



RSA[®]Conference2022

Highlights and Insights

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

RSA Conference 2022: Transform, Indeed



The theme of RSA Conference 2022 was "Transform," and I see it breaking down into three sub-themes:

- "We're Back!" — After our COVID skip year, RSA Conference resumed live sessions and showroom for the first time since 2020.
- "New and Improved!" — No one was talking about SBOMs and SSE two years ago, as they were this year. And discussion of cyberwarfare was more theoretical, as opposed to being part of the daily news.
- "Everything Old Is New Again" — Zero trust, anyone? Application security? Supply chain risk? They are all well-mined topics given new urgency by ransomware, Log4j, Colonial Pipeline and all the headline-making attacks we've seen over the past year.

Even the RSA Conference itself embraced each of these themes. This was the 31st annual RSA Conference, and it was held in its familiar San Francisco home. Yet, the event itself is no longer affiliated with the RSA security company. It's been spun off into independence to pursue its own version of "Transform."

As for ISMG's presence at RSA ... well, we embraced a bit of transformation ourselves. Back as the event's largest media sponsor, we again staffed two distinct video studios at the conference, and we produced more than 150 individual interviews. CEOs, CISOs, analysts, researchers, government leaders — the entire RSA Conference constituency is well represented in our suites of interviews, and you will see them in this publication.

Beyond the interviews, we hosted receptions, briefings, roundtable discussions — we created community within the RSA Conference 2022 community, and those unique events are commemorated here as well.

There is no substitute for attending RSA Conference. But what if you couldn't be there? Or you just wish you'd taken better notes? Let us help. Here. Now. Enjoy!

Best,

A handwritten signature in black ink, appearing to read 'Tom Field', with a stylized flourish at the end.

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

Visit us online for more RSA coverage:

www.databreachtoday.com/rsa-conference



Video Interviews

CEO/Founder Perspective

J. Michael Daniel	4
Jeff Hudson	4
Erwän Keräudy & Jeff Gore	5
Greg Murphy	5
Glenn Chisholm	5
Amit Bareket & Gilley Netzer	5
Wade Baker	7
Stephen Boyer	7
Oz Golan	7
Anton Kruezer	7
Ritesh Agrawal	8
Oz Alashe	8
Michael Assraf	8
Denny LeCompte	8
Art Coviello	9
Rohit Ghai	10
Phillip Reitingner	11
Chris Pierson	11
Brian Dye	11
Diana Kelley	11
Alberto Yépez	12
Mike DeCesare	13
Bryan Ware	14
Aleksandr Yampolskiy	14
Mariano Nunez	14
Regina Phelps	14
Joe Payne	15
Don Pezet	16
Jay Chaudhry	17
Kelly White	18
Ami Luttwak	19
Denise Anderson.....	20

CISO Perspective

Michael Baker.....	21
Glauco Sampaio	21
Fernando Madueira	22
Andre Gomes	22
Helen Patton.....	22
Bernardo Vasquez	22
Dave Stapleton	23
Ankit Patel	23
Jonathan Trull	23

John McClure	23
Michael Cunningham	24
Rich Lindberg	25
Jeff Farinich	26
Milton Almeida	26
Eric Sanchez	26
Rob Hornbuckle.....	26
Nick Coleman	28
Patricia Titus	29
Chris Holden.....	30
Kevin Li & Rocco Grillo	31
Vishal Salvi	32

Government Perspective

Grant Schneider.....	33
Jeremy Grant	33
Lester Godsey	35
Lieutenant Colonel Kurt Sanger.....	36
Kiersten Todt.....	36
Roger Sels	36
Sean Frazier.....	36
Elvis Chan	38
Stephen Dougherty	38
Eric Swalwell	38

Focus on Zero Trust

Abbas Kudrati & Upendra Singh	39
Lionel Jacobs Jr.	39
John Kindervag.....	40
Joe Sullivan	42
Paul Martini	42
Kate Adam.....	42
Jeetu Patel	42
Nikesh Arora.....	43

Focus on OT Security

John Maddison	45
Mex Martinot.....	45
Dawn Cappelli.....	47
Itai Greenberg	48
Lesley Carhart.....	48
Mark Cristiano	48
Wael Mohamed	49
Grant Geyer	50

Focus on Cybercrime/Nation State

Troy Leach	51
Chet Wisniewski	51
Jon DiMaggio	52
Raj Samani	52
Marc Rogers.....	52
Steve Rivers	52
Payal Chakravarty	54
Vitali Kremez.....	54
Allan Liska	54
Steven Teppeler.....	54
Jackie Burns Koven	55
John Fokker	56
Derek Manky	56
Matt Aldridge.....	56
Kimberly Grauer.....	56
Troy Leach & John Kindervag.....	57
Joseph Carson.....	59
Wesley Mullins	59
Roger Grimes.....	59
AJ Nash.....	59
Kal De	60
Ian Gray	61
Chad Sweet	62
Mikko Hypponen	64

Cybersecurity Perspectives

Crane Hassold.....	65
Jessica Hetrick.....	65
Mike Kiser.....	66
Daniele Catteddu.....	66
Richard Bird	66
Mark Brown.....	66
Chase Cunningham.....	67
Robin Andruss.....	68
Ronald Raether	68
Randy Trzeciak.....	68
Merritt Maxim & Paul McKay	68
Marshall Heilman	69
Nick Warner	70
Wendi Whitmore	71

More Content

More Interviews	72
-----------------------	----

Behind the Scenes: ISMG at RSAC 2022	75
--	----

CEO/Founder Perspective

How does a good idea go from a concept to a working product that's providing security services to thousands of people? The CEO/founders in the cybersecurity industry have led countless efforts to build companies from scratch and introduce innovation at scale. We spoke to some of the most well-known and influential leaders in the industry today to find out how they got here and where they're headed.

Cyber Threat Alliance at 5: Information Sharing Expands

J. Michael Daniel on the Pace and Depth of Threat Intel Sharing



The Cyber Threat Alliance – a nonprofit organization that improves the cybersecurity of the global digital ecosystem by enabling high-quality cyberthreat information sharing among cybersecurity providers – just celebrated its fifth birthday, and President and CEO J. Michael Daniel says the membership and information sharing both are growing at an impressive pace. He discusses the ransomware surge and how organizations should respond.

WATCH ONLINE

An 'Epochal Change' in Cybersecurity

Venafi's Jeff Hudson on Technology, Organizational Changes Reshaping Enterprises



From cloud migration to application development, cybersecurity is in the middle of an "epochal change," says Jeff Hudson, CEO of Venafi. He wants enterprise security leaders to envision the possibilities when security and development are in sync.

WATCH ONLINE

Assessing Threats Outside the Perimeter

CEO **Erwän Keräudy** and CRO **Jeff Gore** of CybelAngel Discuss Critical Considerations



Erwän Keräudy and Jeff Gore of CybelAngel say that due to cloud migration, people working remotely, and the connected ecosystem of suppliers, "the perimeter is dead." We need a comprehensive assessment of critical external threats, they say, including a scan of "the infrastructure of the internet."

[WATCH ONLINE](#)

Ransomware, Devices and the Impact in Healthcare

Ordr CEO **Greg Murphy** Addresses Key Threats to Critical Sector



Greg Murphy, CEO of Ordr, says there are three topics healthcare senior leaders and board members keep asking about: ransomware, ransomware ... and ransomware. He discusses how healthcare entities are addressing their biggest threats.

[WATCH ONLINE](#)

How Companies Can Defend a Rapidly Expanding SaaS Footprint

Obsidian Security CPO **Glenn Chisholm** on How to Safeguard SaaS and Cloud Services



The use of software-as-a-service applications has dramatically increased since the onset of the COVID-19 pandemic, and the changing consumption patterns have ushered in a new set of security challenges, according to Obsidian Security co-founder and chief product officer Glenn Chisholm.

[WATCH ONLINE](#)

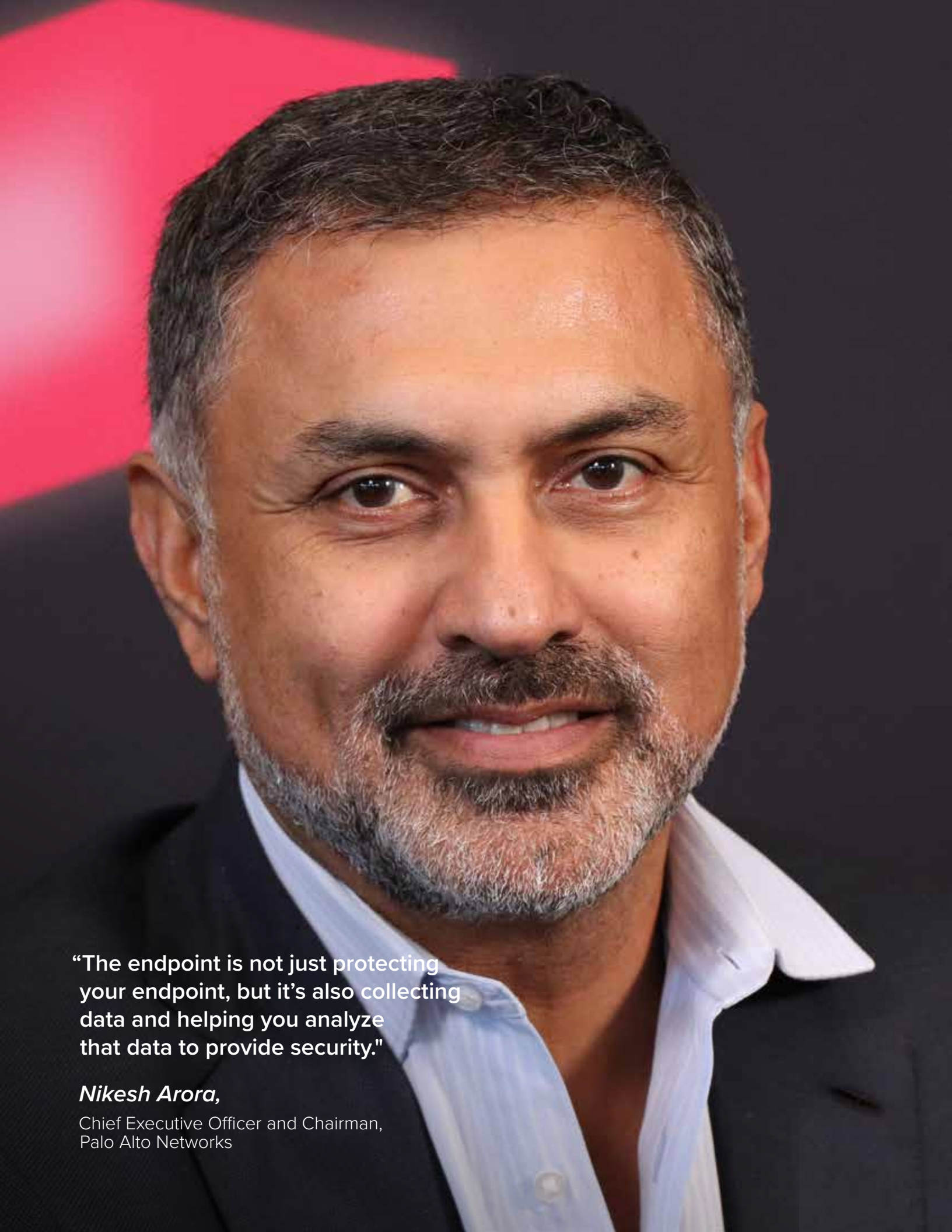
The Future of Corporate Network Security on the Internet

Perimeter 81 Leaders on Cloud-Based Next-Generation Secure Corporate Networks



With the increasing growth of remote working and the cloud, the internet is now the new corporate network, says Amit Bareket, co-founder and CEO of Perimeter 81. Bareket and company CMO Gily Netzer predict a rapid disruption in how organizations consume security as companies move from site-centric security tools to people-centric secure corporate networks over the internet.

