersecurity. They emphasize the importance of historical awareness, effective information sharing and leveraging AI for predictive risk management.

[WATCH ONLINE](#) **CEO/Founder**

The Cyber Risks for Businesses in an Election Year

Expel CEO **Dave Merkel** on How Companies Encounter Geopolitical Risks



As geopolitical tensions rise, businesses across the U.S. find themselves in the crosshairs of international cyber conflicts. The blending of global conflicts into cyberthreats is becoming a reality for companies far removed from the political sphere, said Dave Merkel, CEO of Expel.

WATCH ONLINE

CEO/Founder

Make Zero Trust Happen

Lieuwe Jan Koning, Co-Founder and CTO, ON2IT Dispels Zero Trust Misconceptions



Some organizations start out thinking that it's too challenging to embrace zero trust security or that it is a one-and-done strategy. But taking a slow and steady approach at the beginning can really help in realizing the much wider critical value, said Lieuwe Jan Koning, co-founder and CTO, ON2IT.

WATCH ONLINE

CEO/Founder

The Cost of Cybersecurity in Digital Payments Space

Dharshan Shanthamurthy on Security, Compliance and Growth in Digital Payments



The digital payment landscape is undergoing transformative growth, with cybersecurity at its core. Dharshan Shanthamurthy, CEO at SISA, discussed the urgency of addressing cybersecurity in an industry that is not only lucrative for businesses but also for motivated criminal gangs.

WATCH ONLINE

CEO/Founder



TECHNOLOGY AND SERVICES EXPERTS

RISK MANAGEMENT

At-Bay: InsurSec Can Bridge SMB Cybersecurity Gap

Thom Dekens Says InsurSec Is a Cost-Effective Solution for Better Security Outcomes



Small to mid-sized businesses face many cybersecurity challenges, often compounded by limited budgets and resources. Traditional cybersecurity providers also struggle to meet the specific needs of SMBs, failing to offer cost-effective solutions tailored to their requirements, according to Thom Dekens of At-Bay Security.

WATCH ONLINE

Human-Powered Security in the Era of Rapid Automation

HackerOne's **Mickos** on Human-Centric Cybersecurity for Responsible AI Adoption



HackerOne CEO Marten Mickos discussed assessing the risks associated with generative AI and the role of red teaming exercises and bug bounty programs in securing AI implementations. "AI is good, but only when the human is the steward and governing it," he said.

WATCH ONLINE

CEO/Founder

The Operationalization of Threat Intelligence Programs

Intel 471 CEO **Jason Passwaters** on Out-of-the-Box Approach to Threat Intel Programs



In the early days of threat intelligence, organizations were primarily consuming reports and linking things together. But now more entities are moving toward "operationalization out-of-the-box" for their threat intelligence programs, said Passwaters, CEO of Intel 471.

WATCH ONLINE

CEO/Founder

Applying Human Risk Management for Better Security Awareness

Ashley Rose, Founder and CEO of Living Security, on Targeted Awareness Training



Creating and understanding risk profiles for individual users in an organization can help optimize the effectiveness of security awareness training, which is just one tool under the wider umbrella of human risk management, said Ashley Rose, founder and CEO of Living Security.

WATCH ONLINE

CEO/Founder

AI-Driven Cyberthreats and Remote Work Challenges

ZeroFox CEO **James Foster** on Generative AI Security Risks and Proactive Cybersecurity



"The generative AIs and specifically the ChatGPTs of the world have made it really easy for adversaries to be really good at [cyberattacks]," said James Foster, founder and CEO of ZeroFox. "So, you have to do it differently. We've taken the approach to go after the adversary."