[WATCH ONLINE](#)



“The endpoint is not just protecting your endpoint, but it’s also collecting data and helping you analyze that data to provide security.”

Nikesh Arora,

Chief Executive Officer and Chairman,
Palo Alto Networks

Mitigating the Impact of Ransomware With Data Science

Cyentia Institute Partner **Wade Baker** Shares Insights on Analyzing Ransomware Data



Cybersecurity organizations are sitting on a treasure trove of data about ransomware attacks. Unlocking that data and analyzing it can help security teams become more prepared for future attacks, says Wade Baker, partner at Cyentia Institute.

WATCH ONLINE

Cyber Risk Quantification: The Quest for Transparency

BitSight's **Stephen Boyer** Says Regulations Are Driving Better Board-Level Awareness



How can companies make their cybersecurity posture more transparent to stakeholders? That's a question being asked by both boards of directors and potential investors, says Stephen Boyer, founder and CTO of BitSight.

WATCH ONLINE

Why Adversaries Like Going After APIs – and How to Stop Them

Noname Security CEO **Oz Golan** on Defending One of the Hottest Attack



In the digitally transformed world, APIs suddenly are among the hottest attack vectors. Yet too many organizations fail to even have visibility into their API inventory, much less security. Oz Golan, CEO of Noname Security, discusses API security trends.

WATCH ONLINE

Zero Trust Strategy or Swiss Cheese Model?

Drivelock SE CEO **Anton Kreuzer** on the New Demands for Protecting Data – Anywhere, Anytime



The aftermath of digital transformation is that we produce more data than ever on more devices in more diverse locations. Now, how do we convey the urgency to protect this data during its whole life cycle? Drivelock SE CEO Anton Kreuzer addresses this challenge and more.

WATCH ONLINE

Bridging the Divide Between Digitization and Cybersecurity

Airgap CEO **Ritesh Agrawal** on Reducing On-Premises and Remote Work Security Friction



The job of securing corporate assets is getting harder as remote working has created two sets of tools, policies and personnel to manage remote and legacy cybersecurity, says Airgap Networks CEO and co-founder Ritesh Agrawal. The industry needs to adopt a better way to unify access control connectivity across the hybrid workforce, he says.

WATCH ONLINE

Why User Awareness Training Misses the Mark

Oz Alashe, CEO of CybSafe, Discusses New Approaches to Changing User Behavior



A great deal of awareness training has been offered to users – including phishing simulations – but none of it seems to have led to a significant change in their poor security behaviors and decision-making skills, says Oz Alashe, CEO of CybSafe.

WATCH ONLINE

The Speed of Vulnerability Remediation

Michael Assraf, CEO of Vicarius, on Enterprise IT Vulnerability Challenges



As enterprise IT infrastructures become more complex, the faster vulnerabilities can be identified – and especially remediated – the better, says Michael Assraf, CEO and co-founder of Vicarius.

WATCH ONLINE

Enterprise-Grade Cybersecurity for Midmarket Businesses

Portnox CEO **Denny LeCompte** on the Security Needs and Constraints in the Midmarket



Midmarket companies face many of the same cyberthreats as enterprises but have neither the budget nor the staffing of those larger organizations. Portnox CEO Denny LeCompte is attempting to ensure that the security needs of midmarket companies are at last fully addressed.

WATCH ONLINE



Art Coviello,
Partner,
Rally Ventures

Art Coviello on Market Trends, Emerging Tech

Former RSA CEO Offers Cybersecurity 'State of the Union'

Art Coviello, former CEO of RSA and current partner with Rally Ventures, describes the cybersecurity industry trends he's watching closely as we hit the midway point of 2022, as well as which emerging technologies have not quite evolved in the way he might have anticipated.

In a video interview with Information Security Media Group at RSA Conference 2022, Coviello also discusses:

- The state of the industry;
- Emerging technologies he's watching as an investor;
- How the Russia-Ukraine war has affected security strategies and programs.

“Given the lack of personnel for security operations centers, we see tremendous demand for managed security service providers.”

- Art Coviello

WATCH ONLINE



Rohit Ghai,
CEO,
RSA

RSA CEO Rohit Ghai: 'Disruptions Catalyze Transformation' Channel 'Disruptive Forces at Play' to Drive Essential Cybersecurity Changes

With the ongoing pandemic driving digital transformation and hybrid work, it's no surprise that the theme of this year's RSA Conference was "transform." Carrying forward that theme, RSA CEO Rohit Ghai says that channeling "disruptive forces at play" can be a powerful tool for driving needed changes.

In a video interview with Information Security Media Group at RSA Conference 2022, Ghai also discusses:

- How RSA Conference has transformed, becoming an independent and stand-alone business that is no longer part of the RSA security company;
- The RSA security company's new focus on being an identity business and spinning off its other competencies as stand-alone brands;
- The constants and imperatives that underlie transformation and the dogmas that must be debunked.

WATCH ONLINE

“The best piece of information about whether something is true or not is to know who created it and what's the reputation of the creator?”

- *Rohit Ghai*

How Can We Simplify Cyber Defense?

GCA President **Philip Reiting** on Tackling Complexity



The overlying problem in cybersecurity is scale and the complexity that comes from that scale, says Philip Reiting, president and CEO of the Global Cyber Alliance. He says we need to simplify how we defend ourselves and "give individuals and companies products that meet them where they are."

[WATCH ONLINE](#)

The Growing Need for Digital Executive Protection

BlackCloak CEO **Chris Pierson** on Huge Vulnerabilities Outside Traditional Workplace



Ransomware as a service, supply chain attacks, vulnerable personal devices and home IoT, and the Russia/Ukraine war – they are all factors behind the growing need for digital executive protection outside the traditional workplace. Chris Pierson of Blackcloak shares new research and insights.

[WATCH ONLINE](#)

Harnessing the Power of Open Source to Protect Networks

Corelight CEO **Brian Dye** on Why Network Visibility Is Challenging for Smaller Firms



Organizations face major challenges gaining visibility into networks that grow more complex by the day, and Corelight CEO Brian Dye says the open-source community can help with gathering evidence and insights from networks so that the perimeter is better secured.

[WATCH ONLINE](#)


Cybersecurity Ethics: Artificial Intelligence Imperatives

Machine-Learning Models Must Work for All, Warns Industry Veteran **Diana Kelley**



As a long-time industry veteran who's done everything from building and managing large enterprise networks to advising executives at some of the world's biggest technology giants, Diana Kelley continues to track some of the top trends and issues in cybersecurity.

[WATCH ONLINE](#)

A close-up portrait of Alberto Yépez, a middle-aged man with dark hair, wearing a dark blue suit jacket over a light blue shirt. He is looking slightly off-camera with a serious expression.

Alberto Yépez,
Co-Founder and Managing Director,
Forgepoint Capital

Alberto Yépez of Forgepoint Capital Shares 2022 Market View

2 Years Later, Which Threats Most Test the Cybersecurity Sector?

The world is a much different place since the previous in-person RSA Conference – and so is the cybersecurity marketplace. Alberto Yépez of Forgepoint Capital shares his view of the state of the industry and the market forces that may cause further change in 2022.


In a video interview with Information Security Media Group at RSA Conference 2022, Yépez discusses:

- How the market has evolved since 2020;
- Potential impacts of the Russia-Ukraine war;
- Emerging technologies and companies to watch.

“I think we're going to see real innovation and people trying to solve real problems and adapt to the current threat environment.”

- Alberto Yépez

WATCH ONLINE

A portrait of Mike DeCesare, CEO of Exabeam, against a dark blue background. He is a middle-aged man with light brown hair, wearing a dark blue button-down shirt. He is looking slightly to his right with a neutral expression.

Mike DeCesare,
CEO,
Exabeam

The Importance of Automated Cyberthreat Response

Mike DeCesare, CEO of Exabeam, Discusses Evolving XDR Trends

It's critical to enable companies to not only see what is going on in their IT environments, but to also quickly react, and "sheer manpower" is no longer sufficient to respond to the surge of cyberthreats evolving today, says Mike DeCesare, CEO of Exabeam.

In a video interview with Information Security Media Group at RSA Conference 2022, DeCesare also discusses:

- Taking an "open approach" to XDR;
- The importance of automated response;
- The biggest cybersecurity pain points for many organizations today.

"Companies will have to begin having their cybersecurity products just go and block things automatically on their own."

- *Mike DeCesare*

WATCH ONLINE

Using Cyberthreat Intelligence to Keep Ahead of Adversaries

Bryan Ware, CEO of LookingGlass Cyber Solutions, on Maximizing Insights



While adversaries are often still using many of the same old methods and exploits to compromise their victims, the exposure and consequences of these attacks are becoming increasingly damaging, says Bryan Ware, CEO of LookingGlass Cyber Solutions.

WATCH ONLINE

Why the Physical Russia-Ukraine War Might Become a Cyberwar

SecurityScorecard CEO Aleksandr Yampolskiy on Why This War Is Personal



The ongoing war between Russia and Ukraine isn't an abstract concern for SecurityScorecard CEO Aleksandr Yampolskiy but a deeply personal one since he grew up in Russia and rode the train to Ukraine each summer to visit his grandmother. Yampolskiy has since immigrated and is now a U.S. citizen, but his concern for the people of both countries remains.

WATCH ONLINE

The Importance of Business-Critical Application Security

Onapsis CEO Mariano Nunez on the Challenges Enterprises Face Securing Applications



Business-critical applications, the crown jewels of the modern enterprise, are increasingly targeted due to their significant value, and many organizations are struggling to secure them. These systems must be properly deployed, monitored and maintained, says Onapsis CEO Mariano Nunez.

WATCH ONLINE


COVID-19: The Latest Good and Bad News

Regina Phelps of EMS Solutions Describes Progress, New Risks and Potential Impact



There's good news and bad news regarding the current state of COVID-19 and its impact, says Regina Phelps, founder of Emergency Management and Safety Solutions Inc.

WATCH ONLINE



Joe Payne,
President & CEO,
Code42

The Biggest Security Threat to Company Data: Your Employees

Code42 CEO Joe Payne on How Employers Can Thwart Data Theft by Departing Employees

The "Great Resignation" over the past year has created a host of concerns around both malicious and accidental data theft, says Code42 President and CEO Joe Payne. Even though employees often aren't looking to wreak havoc on their way out, a lack of understanding can lead to serious headaches.

In a video interview with Information Security Media Group at RSA Conference 2022, Payne discusses:

- The most common ways employees cause data breaches;
- How employers can determine if a leak was malicious;
- The differences between insider risk and insider threat.

“We know from Code42 research that when people work from home, they have really poor security habits.”

- Joe Payne

WATCH ONLINE



Don Pezet,
Co-Founder and "Edutainer,"
ITProTV

Cybersecurity Education: The Imperative to Rethink Delivery

Don Pezet of ITProTV on How to Best Address the Gaps in Today's Approaches

Many people enter the cybersecurity field with foundational skills, such as knowledge gleaned from college courses, and giving them "practical skills, to be ready go out on the job floor and be ready to do something – that takes a little bit of something extra," says ITProTV "edutainer" and co-founder Don Pezet.

In a video interview with Information Security Media Group at RSA Conference 2022, Pezet also discusses:

- Gaps he sees in current approaches to cybersecurity education;
- How to change the way cybersecurity education gets delivered today;
- What ITProTV is doing to help.

"There's the challenge of keeping things relevant and current; cybersecurity changes so fast, it's ridiculous."

- Don Pezet

WATCH ONLINE



Jay Chaudhry,
Founder, Chairman and CEO,
Zscaler

How to Distinguish True Zero Trust From Imposters

Zscaler CEO Jay Chaudhry on Why Firewalls and VPN Don't Belong in Zero Trust Design

There's a lot of confusion in the market around what constitutes zero trust architecture, and Zscaler founder, Chairman and CEO Jay Chaudhry believes firewalls and VPNs shouldn't be part of a system that's not supposed to trust anybody or anything by default.

In a video interview with Information Security Media Group at RSA Conference 2022, Chaudhry also discusses:

- How next-gen zero trust can be distinguished from legacy systems;
- Why firewalls and VPNs don't belong in zero trust designs;
- Opportunities to deliver zero trust to U.S. government agencies.

“The problem is the architecture is no longer relevant. A new architecture is needed, and that's what zero trust is trying to do.”

- Jay Chaudhry

WATCH ONLINE



Kelly White,
Co-Founder and CEO,
RiskRecon

How Ransomware Has Changed the Nature of Risk

Kelly White of RiskRecon on Assessing Suppliers' Cyber Hygiene

Ransomware has changed the risk landscape for suppliers and is forcing companies to reconsider their risk relationships, says Kelly White, co-founder and CEO of RiskRecon. "Managing the ransomware risk in the supply chain is not dissimilar to managing the risk of data loss incidents. Suppliers have got to have good cyber hygiene," he says.

In a video interview with Information Security Media Group at RSA Conference 2022, White discusses:

- Managing the ransomware risk in the supply chain;
- The correlation between cyber hygiene, ransomware and data loss;
- The key to developing a strong security culture.

WATCH ONLINE

"Managing the ransomware risk in the supply chain is not dissimilar to managing the risk of data loss incidents. Suppliers have got to have good cyber hygiene."

- Kelly White



Ami Luttwak,
Co-Founder and Chief Technology Officer,
Wiz

How to Mitigate Emerging Security Threats Against the Cloud

Wiz's Ami Luttwak on Why Cloud Security Is Getting So Much Funding and Attention

The need to secure cloud workloads and environments isn't new, but a surge of funding and attention has come to the sector over the past year. One of the most acclaimed cloud security startups has been Wiz, which in October raised \$250 million on a \$6 billion valuation.


In a video interview with Information Security Media Group at RSA Conference 2022, Luttwak discusses:

- Why there's so much talk about cloud security today;
- The most significant cybersecurity risks in cloud environments;
- How CISOs can better secure the digital transformation process.

“Companies are starting to use the cloud, but the question everyone is asking themselves is, ‘Are we doing a good job in securing the cloud?’”

- **Ami Luttwak**

WATCH ONLINE

A portrait of Denise Anderson, President & CEO of H-ISAC. She is a woman with long brown hair, smiling, wearing a blue blazer over a patterned top. The background is dark with a red geometric shape on the left.

Denise Anderson,
President & CEO,
H-ISAC

How the Healthcare Sector Is Battling Top Threats

Denise Anderson, President and CEO of H-ISAC, on Industry Progress, New Risks

While ransomware, third-party risk, phishing scams and insiders continue as the top threats facing healthcare and public health entities, the sector overall is becoming better prepared to deal with these issues than it was just a few years ago, says Denise Anderson, president and CEO of the Health Information Sharing and Analysis Center.

In a video interview with Information Security Media Group at RSA Conference 2022, Anderson discusses:

- The theft of intellectual property from pharmaceutical makers during the COVID-19 pandemic;
- The ransomware attack last year on Ireland's Health Services Executive;
- The impact of new federal breach reporting mandates, including the requirement for critical infrastructure organizations to report ransomware payments within 24 hours.

“One person's defense is everybody else's offense. The more we can get that information out, the better we can crowdsource the response.”

- *Denise Anderson*

WATCH ONLINE



CISO Perspective

The chief information security officer role emerged from the IT world as a point of necessity. Someone needed to take responsibility for cybersecurity. Today, CISOs have a much more visible role in working with every facet of the organization, from business managers to the board of trustees. We spoke with some of the leading CISOs 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.

Threat Watch: Russia-Ukraine War Remains Top CISO Risk

DXC Technology's **Michael Baker** on Top Threats, Recruitment Tips, Career Advice



Threat watch: The ongoing Russia-Ukraine war continues to pose both direct and indirect risks to enterprise networks, says Michael Baker, vice president and IT CISO of IT services and consulting firm DXC Technology.

WATCH ONLINE

Difficulties in Sharing Risks with the Board

Cielo CISO **Glauco Sampaio** on Improving Communications at the Top



In Brazil, organizations face several cybersecurity challenges including the technical difficulty of managing risks and knowing how to translate those risks to the board. Sometimes timing is very important, and companies need to start managing risks, because nowadays those who do not have this capacity cannot evolve or innovate, says Glauco Sampaio, CISO and senior executive of privacy at Cielo, in this Portuguese language interview with Information Security Media Group at RSA Conference 2022.

WATCH ONLINE

Interview conducted in
Portuguese

How to Mitigate and Manage Supply Chain Risks

Cosan Group CISO **Fernando Madueira** on Supply Chain Visibility and Resilience



To manage risks, it is essential to take into account a larger ecosystem: that is, the critical suppliers outside the company and how they interfere in operations, says Fernando Madueira, global CISO at Cosan Group. In this Portuguese language interview with Information Security Media Group at RSA Conference 2022, Madueira also offers tips for large companies on how to start the process of managing supply chain risks.

[WATCH ONLINE](#)

Interview conducted in
Portuguese

The Top 5 Security Practices With the Best Outcomes

Helen Patton, Advisory CISO of Duo Security/Cisco, Discusses New Research



What are the top five security activities that lead to the best outcomes, and why do they work so well? Those critical issues were closely examined in a recent study commissioned by Duo Security/Cisco, says Helen Patton, advisory CISO, who discusses the findings.

[WATCH ONLINE](#)

Attracting and Training OT Professionals

Nexa Resources Executive **Andre Gomes** on Solving OT Security Challenges



The OT market is growing. As a result, the industry is facing a lack of trained professionals with the techniques to secure this function. Therefore, companies need to find a way to attract and train employees to fill this space. Learn more about the need for OT security training in this Portuguese language interview with Information Security Media Group at RSA Conference 2022 with Andre Gomes, product manager at Nexa Resources.

[WATCH ONLINE](#)

Interview conducted in
Portuguese

Security and User Experience: Critical Considerations

Bernardo Vasquez of Palo Alto Networks on Identity Access Management, Zero Trust



As a CISO, it's critical to not implement security without first carefully considering the user's experience, says Bernardo Vasquez, advisory CISO in the strategic client practice of Palo Alto Networks.

[WATCH ONLINE](#)

The Power of a 'True' Third-Party Risk Exchange

Dave Stapleton, CISO of CyberGRX, Discusses Vendor Risk Management Challenges



Effective cyber risk management of vendors is critical to the success of organizations that are increasingly relying on these third parties, says Dave Stapleton, CISO of CyberGRX, who describes the importance of using a "true" third-party risk exchange.

WATCH ONLINE

Profiles in Leadership: Ankit Patel

Humana BISO Discusses How to Engage With Medical Leaders on Security Issues



Humana Business Information Security Officer Ankit Patel says the doctors, physician assistants and leaders that he deals with on a daily basis are laser-focused on providing care to patients and consider technology and security only as it relates to providing patient care.

WATCH ONLINE

Featuring a member of:
CyberEdBoard

Security in the Cloud Requires a New Mindset

CISO of Qualys Shares Strategies to Improve Cloud Security



During the accelerated digital transformation of the past two years, enterprises have fully embraced multi-cloud environments. But security practitioners are learning that security in the cloud requires a new mindset and a unique set of skills, says Jonathan Trull, CISO of Qualys.

WATCH ONLINE

Profiles in Leadership: John McClure


CISO of Sinclair Broadcast Group on the Impact of Emerging Cyber Risk Guidance



Emerging cybersecurity rules and guidance from the U.S. Securities and Exchange Commission are helping to make boards of directors more informed and more eager to discuss cyber risks and how to mitigate them, says John McClure, CISO of Sinclair Broadcast Group.

WATCH ONLINE

Featuring a member of:
CyberEdBoard



Michael Cunningham,
Vice President and CISO,
Graphic Packaging International LLC

The Path to a More Inclusive, Diverse Cyber Workforce

Michael Cunningham of Graphic Packaging International on Advancing the Workplace

To advance a more inclusive and diverse workforce in cybersecurity, it is imperative to consider "every person in the room," says Michael Cunningham, vice president and CISO of Graphic Packaging International LLC.


In a video interview with Information Security Media Group at RSA Conference 2022, Cunningham also discusses:

- The state of diversity and inclusion in cybersecurity today;
- Ways for organizations to become more inclusive and diverse;
- His own career journey.

"Inclusion is someone being receptive of the person coming in, but it's also inspiring other individuals to want to do something."

- *Michael Cunningham*

WATCH ONLINE



Rich Lindberg,
CISO,
JAMS

Profiles in Leadership: Rich Lindberg

JAMS CISO Launched Career in Cybersecurity When He 'Embraced Fun'

Rich Lindberg, CISO of JAMS, didn't set out to have a career in cybersecurity. Instead, he sought to make a living at what he enjoyed – programming. "I embraced fun," he says. Now he wants to help others do the same by growing the diversity of the industry workforce.

In an interview with Information Security Media Group as part of the CyberEdBoard's ongoing Profiles in Leadership series, recorded at RSA Conference 2022, Lindberg discusses:

- His career path;
- How he has responded to threats and challenges;
- How he and his peers are approaching the diversity challenge.

**"Make the industry more friendly.
Make the industry more diverse because we're missing out on so much of the talent."**

- Rich Lindberg

WATCH ONLINE

Featuring a member of:
CyberEdBoard

Profiles in Leadership: Jeff Farinich

CISO's Challenge Was to Build Program from Scratch, Raise Security Maturity Bar



It was the ultimate challenge: Build a cybersecurity program from scratch. Three years later, Jeff Farinich, CISO of New American Funding, talks about the transformation and helping raise the bar on the enterprise's security maturity.

WATCH ONLINE

Featuring a member of:
CyberEdBoard

Challenges of Building a Global Security Program

CISO **Eric Sanchez** Says Strategize Globally, Act Locally



CISO Eric Sanchez of Kyowa Kirin North America discusses the nuances and challenges of building a security program at an international company. He shares strategies for managing the people, operations and technology and explains why strong interpersonal and crisis management skills are a must.