WATCH ONLINE

CEO/Founder

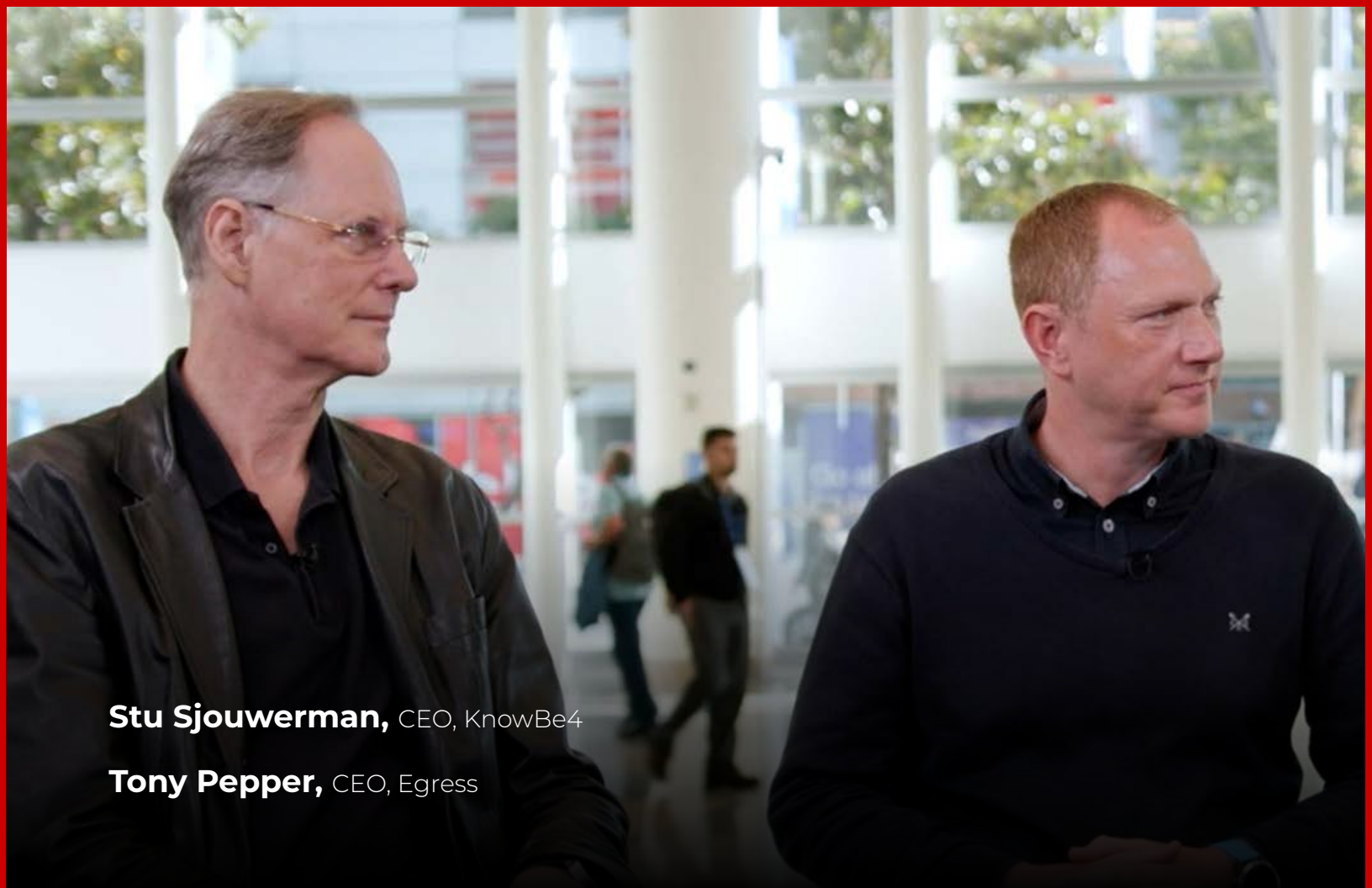
Cybersecurity Integration a Must, Post-M&A Imperative

Robert Booker Highlights Key Cybersecurity Practices During Mergers



Cybersecurity is no longer a secondary consideration in healthcare M&A. Robert Booker, chief strategy officer at HITRUST, emphasized the importance of thinking about third-party risks and system integration to safeguard sensitive information during and after M&A activities.

WATCH ONLINE



Stu Sjouerman, CEO, KnowBe4

Tony Pepper, CEO, Egress

Inside KnowBe4's Acquisition of Egress

KnowBe4's **Sjouerman** and Egress' **Pepper** on Integrated Solutions for Email Security

In a strategic move aimed at addressing evolving cybersecurity challenges, KnowBe4, a leading provider of security awareness training, has recently announced its acquisition of Egress, a specialist in email security solutions.

In this video interview with Information Security Media Group at RSA Conference 2024, Sjouerman and Pepper also discussed:

- How the integration enables personalized training and education for users based on real-life telemetry data;
- The road map for fully integrating Egress into KnowBe4;
- The role of AI-driven technologies in addressing behavioral-based attacks.

“AI needs data. Data needs AI. So, with the two together, it is much more empowering to the user to get them to a point where you can create a strong security culture.”