WATCH ONLINE

Addressing the Talent Shortage

EDP Brazil CISO **Almeida Milton** on Building Up Cybersecurity Skills



Cybersecurity demands and risks have increased at a very high rate due to the recent transformational crises around the world. As a result, the development of cybersecurity professionals has not kept up with the demand. In this Portuguese language interview with Information Security Media Group at RSA Conference 2022, EDP Brazil CISO Milton Almeida shares thoughts on how the industry can build more talent in the cybersecurity field.

WATCH ONLINE

Interview conducted in
Portuguese

Profiles in Leadership: Rob Hornbuckle


Allegiant Air CISO Details Top Strategies for Effective Recruitment



Beyond advising the senior-most levels of the business in the strategic use of technology, the need to recruit new cybersecurity professionals often also tops the list of top tasks facing today's security leaders. "We've had a lot of people retire, and retire early with COVID coming up, especially the older generation with lots more experience in the field," says Rob Hornbuckle, CISO of Las Vegas-based airline Allegiant Air.

WATCH ONLINE


Featuring a member of:
CyberEdBoard

A man with short dark hair and a beard, wearing a dark blue blazer over a white button-down shirt, is speaking. He is positioned in front of a background that features a traditional Japanese building with a tiled roof and autumn-colored trees.

“We’re actually seeing live cybersecurity play a very real role in a physical military conflict. So we’re looking at the application of destructive malware and other tactics, which is increasing the risk threshold across the world.”

Michael Baker,

Vice President, IT CISO, DXC Technology

A portrait of Nick Coleman, a man with short brown hair and glasses, wearing a dark blue suit jacket over a white shirt. He is smiling slightly and looking off-camera to the right. The background is a blurred cityscape with a blue sky and a tall building on the right.

Nick Coleman,
CSO, Real Time Payments,
Mastercard

Securing Digital Payments in the Future

Mastercard's Nick Coleman Discusses 'Threatcasting' and Real-Time Payments

Ten years from now, "the ability to transact on a global basis will continue," says Nick Coleman, CSO, real-time payments at MasterCard, who adds, "Maybe my car will buy stuff for me." Coleman discusses the future of digital payments and the technologies that can help secure that future.

In a video interview with Information Security Media Group at RSA Conference 2022, Coleman discusses:

- How digital payments have evolved;
- How Mastercard's Fusion Center practices "threatcasting" to isolate the threats that will be important tomorrow;
- The future of real-time payments.

"We have a lot of challenges in the world. We have traditional threats like ransomware, and we also have new and emerging threats."

- *Nick Coleman*

WATCH ONLINE



Patricia Titus,
Chief Privacy and Information Security Officer,
Markel Corp.

Why Diversity Is the Defender's Greatest Weapon

CISO Patricia Titus on Changing Our Recruitment Practices

CISO Patricia "Patti" Titus says the cybersecurity sector is "still struggling" with the diversity and inclusion it requires. "The things we do really impact all of our end users, employees and customers," she says, so you need "the broadest skill set possible when you're making decisions."

In a video interview with Information Security Media Group at RSA Conference 2022, Titus discusses:

- The current state of diversity and inclusion in the industry;
- Where we have improved and what issues still need to be addressed;
- Advice to security leaders who want recruit more diversely.

"Take a risk on someone, open your door to let them come in, and ask questions and be available."

- Patricia Titus

WATCH ONLINE



Chris Holden,
CISO,
Crum & Forster

What Cybersecurity Leaders Wish They Knew Before a Breach

Chris Holden, CISO at Crum & Forster, on How Firms Can Strengthen Incident Response

Crum & Forster CISO Chris Holden has helped organizations respond to many breaches over the years, and through this experience he has developed an excellent sense of who companies should call first and have on their response team if they suspect that a security incident has taken place.

In a video interview with Information Security Media Group at RSA Conference 2022, Holden discusses:

- What CISOs wish they knew before experiencing a breach;
- What needs to happen once an incident is suspected;
- How to deal with cyber insurance provider requirements.

“ou need to change the culture of 'security is telling you to do this' to having them understand why.”

- *Chris Holden*

WATCH ONLINE



Kevin Li,
CISO,
MUFG Securities Americas



Rocco Grillo,
Managing Director,
Alvarez & Marsal

'When, Not If': Crafting Cyber Resilience Plans That Work

Best Practices From CISO Kevin Li and Incident Response Expert Rocco Grill

To excel at cybersecurity incident response, start with planning, preparation and, ideally, regular tabletop exercises, say Kevin Li, CISO for MUFG Securities Americas, and Rocco Grillo, managing director of Alvarez & Marsal's Disputes and Investigations Global Cyber Risk Services practice.


In a video interview with Information Security Media Group at RSA Conference 2022, Li and Grillo also discuss:

- Top people, process and technology challenges around incident response;
- Best practices for setting cyber resilience expectations with senior managers and boards of directors;
- How the discipline of cyber and business resilience looks set to evolve.

WATCH ONLINE

“It’s all muscle memory. It comes down to identifying what the threat is and trying to be proactive.”

- Kevin Li



Vishal Salvi,
CISO and Head of the Cyber Practice,
Infosys

Strategies for Reskilling and Filling Cybersecurity Jobs

Infosys CISO Vishal Salvi on Mentoring, Online Training and Foundational Skills

The gap between cybersecurity workforce demand and the number of skilled workers available to fill those jobs widened during the pandemic. So organizations need to take a multi-pronged approach to attract, reskill and retain employees, says Vishal Salvi, CISO and head of cyber practice at Infosys.

In a video interview with Information Security Media Group at RSA Conference 2022, Salvi also discusses:

- The discipline and passion for continuous learning in cybersecurity;
- The need for diverse backgrounds and perspectives in the field;
- Key strategies for recruiting new personnel.

“The foundational element of cyber is very important and it should be done when we catch them young.”

- *Vishal Salvi*

WATCH ONLINE

Government Perspective

Government agencies have always been on the front lines of the war between threat actors and society. However, 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

Getting Ready for Software Bills of Material

Grant Schneider of Venable on What's Needed to Make SBOMs Ubiquitous



Software bills of material, or SBOMs, are still "years away" from being ubiquitous, says Grant Schneider, senior director for cybersecurity services at Venable. He says it will take time for them to catch on, and a set of standards and other critical components for industry need to be defined.

[WATCH ONLINE](#)

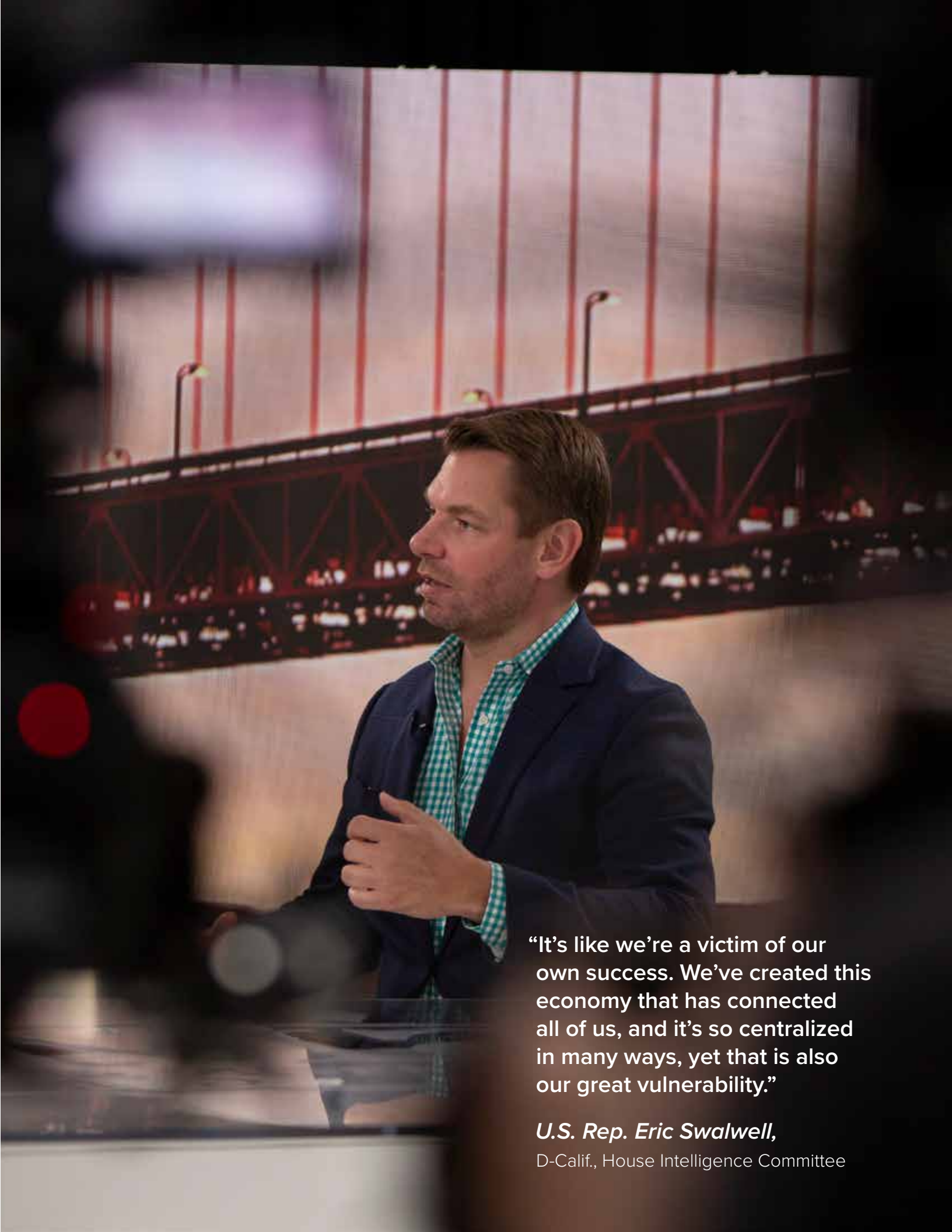
Are We on the Verge of Getting to Passwordless?

Identity Expert **Jeremy Grant** Discusses the Shift to Cryptographic Keys




Jeremy Grant of Venable says we are getting closer to eradicating the password. He says that in the next 12 to 18 months, "There will be a lot of uptake from big, consumer-facing brands to finally kill the password and let people instead create a passkey when they sign up for an account."

[WATCH ONLINE](#)

A man with short brown hair, wearing a dark blue blazer over a green and white checkered shirt, is shown in profile, looking towards the left. He is standing in front of a large, illuminated bridge at night. The bridge has a complex steel truss structure and is lit with warm lights. The background is dark, with some blurred lights from the bridge and surrounding area.

“It’s like we’re a victim of our own success. We’ve created this economy that has connected all of us, and it’s so centralized in many ways, yet that is also our great vulnerability.”

U.S. Rep. Eric Swalwell,
D-Calif., House Intelligence Committee

A portrait of Lester Godsey, a man with short dark hair and glasses, wearing a dark blue suit, a light blue striped shirt, and an orange patterned tie. He is speaking and gesturing with his right hand. The background is a solid light pink color.

Lester Godsey,
CISO,
Maricopa County, Arizona

Social Media and the Threat to Cybersecurity

CISO of Maricopa County, Arizona on Strengthening Election Security

"Social media is probably the newest and most impactful thing that we've seen from a cybersecurity perspective at Maricopa County," says its CISO, Lester Godsey. The only response to misinformation and disinformation campaigns, he says, is to use the same platform and respond with the facts.

In a video interview with Information Security Media Group at RSA Conference 2022, Godsey discusses:

- How social media is affecting the threat landscape;
- How Maricopa County is monitoring the social media threat to security;
- How to incorporate social media into threat intel programs.

"Social media sentiment has a direct correlation with not only increased cyber risk or threat to the organization, but also kinetic or physical risk."

- **Lester Godsey**

WATCH ONLINE

Calling Cyber-Experienced Attorneys: Uncle Sam Needs You

Have Fun While Boosting National Security, Says Cyber Command Lt. Col. **Kurt Sanger**



Specifically, the U.S. Department of Defense is seeking attorneys who are cybersecurity subject matter experts and can embed inside each agency, maintain a base of understanding and work closely with each other, says Lt. Col. Kurt Sanger, deputy staff judge advocate of U.S. Cyber Command.

[WATCH ONLINE](#)

The Critical Role of Private-Public Cyber Collaboration

Kiersten Todt, CISA chief of staff, on Industry Engagement, Workforce Development



One of the most important recent developments by CISA has been the creation of the Joint Cyber Defense Collaborative, or JCDC, which is focused on operational private-public collaboration, says Kiersten Todt, CISA chief of staff

[WATCH ONLINE](#)

Proposed SEC Rules Will Force Boards to Double Down on Cyber

BlackBerry's **Roger Sels** on the SEC Mandating More Stringent Oversight of Cyber Risk



Publicly traded companies will need to beef up their cybersecurity knowledge since the the U.S. Securities and Exchange Commission is proposing rules and guidelines that would mandate more stringent oversight of cyber risk, says Roger Sels, vice president of cyber solutions for BlackBerry.

[WATCH ONLINE](#)


The Push on Capitol Hill for Passwordless Authentication

Okta's **Sean Frazier** on Securing the Supply Chain, Software Development Life Cycle



Interest in passwordless authentication architecture continues to grow among U.S. government agencies and departments as they embrace more modern approaches to identity and access management, says Sean Frazier, federal chief security officer at Okta.

[WATCH ONLINE](#)

A medium shot of Kiersten Todt, a woman with long brown hair, wearing a white blazer over a white top. She is wearing large gold hoop earrings, a gold necklace with a feather pendant, and several rings. She is gesturing with her hands while speaking. The background is a blurred cityscape at night.

“While we don’t want nor should we have government on our networks, letting industry share that information is so critical to our ability to merge the data so we get a better sense of what’s actually happening.”

Kiersten Todt,

Chief of Staff,
CISA

Preparing for Retaliatory Attacks From Russia

FBI's Elvis Chan Warns Businesses Against Complacency



"I'm concerned that at some point the Russians are going to launch cyber retaliatory attacks against the United States at election infrastructure and the transportation, financial and energy sectors," says Elvis Chan, supervisory special agent at the San Francisco Division of the FBI.

[WATCH ONLINE](#)

The Criticality of Reporting Cybercrimes

Investigator **Steve Dougherty** on Accelerating Reporting



For the seventh year in a row, business email compromise has produced the largest losses of any type of cybercrime, according to Steve Dougherty of the U.S. Secret Service. He says organizations need to build and maintain relationships with law enforcement agencies before an attack happens.

[WATCH ONLINE](#)

Defending Against Major Nation-State Cyberattacks

U.S. Rep. **Eric Swalwell**, D-California, Discusses Top National Cybersecurity Concerns



The U.S. is on "borrowed time" for a major cyberattack that could potentially seriously disrupt critical infrastructure, but the nation can secure its systems and resources to avoid such cybersecurity disasters, says Rep. Eric Swalwell, D-California.

[WATCH ONLINE](#)



Focus on Zero Trust

The concept of using firewalls, identity management and endpoint controls to protect enterprises has changed very little since cybersecurity began, but all that's evolving with zero trust. Zero trust, the simple framework of "never trust, always verify," replaces the reliance on protecting the perimeter and focuses on securing applications and data. We spoke with the founders of zero trust, as well as key industry leaders implementing it, to find out what needs to be done to enable a whole new architecture that will stop threat actors at the gates.

Safeguarding the Enterprise Across Multiple Public Clouds

Microsoft's **Abbas Kudrati** and HCL's **Upendra Singh** on Zero Trust and Cloud Security



Organizations have created significant security challenges by rapidly migrating applications, data and workloads to multiple public clouds over the course of the COVID-19 pandemic, according to Abbas Kudrati, Microsoft's director and chief cybersecurity adviser in APAC, and Upendra Singh, HCL's head of global IT security.

WATCH ONLINE

Critical Infrastructure: How to Counter Rising Threats

Palo Alto Networks' **Lionel Jacobs Jr.** on Locking Down Industrial Cybersecurity



Threats facing industrial control systems are well-documented, and as the Russia-Ukraine war continues, concerns are rising about reprisals aimed at poorly protected Western critical infrastructure, says Lionel Jacobs Jr., security architect for ICS and SCADA systems at Palo Alto Networks.

WATCH ONLINE

A portrait of John Kindervag, a man with a beard and glasses, wearing a dark blue suit jacket over a dark blue shirt. He is looking directly at the camera. An American flag pin is visible on his lapel.

John Kindervag,
Creator of zero trust

Zero Trust: 'What Are You Trying to Protect?'

Father of Zero Trust, John Kindervag, on How Conversation, Industry Have Evolved

In the wake of digital transformation and President Biden's 2021 cybersecurity executive order, an entire industry has sprung up around the concept of zero trust. John Kindervag, the researcher who created the architecture, weighs in on how the discussion has evolved.

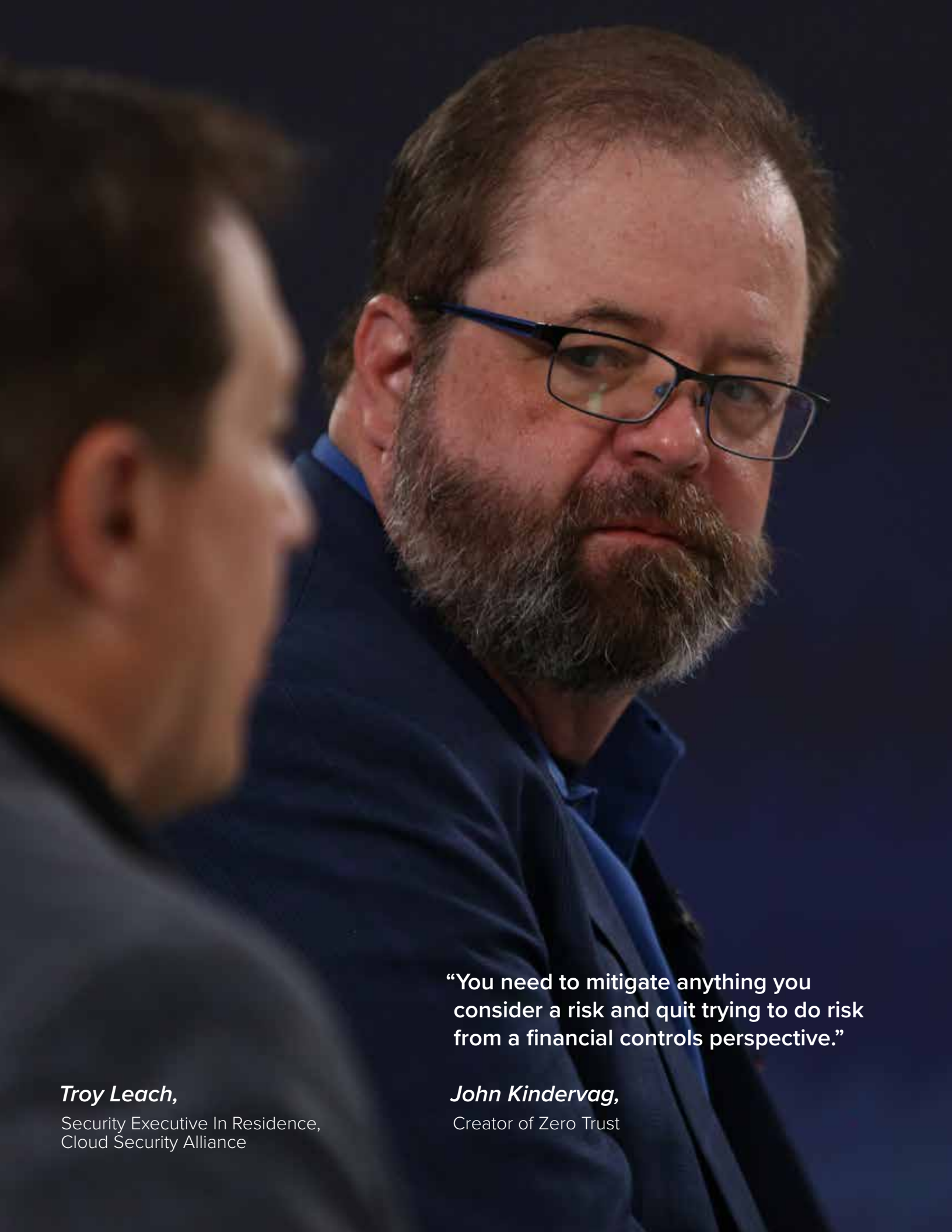
In a video interview with Information Security Media Group at RSA Conference 2022, Kindervag also discusses:

- Why too many people are stuck on defining zero trust;
- The industry that's been spawned;
- The impact of Biden's executive order.

“The most important thing is: What do I need to protect? If you have one of those no-vendor-left-behind approaches, you’re going to fail.”

- John Kindervag

WATCH ONLINE



“You need to mitigate anything you consider a risk and quit trying to do risk from a financial controls perspective.”

Troy Leach,

Security Executive In Residence,
Cloud Security Alliance

John Kindervag,

Creator of Zero Trust

Does Zero Trust Feel Too Overwhelming? Here's How to Start

Cloudflare CSO **Joe Sullivan** on Why Zero Trust Must Be Broken Into Bite-Sized Chunks



Evolving to a zero trust architecture can be overwhelming for organizations, leaving many unsure of where they should even start. Cloudflare Chief Security Officer Joe Sullivan urges CISOs to break the journey into bite-sized chunks that can be easily digested.

[WATCH ONLINE](#)

How Zero Trust Keeps Users, Applications and Data Protected

iboss CEO, **Paul Martini**, on How Zero Trust and Security Service Edge Work Together



Businesses have embraced zero trust architectures in an effort to increase their protection while reducing cost and complexity for the organization, according to iboss CEO Paul Martini. Martini says companies are turning to zero trust to more effectively protect their users, applications and data.

[WATCH ONLINE](#)

What's Needed for Firms to Bring SASE and Zero Trust to Life

Juniper's **Kate Adam** on the Challenges and Opportunities for SASE and Zero Trust



Implementing modern architectures such as zero trust and secure access service edge (SASE) remains an issue for many organizations. This challenge has been amplified by the shortage of skilled cybersecurity personnel, says Kate Adam, senior director of enterprise product marketing at Juniper Networks.