- **Stu Sjouerman**

WATCH ONLINE **CEO/Founder**

Double-Click on Risk-Based Cybersecurity

Niloofar Razi Howe, Pondurance, on Technology-Based vs. Risk-Based Cyber Defense



In today's cybersecurity landscape, where threats such as ransomware evolve rapidly, organizations must shift their approach to cybersecurity from technology-based to risk-based, said Niloofar Razi Howe, chair of the board, Pondurance.

[WATCH ONLINE](#)

Why Cyberthreats in Ad Tech Mirror Traditional Enterprises

Stu Solomon, CEO, HUMAN, on Shared Challenges Across Diverse Cyber Landscapes



While threat actors and environments may differ, the volume and scale of digital interactions in advertising tech and enterprises create challenges in detecting and mitigating threats, said Stu Solomon, CEO, HUMAN. He discusses the need to address privacy concerns amid the evolving threat landscape.

[WATCH ONLINE](#)

CEO/Founder

Assess the Security of Code in All Supply Chain Components

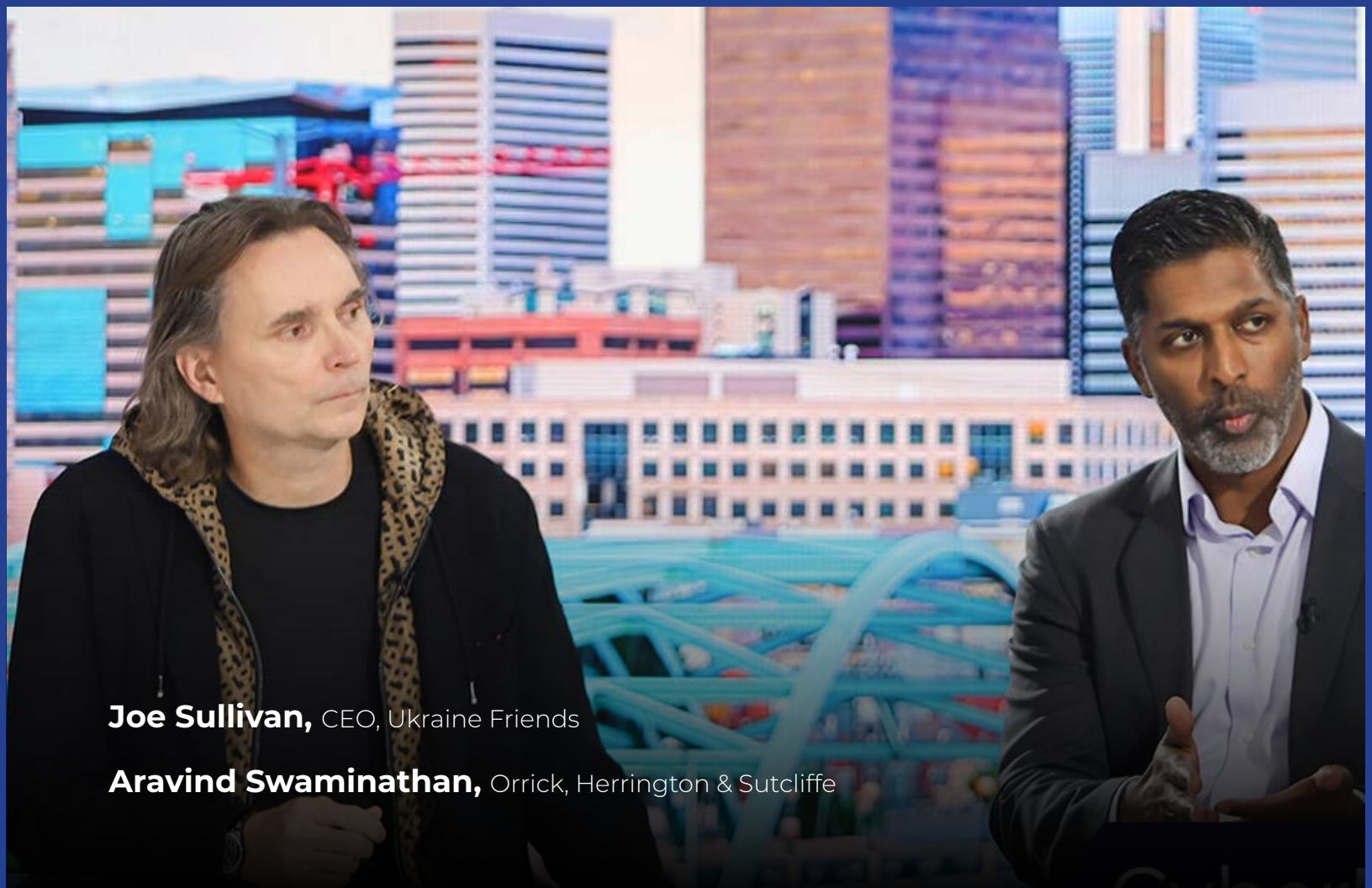
Alex Bazhaniuk of Eclipsium on Strategies for Strengthening Supply Chain Security