[WATCH ONLINE](#)

Boosting Security Resilience and Defending the IT Ecosystem

Jeetu Patel of Cisco Discusses the Critical Ability to 'Bounce Back' From Incidents



With rising threats facing critical infrastructure sectors, such as healthcare and financial services, "society as a whole, and the safety of society is completely dependent on cyber risk" - and being security resilient, says Jeetu Patel, executive vice president and general manager, security and collaboration business units, Cisco.

[WATCH ONLINE](#)



Nikesh Arora,
CEO and Chairman,
Palo Alto Networks

Nikesh Arora on the Palo Alto Networks Growth Strategy

CEO Opens Up About Network, Cloud, SecOps and ZTNA 2.0

Most publicly traded security vendors specialize in one technology category, but Palo Alto Networks has built out industry-leading practices around network security, cloud security and security operations. CEO Nikesh Arora discusses this unique path.

In a video interview with Information Security Media Group at RSA Conference 2022, Arora also discusses:

- The value of platform over products;
- The value of automation in reducing response times;
- What makes Palo Alto Networks' approach to CNAPP and XDR unique.

“Every security company gets really good at one thing and then misses the boat on the next thing.”

- Nikesh Arora

WATCH ONLINE

A medium shot of Jay Chaudhry, an older man with glasses, wearing a dark polo shirt. He is standing in a server room with rows of server racks visible in the background. His hands are resting on a dark surface in the foreground.

“Zero Trust architecture was created to really move away from legacy firewall and VPN-based architecture. Unfortunately, every firewall and VPN company is calling themselves zero trust.”

Jay Chaudhry,

Founder, Chairman and CEO, Zscaler



Focus on OT Security

The Colonial Pipeline ransomware attack in 2021 and resulting gasoline shortage demonstrated just how fragile our critical infrastructure can be. Cybersecurity isn't just about protecting IT assets. It's also about protecting the operational technologies (OT) that run in manufacturing facilities, medical equipment, power plants and many more businesses. We spoke to the top OT security experts in the field about strategies for protecting devices in the supercharged world of highly organized ransomware groups and cyberwarfare.

How CISOs Are Dealing With a Growing Digital Attack Surface

John Maddison, Fortinet CMO & EVP Products, on the Major Cyber Concerns for CISOs



Customers, channel partners and technology partners are dealing with a broad range of security concerns spanning the gamut from the sophistication of the threat landscape to the skills shortage. John Maddison, Fortinet's CMO and EVP, products breaks down the most urgent priorities.

WATCH ONLINE


Tracking the Convergence of IT and OT in the Energy Sector

Threats Facing the Energy Sector Are Changing, Warns Siemens Energy's **Mex Martinot**



As information technology (IT) and operational technology (OT) continue to converge, organizations must stay ahead of new security challenges and threats, says Mex Martinot, vice president and global head of industrial cybersecurity at Siemens Energy.

WATCH ONLINE

A man with short, light-colored hair, wearing a dark suit jacket over a light blue button-down shirt, is speaking at a clear podium. He is looking slightly to his left. The background is a blurred city skyline at night, with many lights from buildings and streets. A red railing is visible in the foreground, partially obscuring the podium.

"I think there's a gap for the typical CISO, who came from IT and doesn't really understand the uniqueness of OT. I also think that the No. 1 metric for success is you have to have leadership from the top down to sponsor these cybersecurity programs."

Mark Cristiano,

Commercial Director, Global Services Business,
Rockwell Automation



Dawn Cappelli,
OT CERT Director,
Dragos

Partnering to Secure Industrial Infrastructure

Dawn Cappelli on the Mission of the New Dragos OT-CERT Initiative

Former CISO of Rockwell Automation Dawn Cappelli is now the director of the the new Dragos OT-CERT, a cybersecurity resource designed to help industrial asset owners and operators build their OT cybersecurity programs, improve their security postures and reduce OT risk.

In a video interview with Information Security Media Group as part of RSA Conference 2022, Cappelli discusses:

- The mission of the Dragos OT-CERT;
- The threats and vulnerabilities the OT-CERT aims to respond to and mitigate;
- The role partnerships will play and the partners involved in the initiative.

“The big companies are harder targets, and so more and more we see that the adversaries are going after the small- and medium-sized companies.”

- *Dawn Cappelli*

WATCH ONLINE

How Modern Tech Is Changing Vulnerabilities and Responses

Check Point CSO **Itai Greenberg** on the Impact of IoT, Cloud AI and Deep Learning



Modern technologies are a double-edged sword in cybersecurity, says Itai Greenberg, chief strategy officer at Check Point Software Technologies.

[WATCH ONLINE](#)

Why OT Cybersecurity Is Daunting and How to Address It

Lesley Carhart of Dragos on Responding to OT Cybersecurity Risks



In the ever-shifting cybersecurity threat landscape, IT risks have never been more prominent. But what about operational technology? Lesley Carhart of Dragos discusses OT vulnerabilities, how adversaries are taking advantage and why Dragos has launched a new OT CERT.

[WATCH ONLINE](#)

Responding to Federal Directives on Critical Infrastructure

Mark Cristiano of Rockwell Automation on Why Uptime Is Crucial for Infrastructure



Critical infrastructure providers face a unique set of challenges when it comes to securing their environment from the cruciality of uptime to complying with new federal directives, according to Mark Cristiano, commercial director for Rockwell Automation's global services business.

[WATCH ONLINE](#)



Wael Mohamed,
CEO,
Forescout

How to Ditch the Silo and Safeguard Medical Devices

CEO Wael Mohamed on Why Forescout Bought IoMT Firm CyberMDX, Analytics Firm Cysiv

Since joining Forescout 15 months ago as CEO, Wael Mohamed has aggressively pursued acquisitions, scooping up CyberMDX in February to safeguard internet of medical things devices and Cysiv in June to help OT and IoT customers analyze, detect and respond to threats using cloud-native data analytics.


In a video interview with Information Security Media Group at RSA Conference 2022, Mohamed discusses:

- The top challenges of gaining visibility into medical devices;
- How customers benefit from having IoMT on the platform;
- Why automation has become a significant area of focus.

“One of the biggest challenges for us as an industry is the amount of alerts and amount of data we have to deal with. We have to use machines.”

- *Wael Mohamed*

WATCH ONLINE



Grant Geyer,
Chief Product Officer,
Claroty

How to Defend Critical Infrastructure Against New Threats

Claroty CPO Grant Geyer on What's Getting Overlooked Around Infrastructure Security

The dangers associated with compromising critical infrastructure assets burst into public view with the May 2021 Colonial Pipeline ransomware attack, prompting significant investment from both the government and the private sector, according to Claroty Chief Product Officer Grant Geyer.

In a video interview with Information Security Media Group at RSA Conference 2022, Geyer also discusses:

- The top overlooked areas around securing critical infrastructure;
- How the Russia-Ukraine war has affected critical infrastructure;
- How remote work has created risk and exposure for OT systems.

“What a lot of organizations don’t simply realize is how much critical infrastructure they may have in their environments that’s at risk.”

- **Grant Geyer**

WATCH ONLINE

Focus on Cybercrime/Nation State

The war in Ukraine has changed the game of cybersecurity. Cyberwarfare concepts that were once theoretical are now being played out on the world stage, and public and private sector organizations remain on a heightened state of alert. While authorities have just begun to succeed in thwarting cybercriminal groups, the threat landscape is no safer. We spoke with top practitioners and analysts about the state of cybercrime and what the industry needs to do to get ahead of the attackers.

Assessing Crypto and Third-Party Risks

Troy Leach of Cloud Security Alliance
on Emerging Trends



Billions of dollars have already been lost in crypto exchanges, and some of the some losses have been due to "basic" security failures, including third parties not implementing common controls, says Troy Leach, security executive in residence, Cloud Security Alliance.

[WATCH ONLINE](#)

Maximizing Opportunities to Stop Ransomware Attacks

Chet Wisniewski of Sophos on
Latest Research Findings



The median dwell time that hackers are spending in victims' networks – from the time a compromise, such as a phishing incident or a vulnerability exploit, begins to the time ransomware encryption is triggered – has grown from 11 to 15 days. That means organizations now have a little more precious time to stop an attack "before the worst happens," says Chet Wisniewski, principal research scientist at Sophos.

[WATCH ONLINE](#)

Cybercrime Chatter: US Critical Infrastructure Off-Limits?

Analyst1's **Jon DiMaggio** Also Says Criminals Find No Safe Haven in Cryptocurrency



As the Russia-Ukraine war continues, and analysts watch for retaliatory cyberattacks against Ukraine's allies, cybercrime tracker Jon DiMaggio of Analyst1 says there's good news, in that Russian cybercriminals seem to have little or no incentive to move against U.S. critical infrastructure.

[WATCH ONLINE](#)

Battling Ransomware: 'We're Targeting the Entire Ecosystem'

Marc Rogers of Okta Reviews Progress on Ransomware Task Force Recommendations



More than one year after devastating ransomware attacks disrupted critical infrastructure in numerous countries, including Colonial Pipeline in the United States, the problem hasn't gone away. But numerous governments have helped to marshal a better response by focusing on improving the resilience of domestic businesses, combating the illicit use of cryptocurrency and devoting increased law enforcement resources to track and disrupt criminal syndicates, says Marc Rogers, senior director of cybersecurity at Okta.

[WATCH ONLINE](#)

Ransomware Response Essential: Fixing Initial Access Vector

'They'll Hit You Again and Again,' Warns Rapid7 Chief Scientist **Raj Samani**



A lot has changed in the three years since cybersecurity veteran Raj Samani was last able to attend the RSA Conference in San Francisco. But what hasn't changed is the innovation being practiced by ransomware groups and the challenges facing cybersecurity teams, including dealing with the latest vulnerabilities, or "vuls."

[WATCH ONLINE](#)

Ransomware Groups Pursue Fresh Monetization Strategies

Kela's **Steve Rivers** Sees Ransomware Groups Using New Techniques to Extract Ransoms



Ransomware-wielding criminals constantly refine their behavior and tactics to maximize the chance of a payday, and recently they have been implementing fresh strategies for monetizing stolen data, says Steve Rivers at threat intelligence firm Kela.

[WATCH ONLINE](#)



“We should be aware that we, our generations, are now making these decisions for all future generations. And it is a big deal to think about.”

Mikko Hypponen,
Chief Research Officer,
WithSecure

Ransomware Defenses: Cyber Insurer Details Best Practices

Coalition's **Payal Chakravarty** Talks Ransomware Trends and Cyber Insurance



Insurance claims being filed by ransomware victims are growing as criminals continue to hit businesses with crypto-locking malware. To avoid these claims, organizations can take a number of proven steps to better protect themselves, says Payal Chakravarty of insurer Coalition.

[WATCH ONLINE](#)

Unexpected Pairings: Wine Tasting and Threat Intelligence

Certified Sommelier **Allan Liska** on the Deductive Craft of Understanding Threats



In his spare time, ransomware expert Allan Liska likes to taste wine, so much so that he recently became a certified sommelier. While he thought he was branching out from his day job as principal intelligence analyst at Recorded Future, Liska says he's found numerous parallels between the two processes.

[WATCH ONLINE](#)

Conti Ransomware Group Explores Post-Encryption Future

AdvIntel's **Vitali Kremez** Says Data Theft Without Encryption Is Increasingly Common



The February leak of internal communications from Conti, one of the world's most notorious ransomware groups, highlighted the extent to which such cybercriminal groups are running sophisticated and innovative business operations, says Vitali Kremez, chairman and CEO of New York-based Advanced Intelligence, aka AdvIntel.

[WATCH ONLINE](#)

Watch Out for Cyber Insurance Caveats

Attorney **Steven Teppler** of Sterlington PLLC on Meeting Insurers' Latest Demands



Cyber insurance is getting much tougher to obtain, and coverage for security incidents is not guaranteed even when policies are issued, says attorney Steven Teppler, chair of the privacy and cybersecurity practice of law firm Sterlington PLLC.

[WATCH ONLINE](#)



Jackie Burns Koven,
Cyberthreat Intelligence Lead,
Chainalysis

Why Blockchain Is a Double-Edged Sword for Criminals

Chainalysis' Jackie Burns Koven Shares Netwalker Ransomware Disruption Highlights

The disruption of the Netwalker ransomware group in January 2021 by U.S. and Bulgarian authorities resulted in the seizure of \$30 million, the largest-ever recovery of ransomware funds, but it was also notable for the way cybersecurity teams took down the group.

In a video interview with Information Security Media Group at RSA Conference 2022, where she served as a session panelist for "BTC as an IOC: Inside the Largest Ever Ransomware Funds Seizure," Koven discusses:

- Highlights from the January 2021 Netwalker disruption, including the arrest of a key affiliate;
- Why blockchain can be a double-edged sword for criminals;
- How the ransomware, ransomware-as-a-service and affiliate-based ecosystem is expected to evolve.

WATCH ONLINE

“This is a global crime that can exist in our backyard. It also shows with the imposition of costs, we can make a dent in these ransomware ecosystems.”

- Jackie Burns Koven

Russia, Ukraine and the Future Cybercrime Landscape

John Fokker of Trellix on Latest Findings of Cyberwar Activities in Ukraine



The invasion of Ukraine by Russia is changing global cybercrime dynamics. John Fokker of Trellix explains why, drawing from new research, attacks and adversarial trends that point to a new evolution of the cybercrime landscape.

WATCH ONLINE

4 Emerging Attack Techniques Cyber Adversaries Are Using

Derek Manky, Head of Fortinet's FortiGuard Labs, on New, Hard-to-Fight Techniques



Cyber adversaries are embracing defense evasion, triple extortion, wiper malware and the accelerated exploit chain, and that is significantly reshaping the threat landscape that CISOs have to deal with, according to Derek Manky, head of Fortinet's FortiGuard Labs.

WATCH ONLINE

The Cybersecurity Dilemma for SMEs

Matt Aldridge of OpenText on the Key to Resilience



SMEs recognize the need to increase their cybersecurity spend, but limited resources can make them uncertain about which tools to invest in, says Matt Aldridge, principal solutions consultant at OpenText. He explains why a comprehensive approach is key to achieving and maintaining cyber resilience.

WATCH ONLINE

Cybercrime Deep Dive: Hydra Marketplace Takeaways

Darknet Market Money Laundering Tools Popular, Chainalysis' Kimberly Grauer Says



Why do darknet markets continue to thrive despite the prevalence of law enforcement infiltration, disruptions and exit scams? Blame a lack of good alternatives, as well as markets so often providing easy access to buyers, sellers and valuable services, such as cryptocurrency mixing tools and other money laundering facilities, says Kim Grauer, director of research at blockchain analytics firm Chainalysis.

WATCH ONLINE



John Kindervag,
Zero Trust Creator, SVP of Cybersecurity Strategy,
ON2IT Cybersecurity

Troy Leach,
Security Executive in Residence,
Cloud Security Alliance

What Should Security Leaders Be Preparing for Now?

Troy Leach and John Kindervag Discuss Risk, Ransomware

For the remainder of 2022, security leaders should not ignore current geopolitical tensions, which are going to infiltrate into private sectors, says Troy Leach, security executive in residence at the Cloud Security Alliance. Both the war in Ukraine and conflicts in Asia are "going to be very disruptive, and there are going to be very innovative ways of developing malware because of this," he says.

In a video interview with Information Security Media Group as part of RSA Conference 2022, Leach and Kindervag discuss:

- Trends in 2022 and beyond;
- How ransomware has affected cyber insurance;
- How a Zero Trust strategy can prevent a ransomware attack.

“Exploits are just a minimal part of the overall vulnerabilities. So, how do we address the third parties of third parties?”

- *Troy Leach*

WATCH ONLINE



“Criminals and criminal activity in crypto space and non-crypto space is constantly adapting because of this law enforcement pressure. That’s why we see darknet markets continue to thrive.”

Kim Grauer,

Director of Research,
Chainalysis

Cybersecurity Retention: Don't Forget the Fun Factor

Delinea's **Joseph Carson** to Industry: We Need to Dial Down the Stress and Scariness



Never forget the fun factor when it comes to recruiting and retaining cybersecurity talent, not least to help address the nonstop stress and scariness that so often accompany positions in the field, says Joseph Carson, chief security scientist at Delinea.

[WATCH ONLINE](#)

Accelerating Cyberthreat Response Times

Wesley Mullins, CTO of Deepwatch, on Overcoming Response Hurdles



Trying to respond manually to threats solely as a cyber team that does not have control over the entire IT ecosystem can severely slow down response times, says Wesley Mullins, CTO of Deepwatch.

[WATCH ONLINE](#)

The Evolution of Phishing From Email to SMS and Voice Hacks

KnowBe4's **Roger Grimes** on Why MFA Alone Isn't a Successful Hack Prevention Strategy



Phishing is no longer restricted to just emails. As attackers broaden their arsenal, businesses today also need to be on the lookout for impersonation attempts via SMS text messages or voice calls, says Roger Grimes, a data-driven defense evangelist at KnowBe4.

[WATCH ONLINE](#)

Move From a Reactive to a Proactive State With Intelligence

AJ Nash, ZeroFox's VP of Threat Intel, on How Private Firms Are Using Intelligence



Building out a threat intelligence program is no easy feat for even the largest and most resource-rich organizations, and the challenges are only amplified for smaller companies that have limited budget or personnel, according to AJ Nash, ZeroFox's vice president of threat intelligence.

[WATCH ONLINE](#)



Kal De,
General Manager,
VMware Security Business Unit

How to Keep Business Flowing During a Ransomware Attack

VMware Security GM Kal De on What Gets Overlooked in Ransomware Defense Strategies

Time is money, and at no time is that adage more apparent than following a ransomware attack, where every second of downtime costs businesses in industries such as retail and e-commerce large sums of cash. Business continuity is therefore vital even before determining whether ransomed data or systems can be recovered, says Kal De, general manager of VMware's security business unit.

In a video interview with Information Security Media Group at RSA Conference 2022, De also discusses:

- What businesses overlook around ransomware defense;
- Top business continuity challenges following a ransomware attack;
- Why network and endpoint visibility is needed for true XDR.

[WATCH ONLINE](#)

“There are a lot more applications systems that are wired together. It’s a much, much broader attack surface than what we knew 10 years ago.”

- *Kal De*



Ian Gray,
Senior Intelligence Director,
Flashpoint

Hydra Darknet Market: Threat Intelligence Lessons Learned

Flashpoint's Ian Gray on Cybercrime Marketplace Dynamics and Impact of Takedowns

Darknet markets continue to thrive as hubs for criminality, including for narcotics and firearm distribution, malware supply, ransomware recruitment and other cornerstone cybercrime-as-a-service activities.

In a video interview with Information Security Media Group at RSA Conference 2022, where he served on the session panel for "Hydra Marketplace: Where Crypto Money Laundering Trail Goes Cold," Gray also discusses:

- The dynamics of cybercrime marketplaces and the effects of law enforcement takedowns;
- What threat intelligence and blockchain investigations reveal about how sellers and cybercriminals used the Hydra marketplace to launder gains;
- The correlation between geopolitics and cybercrime: how the war in Ukraine is affecting tactics, techniques and procedures, as well as goals.

“There’s a high demand for these types of services, but there is always a high degree of risk. Is law enforcement going to be tracking these cryptocurrencies?”

- Ian Gray

WATCH ONLINE



Chad Sweet,
CEO and Co-Founder,
The Chertoff Group

Russia's Lie: It's Hardly Hitting Ukraine With Cyberattacks

Don't Fall for the Misinformation, Warns Chad Sweet of The Chertoff Group

With the Russia-Ukraine war having lasted over 100 days, many commentators continue to highlight the apparent lack of cyberattacks being launched by Moscow against Kyiv.


In a video interview with Information Security Media Group at RSA Conference 2022, Sweet also discusses:

- Risk mitigation advice pertaining to the ongoing Russia-Ukraine war and potential spillover;
- The Chertoff Group's free ransomware risk assessment;
- Supply chain attack trends.

WATCH ONLINE

“A lot of the risks in cyber have been out there but the situation in Ukraine is elevating that in a very visible way for the world to see.”

- Chad Sweet

A woman with long, wavy brown hair, wearing a black blazer over a patterned top, is speaking at a dark podium. The background is a blurred city skyline at night.

“We’re starting to truly make an impact and understand how these networks work, how these operators work and how we can start disrupting their attacks.”

Wendi Whitmore,

SVP and Head of Unit 42,
Palo Alto Networks

A portrait of Mikko Hypponen, a man with light brown hair tied back, wearing round glasses and a blue checkered blazer over a white shirt. He is looking slightly to the right with a serious expression. The background is a blurred purple and blue.

Mikko Hypponen,
Chief Research Officer,
WithSecure

Russia's Cyber Offensive Against Ukraine Continues Nonstop

Cybersecurity Expert Mikko Hypponen Says Ukraine's Ability to Stay Online Highlights Its Defensive Mojo

Russia doesn't appear to be pummeling Ukraine with online attacks, given the ability of the Ukraine government and most of the country to remain online. But Russia appears to be trying very hard to take down Ukraine's internet infrastructure, says Mikko Hypponen, chief research officer at WithSecure.

In a video interview with Information Security Media Group at RSA Conference 2022, Hypponen also discusses:

- Cyber lessons learned so far from the ongoing Russia-Ukraine war;
- How what should count as critical infrastructure may not be obvious before it gets disrupted;
- A preview of his new book, "If It's Smart, It's Vulnerable," which is due to be published in August.

“Ukraine is the best country in Europe to defend their networks against Russian nation-state attacks. Why? Because they've been doing it for eight years.”

- Mikko Hypponen

WATCH ONLINE



Cybersecurity Perspectives

The field of cybersecurity is growing broader every day as technologies, threats, vulnerabilities and geopolitical conditions evolve. A growing number of specializations are emerging that help the industry as a whole stay a little safer. We spoke to a variety of top cybersecurity experts and practitioners about a range of topics including supply chain risk, operational resiliency, cloud and hybrid IT security, data protection, training, and the latest tactics and techniques.

Insights on Financial Supply Chain Compromise

Crane Hassold of Abnormal Security on Latest Financial Crime Research Findings



Abnormal Security is out with new financial crimes research, and it shows that traditional business email compromise is evolving into new forms of financial supply chain compromise. Crane Hassold shares insights on the crimes and how best to detect, deter and respond to them.