A piece of infrastructure, such as a laptop, contains components from hundreds of vendors, and even the smallest vendor presents a risk. That's why it is important to assess the security of code for all components to ensure supply chain security, said Alex Bazhaniuk, CTO and co-founder, Eclipsium.

[WATCH ONLINE](#)

CEO/Founder



Joe Sullivan, CEO, Ukraine Friends

Aravind Swaminathan, Orrick, Herrington & Sutcliffe

CyberEdBoard Talks: Balancing Security and Compliance

Expert Panel Unpacks Evolving CISO Responsibilities in Today's Regulatory Setting

CISOs face increasing legal and compliance responsibilities amid growing cybersecurity challenges. Ex-CSO Joe Sullivan of Ukraine Friends and Aravind Swaminathan of Orrick, Herrington & Sutcliffe discuss the need for fundamental processes and constant communication with stakeholders.

In this video interview with Information Security Media Group as part of the CyberEdBoard's ongoing CyberEdBoard Talks series, recorded at RSA Conference 2024, Sullivan and Swaminathan also discussed:

- The impact of the evolving regulatory landscape;
- Balancing security responsibility with legal compliance;
- Community collaboration among CISOs;

“Security, simply put, is hard. Cybersecurity is constantly evolving. The threats are constantly evolving. The technology we're trying to secure is constantly evolving.”

- **Joe Sullivan**

WATCH ONLINE

CyberEdBoard | Member



TECHNOLOGY AND SERVICES EXPERTS

SECURE ACCESS & IDENTITY MANAGEMENT

Rolling Out the Passwordless Future

1Password CEO **Jeff Shiner** Discusses When, Why and How to Adopt Passkeys



Humans continue to reuse simple passwords that criminals can access, and passwordless continues to be the way forward. Jeff Shiner, CEO of 1Password, said we're making progress toward the future of authentication - passkeys.

WATCH ONLINE

CEO/Founder

The Role of Identity in Network Security

Cisco's **Tom Gillis** on the Latest Security Trends and Challenges



It's a familiar pattern: A new threat appears on the horizon, organizations get hacked and teams of security vendors offer new security tools to defend the enterprise. Over time, many security organizations have acquired hundreds of tools, and instead of being more secure, detection and analysis across a broad spectrum of solutions is even harder.

WATCH ONLINE

Embracing a Unified Identity-Centered Zero Trust Approach

Clay Rogers of CyberArk, Amit Chhikara of Deloitte Discuss Critical Considerations

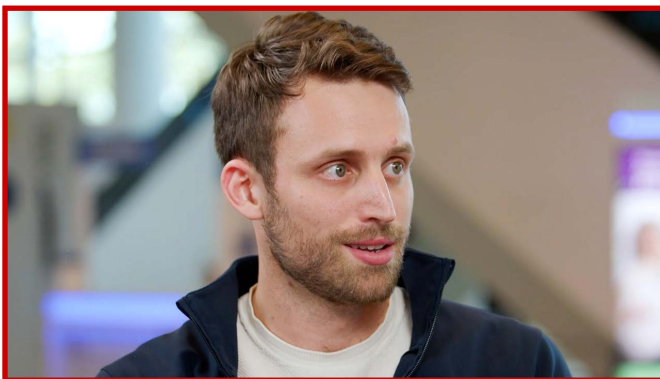


With the ever-evolving threat landscape overlaid onto the continuous digital transformation underway at so many organizations across all sectors, a unified identity-centered zero trust security approach has never been more important, said Clay Rogers of CyberArk and Amit Chhikara of Deloitte.

WATCH ONLINE

Nonhuman Identity Management Revolution

Oasis Security CEO **Danny Brickman** on NHI Evolution, Risks and Defenses



Over the past year, the threat posed by nonhuman identities, or NHIs, has evolved significantly. NHIs encompass a broad spectrum of entities, including automation tools, AI agents and cloud applications that authenticate differently from traditional human identities, such as usernames and passwords, said Danny Brickman, co-founder and CEO, Oasis Security.

WATCH ONLINE

CEO/Founder

The Growing Threat of Advanced Ransomware Attacks

Mandiant's **Charles Carmakal** Discusses the Growing Threat of Advanced Ransomware



The ever-changing and constantly present threat of ransomware has become more sophisticated thanks in part to emerging technologies such as artificial intelligence. Cybercriminals have also evolved their attack methods, using advanced tactics to exploit zero-day vulnerabilities and focusing on vulnerable network edge devices.

WATCH ONLINE

Rising Cybersecurity Threats: Focus on Identity Protection

Okta's CSO Discusses Threat Landscape Changes, AI's Impact on Identity



David Bradbury, chief security officer at Okta, discusses the shift in the cyberthreat battleground, the effect of artificial intelligence technology on identity protection, Okta's investments into its own security and lessons learned along the way.

WATCH ONLINE



Data
Prevention. Response.

Brandon Traffanstedt, Senior Director, Field Technology Office, CyberArk

Sunil Patel, Managing Director, Accenture

Matt Girdharry, WW Leader for Observability Security Partnerships, AWS

Why the Future of Security Is Identity

Experts Discuss Rise in Advanced Cyberattacks and Rapidly Changing Threat Landscape

The proliferation of identities, combined with cloud migration and the growing sophistication of attacks, has created the perfect storm for security teams. But as the number of identities grows, "you can do more with less," said Sunil Patel of Accenture Security, Matt Girdharry of AWS and Brandon Traffanstedt of CyberArk.

In this video interview with Information Security Media Group at RSA Conference 2024, Patel, Girdharry and Traffenstedt also discussed:

- How attackers have changed their tactics - logging in, rather than hacking in;
- How enterprises are using generative AI in their identity security programs;
- The rise in the types of identities and the need for every identity to access data across disparate resources.

[WATCH ONLINE](#)

“We tend to take all of these new identities and all of these new environments, and we begin to try and secure them in the same way. And we may not distinguish between a green Skittle or a purple Skittle.”

- **Brandon Traffanstedt**

A portrait of Mark McClain, an older man with white hair, wearing a dark suit jacket over a light-colored collared shirt. He is smiling slightly and looking directly at the camera.

Mark McClain

Founder & CEO, SailPoint

Facing the Complexity of Unified Identity, Third-Party Risk

SailPoint CEO **Mark McClain** Discusses Identity Security Challenges

In the identity security market, mid- to large-scale enterprises often grapple with understanding who has access to what within their IT environments. Mark McClain, CEO of SailPoint, said that traditional perimeter-based security has expanded, so security teams need to understand access in a world of mobile and cloud computing.

In this video interview with Information Security Media Group at RSA Conference 2024, McClain also discussed:

- The difference between converged identity and unified identity;
- The significance of regulatory governance in critical sectors such as healthcare;
- Emerging threats associated with nonemployee and nonhuman identities.

WATCH ONLINE

CEO/Founder

“The most notable thing we're seeing - and we're certainly hearing this from so many of our customers - is: They are still wrestling deeply with the threats against their own employees and the identities that they think they know well - the people that work for them, that get paid by them.”

- **Mark McClain**

Why AI Is the Best Defense Against AI-Enabled Fraud Attacks

Christophe Van de Weyer, CEO, Telesign, on Fighting AI With AI



Artificial intelligence has enabled cybercriminals to refine their tactics and modify fraud and cyberattack tools, but the same technology now presents itself as the best defense against automated cyberattacks in various forms, said Christophe Van de Weyer, CEO, Telesign.

WATCH ONLINE

CEO/Founder

How SASE Is Evolving as the Workforce Remains Remote

David Batty of iboss on Keeping User Traffic Safe



The need for SASE is growing as more and more organizations realize that the majority of their workforce will remain remote and there is no longer a "safe network" within a building but rather "all networks become an external network," said David Batty, vice president of solution architecture and technology at iboss.

WATCH ONLINE

SMBs Now See Privileged Access Management Working for Them

Maurice Côté of Devolutions on Bridging the Gap Between Enterprises and SMBs



Cybersecurity companies initially designed privileged access management as a concept with large enterprise customers in mind, but the technology is beginning to work for smaller businesses, said Maurice Côté, vice president, products, Devolutions.

WATCH ONLINE



TECHNOLOGY AND SERVICES EXPERTS

SECURITY OPERATIONS

Transforming Your Cyber Defense Strategies With AI

Nayaki Nayyar of Securonix on AI's Dual Impact on Cybersecurity



As businesses increasingly integrate artificial intelligence into their cybersecurity strategies, they encounter a double-edged sword. At the World Economic Forum this year, more than 55% of respondents believed attackers benefit more from AI, which is alarming, said Nayaki Nayyar, CEO of Securonix.

WATCH ONLINE

CEO/Founder

Threat Versus Risk: Rethinking Cybersecurity Fundamentals

Splunk's Anthony Pierce on Cybersecurity Strategies Beyond Threat Management



Cybersecurity strategies often focus primarily on threat response, which only solves part of the problem. To effectively implement threat identification and risk management, companies should first distinguish between threat and risk.

WATCH ONLINE



Bruce Johnson, Senior Director, Enterprise Security, TekStream

Mary Lou Prevost, Group Vice President, U.S., SLED, Splunk

Public-Private Partnership Puts College Students in SOCs

TekStream's **Johnson** and Splunk's **Prevost** on Tapping Into Student Talent for the SOC

The threat landscape has evolved for state and local government entities as well as higher education institutes. Mary Lou Prevost from Splunk and Bruce Johnson of TekStream discuss innovative public-private partnerships that boost institutional defense mechanisms.

In this video interview with Information Security Media Group at RSA Conference 2024, Prevost and Johnson also discussed:

- Unique cybersecurity challenges faced by different educational institutions;
- How a student-powered SOC at LSU has improved detection and response - and alleviated workforce challenges - in a program that uses student talent in operational security roles who collaborate with technology providers and state and local governments;
- How a shared SOC model can scale.

[WATCH ONLINE](#)

“They don't have this elaborate budget to hire all the people that they would like to hire. So as soon as they have invested a year or three into an individual, they are plucked off by the private sector because they can pay more.”

- **Mary Lou Prevost**



TECHNOLOGY AND SERVICES EXPERTS

THREAT DETECTION & RESPONSE

Lessons From Change Healthcare and System Interoperability

Huntress CEO **Kyle Hanslovan** on Implications of Healthcare Industry's Biggest Hack



U.S. healthcare interoperability - across doctors, dentists, other healthcare providers and vendors that support them - brings new opportunities for hackers to monetize disruption of badly needed services, said Kyle Hanslovan, CEO, Huntress.

[WATCH ONLINE](#) **CEO/Founder**

Make Way for the Intelligent SOC

Will Gragido of NetWitness on the SOC's Evolution From Traditional to Intelligent



Traditional SOC's, overwhelmed by the sheer volume of data and alerts, are making way for the intelligent SOC. Will Gragido, head of product management and intelligence, NetWitness, explores this "enriched contextual value that's highly actionable and drives decisions in a confident fashion."

[WATCH ONLINE](#)

Overcoming Frustration With Network Security

Phil Owens of Stamus Networks Explores the Shift in Network Security



The network security landscape is undergoing a significant transformation. Phil Owens, vice president of customer solutions at Stamus Networks, shared insights on how the need for transparency is reshaping client experiences and expectations in cybersecurity. This strategic shift focuses on minimizing noise and maximizing clarity for security operations center analysts.

[WATCH ONLINE](#)

Not Just MOVEit: 2023 Was a Banner Year for Zero-Days

Verizon Data Breach Investigations Report Author Details Online Criminal Trends



If there's one data breach trend that stands out, it's hackers' vigorous focus on finding zero-day or recently patched flaws and exploiting them through automated scanning. "There are people scanning the whole wide internet," said Alex Pinto, senior manager, Verizon Threat Research Advisory Center.

[WATCH ONLINE](#)



TECHNOLOGY AND SERVICES EXPERTS

OT/IOT SECURITY

SEC Regulations Demand Greater Transparency in OT Security

Capdevielle of Nozomi Networks on CISO-Board Dynamics and Cybersecurity Governance



Amid new SEC disclosure regulations, CISOs have transitioned to more active roles in engaging company boards, redefining the dynamics of cybersecurity governance. These regulations require organizations to report cybersecurity incidents and state their cybersecurity posture, said Edgard Capdevielle, president and CEO, Nozomi Networks.

WATCH ONLINE

CEO/Founder

Building Your OT Security Business Case

Rick Kaun Shares Strategic Paths for Advanced Operational Security



Despite the persistent threats and complexities in the OT world, it's tough for security practitioners to define a clear business case. Rick Kaun, vice president of solutions at Verve Industrial Protection, a Rockwell Automation Company, emphasized the nuanced approach required for building effective security frameworks.

WATCH ONLINE



Theresa Lanowitz, Head of Cybersecurity Evangelism, AT&T Cybersecurity

Focusing on Cyber Resilience, Not Just Security

Theresa Lanowitz of AT&T/LevelBlue on the Overlooked Benefits of Cyber Resilience

There is a big difference between cyber resilience and security, even though the challenges across industries are almost the same. AT&T's LevelBlue Futures Report: Beyond the Barriers to Cyber Resilience is designed to help cyber stakeholders understand these differences and make more effective cyber resilience decisions, said Theresa Lanowitz, chief evangelist, AT&T Cybersecurity/LevelBlue.

In this video interview with Information Security Media Group at RSA Conference 2024, Lanowitz, discussed:

- Highlights from the LevelBlue Futures Report: Beyond the Barriers to Cyber Resilience;
- Overcoming the barriers to improving cyber resilience;
- Threats to organizational resilience.

[WATCH ONLINE](#)

“It is not just about cybersecurity controls that we are implementing. It is really about understanding what we are going to do to make business resilient.”

- Theresa Lanowitz



Dawn Cappelli, Head of OT-CERT, Dragos

The OT Security Revolution and the Need for Robust Defenses

Dawn Cappelli, Head of OT-CERT at Dragos, on Emerging Threats to OT Environments

In the wake of geopolitical tensions, nation-state threats have "crossed the line more often than they ever have," said Dawn Cappelli, head of OT-CERT at Dragos, warning of the growing threat to critical infrastructure and emerging challenges for small and medium-sized enterprises, SMEs.

In this video interview with Information Security Media Group at RSA Conference 2024, Cappelli also discussed:

- How the OT cyberthreat environment has changed in the past year;
- Dragos OT-CERT's Community Defense Program;
- Strategies for SMEs to enhance their security posture.

[WATCH ONLINE](#)

"Just recently, different types of cyberthreats are hitting the small and medium organizations."

- **Dawn Cappelli**



Robert M. Lee, CEO, Dragos

Effective Operational Technology Security? Embrace Response

Critical Infrastructure Over-Focuses on Prevention, Says Dragos'
Robert M. Lee

An uptick in the tempo of attacks targeting operational technology networks means the industry must improve its ability to respond to such attacks, said Robert M. Lee, CEO and co-founder of industrial cybersecurity firm Dragos.

In this video interview with Information Security Media Group at RSA Conference 2024, Lee also discussed:

- How the risk management discussion is changing as CEOs and boards sharpen their focus on OT cybersecurity and risk;
- Best practices for prioritizing vulnerability management in OT environments;
- How a medium-size organization repelled a nearly yearlong effort by the China-linked Volt Typhoon APT group to pivot from its IT to OT network, thanks to doing the basics.

“We try to help people identify the 2% to 3% of vulnerabilities that actually matter because that's about all it is: Here are the corrections and mitigation guidance you need.”

- **Robert M. Lee**

WATCH ONLINE

CEO/Founder



“It has become a number one or number two topic at the board level, and we see a lot more executives saying, 'This has got to get solved. What do you need?' And that's driving a much more mature conversation.”

Robert M. Lee

CEO, Dragos



May Wang, CTO, Internet of Things Security, Palo Alto Networks

AI and IoT Synergy for Enhancing Cybersecurity

Palo Alto Networks CTO **May Wang** on Need for Precision AI to Detect Threats

Artificial intelligence and the internet of things have complementary features, and when used together they can strengthen IoT security. With the widespread use of IoT devices today, the stakes are high if these devices are compromised. IoT devices are different from IT devices but AI can address IoT security challenges, said May Wang, CTO of IoT security at Palo Alto Networks.

In this video interview with Information Security Media Group at RSA Conference 2024, Wang also discussed:

- Integrating AI and ML to improve threat detection;
- The challenges in protecting IoT devices;
- Using precision AI to accurately detect threats.

[WATCH ONLINE](#)

“Even 0.001 inaccuracy can cause disaster. That's why we are promoting precision AI, especially for cybersecurity. We need extreme accuracy to make cybersecurity work.”

- *May Wang*

Critical Infrastructure Under Cyber Siege: How to Respond

Brad Brooks Shares Insights About Heightened Threats to Evolving Defenses



The alarming reality of heightened cyberthreats extends from vulnerable home office routers all the way to essential water supply systems, warned Brad Brooks, CEO at Censys, who explained the intricate web of cyber risks entangling critical infrastructure.

[WATCH ONLINE](#)

CEO/Founder

Challenges in Adopting Post-Quantum Cryptography

Riscure's **Marc Witteman** on the Need for Quantum-Resistant Cryptographic Algorithms



Quantum computing poses a significant threat to existing public key cryptographic algorithms such as RSA, potentially rendering them obsolete. As the threat landscape grows exponentially with new developments in quantum computers' capabilities, cryptographic standards that can withstand quantum disruptions have become critical.

[WATCH ONLINE](#)

CEO/Founder

● REC

00:00:01:00

1H 20M

iSMG



4K HD 1080

iSMG
Studio

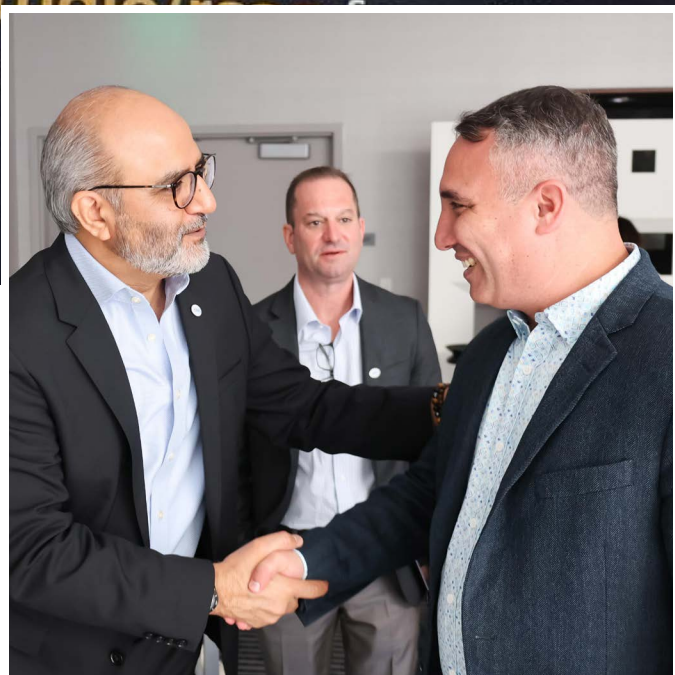
MENU III

Behind the Scenes

Information Security Media Group, the largest media sponsor team at RSA Conference, conducted video interviews with top leaders in information security, risk management and privacy. Here's a look at the team behind the scenes.



Ukraine Friends CEO and CyberEdBoard member Joe Sullivan prepares for an interview with ISMG's Anna Delaney.



ISMG CEO Sanja Kalra greets HUMAN CEO Stu Solomon.



ISMG CEO Sanjay Kalra, NightDragon CEO Dave DeWalt and David Elichman, chief collaboration officer, ISMG



ISMG's global brands encompass world-class events, programs and services focused on helping organizations gain cybersecurity insights.

Anna Delaney, ISMG director of productions, behind the scenes





Carnegie Mellon's Clarence Worrell with ISMG's Rahul Neel Mani at the Marriott news desk



ISMG CEO Sanja Kalra with CyberEdBoard members Grant Schneider, Tiauna Ross and Jerry Cochran





ISMG CEO Sanjay Kalra, ISMG's Michael Novinson and SailPoint CEO Mark McClain



The ISMG Editors' Panel - Mathew Schwartz, Tom Field, Anna Delaney, Rahul Neel Mani and Michael Novinson - toasts the final day of RSA.



ISMG's Varun Haran and Sanjay Kalra with Matt Girdharry of AWS and friends from Payatu.



Cato Networks CEO Shlomo Kramer, left, chats with ISMG CEO Sanjay Kalra

Datta Junnarkar, CIO of Maritime at Boeing, prepares for an interview.



Above, Elastic's Mike Nichols in an interview with ISMG's Tom Field, senior vice president, editorial

ISMG General Manager Mike D'Agostino, Photographer Victoria Webb, ISMG CEO Sanjay Kalra and ISMG Chief Collaboration Officer David Elichman



Right: Zscaler CEO Jay Chaudhry at the news desk



Right: panelists Piyush Malik, Sarfraz Nawaz and Harnath Babu





ISMG.Studio,
the leading
platform for
cybersecurity
and
technology
leaders



ISMG's video
production team
recorded 150
interviews across
two studios.



See you at RSA Conference 2025!



The on-location ISMG team comes together at the end of the conference for one last photo.

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