WATCH ONLINE

Why Improved Recovery From Cyber Incidents Is Critical

Optiv's Jessica Hetrick Discusses the Need to Focus on Recovery and Resiliency



Ransomware is making it increasingly important for organizations to proactively and comprehensively consider what cyber recovery means. Jessica Hetrick, cyber resilience leader at Optiv, advises understanding technology interdependencies across the business and how to protect them.

WATCH ONLINE

Visibility Into Distributed Cloud Environments

Mike Kiser, Director of Strategy and Standards at SailPoint, on the Evolving Needs



Companies need better visibility into their ever-changing distributed environments "like never before," says Mike Kiser, director of strategy and standards at SailPoint.

[WATCH ONLINE](#)

How Can We Fill the Cybersecurity Education Gap?

CTO Daniele Catteddu on Industry's Outdated Approach to Training



CTO Daniele Catteddu of the Cloud Security Alliance sees significant gaps in how the cybersecurity industry delivers education and training. For example, he says, while organizations are demanding Zero Trust services and guidance on implementation, the industry's offerings do not meet that demand.

[WATCH ONLINE](#)

Despite Fervor for the Cloud, Here's Why Hybrid Is Forever

Richard Bird on Cloud and Hybrid Realities, Control Domains and Managing Identity



Cloud has a dirty little secret: While most say moving to cloud is inevitable, not everything today can or even should run in the cloud, says SecZetta's Richard Bird. He explains why hybrid approaches are here to stay and how security teams must respond, especially when it comes to identity.

[WATCH ONLINE](#)

Expanding Beyond Cybersecurity to Take on Digital Trust

Mark Brown, BSI Group Global Managing Director, on What Compromises Digital Trust



BSI Group has expanded its consulting practice beyond just cybersecurity to take on broader questions around digital trust, helping customers address everything from digital supply chain risk to the ethics of artificial intelligence, according to Mark Brown, global managing director for digital trust consulting.

[WATCH ONLINE](#)



Chase Cunningham
CSO,
Ericom Software

Cyberwarfare Strategy and How It Applies to Businesses

Chase Cunningham of Ericom on the Need to Appreciate the Adversaries' Perspectives

Cyberwarfare has emerged as the bridge between espionage and kinetic conflict. "It's here," says Chase Cunningham of Ericom Software. He discusses how enterprise cybersecurity leaders should now think more deeply about their adversaries' motivations and capabilities.

In a video interview with Information Security Media Group at RSA Conference 2022, Cunningham also discusses:

- Technology's evolution;
- Perfect vs. realistic security;
- How small to midsize organizations can still enjoy enterprise-level defenses.

“Cyberwarfare is the bridge between espionage and kinetic operations. This is it. We’re here. Know that it’s a real thing.”

- Chase Cunningham

WATCH ONLINE

How to Proactively Build Privacy Into Products

Chief Privacy Officer **Robin Andruss** on Skyflow's Unique Approach to Data Privacy



Organizations need to ensure the push to maximize profits doesn't jeopardize the privacy of user information. Skyflow Chief Privacy Officer Robin Andruss says businesses need to maintain guardrails around customer data in the face of massive technological change.

WATCH ONLINE

Legal and Litigation Trends in 2022

Troutman Pepper's **Ronald Raether** on Why Collaboration Is Key



Ronald Raether of Troutman Pepper says privacy, data security and information governance departments must collaborate to reduce unauthorized access to systems by criminals and make data operationalization more effective. He also says proper data mapping, governance and classification are critical.

WATCH ONLINE

Essential Steps for Building a Risk Management Program

Randy Trzeciak on How Insider Threats Have Changed



When building an insider risk management program, don't start "too large or too quickly," says Randy Trzeciak of Carnegie Mellon University. He says the first step is to protect your organization's critical assets and services and then "build a risk program appropriate to those assets."

WATCH ONLINE

The Future of Authentication Is Biometrics and Passwordless

Forrester's **Merritt Maxim** and **Paul McKay** on How Remote Work Changes Authentication



The need for more modern identity and access management capabilities such as biometric and passwordless authentication has been amplified by the COVID-19 pandemic and the shift to remote work, say Paul McKay, principal analyst, Forrester, and Merritt Maxim, vice president and research director, Forrester.

WATCH ONLINE



Marshall Heilman
Executive Vice President and CTO,
Mandiant

The Switzerland of Security: Why Being Independent Matters

CTO Marshall Heilman on How Mandiant Gets by With a Little Help From Its Friends

Mandiant had the opportunity to become truly vendor-agnostic once the company sold its FireEye products business, since renamed Trellix, to Symphony Technology Group in October, according to executive vice president and chief technology officer Marshall Heilman. Heilman says Mandiant has therefore pursued deep integrations with all the leading vendors in the endpoint security space.

In a video interview with Information Security Media Group at RSA Conference 2022, Heilman discusses:

- Why partnerships are central to Mandiant's strategy;
- The latest integration with CrowdStrike and SentinelOne;
- What getting bought by Google means for the company.

“This is a mission-focused partnership to make sure our customers are getting better outcomes than they would have had beforehand.”

- *Marshall Heilman*

WATCH ONLINE



Nick Warner
President of Security,
SentinelOne

How XDR Is Fulfilling the Promise that SIEM Never Did

SentinelOne President Nick Warner on How Attivo and Scalyr Advanced the XDR Mission

SentinelOne has expanded its detection and response capabilities beyond the endpoint in recent years with the acquisition of data analytics tech developer Scalyr and identity and deception technology vendor Attivo Networks, says Nicholas Warner, president of security.

In a video interview with Information Security Media Group at RSA Conference 2022, Warner also discusses:

- How legacy SIEM systems suffer from using third-party data analytics;
- Why XDR vendors need an active rather than passive alert system;
- How acquiring Attivo will unleash the joint power of security and identity.

WATCH ONLINE

“Because we're running on the control plane, we can immediately take action and respond.”

- Nick Warner



Wendi Whitmore
Senior Vice President and Head of Unit 42,
Palo Alto Networks

Total Business Email Compromise Losses Trump Ransomware

Wendi Whitmore, Head of Palo Alto Networks' Unit 42, Details Latest Attack Trends

Ransomware continues to pummel organizations, with the average ransom payment reaching \$925,000 so far this year, but the aggregate financial impact of business email compromise (BEC) attacks is even worse, says Wendi Whitmore, head of Unit 42 at Palo Alto Networks.

In a video interview with Information Security Media Group at RSA Conference 2022, Whitmore also discusses:

- Threat intelligence teardown and Unit 42's mission;
- Recent ransomware trends;
- How BEC campaigns continue to evolve.

“Ransomware is top of mind and it's involved not only in what's going on in financial crime sectors, but we're seeing much overlap in nation state attacks.”

- *Wendi Whitmore*

WATCH ONLINE

More RSA Conference 2022 Content from ISMG



[Why Implementing Security Technology Is Such a Challenge](#)

Amol Kulkarni of CrowdStrike on Why Companies Must Focus More on Runtime Protection



[Latest Blow Falls on the 'Scourge of Passwords'](#)

FIDO Alliance Director Andrew Shikiar on New Deal With Google, Apple and Microsoft



[Addressing Misconceptions About Cryptography](#)

Entrust's Brad Beutlich on Rethinking Security Spending



[Why Supply Chain Attackers Love Managed Service Providers](#)

Economies of Scale and Automation Drive Attacks, Says Candid Wuest of Acronis



[Looking Beyond Silicon Valley for Cybersecurity Talent](#)

Arctic Wolf Chief Product Officer Dan Schiappa on Finding Good Talent in New Places



[Envisioning a New Model for Information Sharing](#)

Microsoft's Edna Conway on Why the Information-Sharing Model Needs to Change



[How Cloud Security Has Changed in the Age of COVID-19](#)

Omdia's Fernando Montenegro on What Customers Need to Secure Cloud Environments



[The Most Concerning Developments in P2P Payments Fraud](#)

Outseer's Jim Ducharme and MUFG Union Bank's retired Director Ken Palla on Authorized Versus Unauthorized Fraud



[Next-Gen SecOps Demands Advanced Detection and Response](#)

Optiv's John Ayers on How It All Has to Start With the Threat



[Why CISO Is the Most Challenging Role in Cybersecurity](#)

John Horn of Aite-Novarica Group Shares Findings From New Research



[How Security Risks Might Halt the Use of AI in Applications](#)

F5's Kara Sprague on How the Application Security Threat Landscape Has Changed



[Demystifying Managed Detection and Response Services](#)

Lyndon Brown of Pondurance on Questions Customers Must Ask About Modern MDR



[Cybersecurity: Why It's Not Just an 'IT Problem'](#)

Adlumin's Mark Sangster on How Security Is Now a Business Risk to Manage



[Overcoming Digital Challenges of OT Security](#)

Nozomi Networks Sales Director Nycholas Szucko Says Get Back to the Basics

Featuring a member of:

CyberEdBoard



[Attack Paths: Just 4 Steps Can Compromise 94% of Assets](#)

XM Cyber's Paul Giorgi on Using Attack Path Management to Simulate Break-In Points

Interview conducted in

Portuguese



[Managed Detection and Response: It's More Than Endpoints](#)

Rick Miller, COO of GoSecure, on What to Know About MDR



[Techniques to Improve Supply Chain Confidence](#)

Highlights from ISACA's Supply Chain Security Report



[The Security Testing Imperative](#)

Scott Register, VP of Security Solutions at Keysight, on Why Testing Matters



[The Ever-Increasing Pressure to Develop Secure Code](#)

Sonali Shah of Invicti Security Describes the Challenges Developers Face



[Why Zero-Day Attacks on Open-Source Libraries Are Surging](#)

Contrast Security CPO Steve Wilson on Why Log4j Hack Is a Sign of Things to Come



[Extending Encryption and Key Management into the Cloud](#)

Todd Moore, Thales' VP of Encryption Products, On Data Sovereignty and the Cloud



[How MDR Helps to Simplify Complex IT Environments](#)

Tom Powledge, Chief Product Officer at Trustwave, on Advancing MDR



[The State of Phishing and Email Security](#)

Cofense's Tonia Dudley on What's Not Working, Threat Predictions



[Rapid Cybersecurity Changes Demand Agile Education](#)

Hack The Box's Trevor Nelson and Emma Brothers Detail Current Educational Gaps

Watch all 150+ interviews online

View over 150+ interviews with the foremost thought leaders in security today as part of our ongoing coverage of the RSA Conference: www.databreachtoday.com/rsa-conference



Behind the Scenes: iSMG at RSA Conference 2022

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



Left: ISMG Studio set up in Marriott Marquis; below: ISMG's Mathew Schwartz conducts an interview.



Above: ISMG's Mike D'Agostino prepares for the long day of interviews; ISMG's Anna Delaney with Deepwatch's Wesley Mullins





Above, Wendi Whitmore of Palo Alto Networks speaks with ISMG's Mathew Schwarz; below, the ISMG team with Congressman Swalwell.





Above: Michael Novinson interviews Abbas Kudrati of Microsoft, and Upendra Singh of HCL Technologies; left: ISMG's Anna Delaney during an interview.



Above: Someone snaps a quick picture before an interview begins.



Left: ISMG team in the ISMG Studios at Marriott Marquis;
below: ISMG's Michael Novinson with Abbas Kudrati and Upendra Singh



Left: Art Coviello being interviewed by ISMG's Anna Delaney



Above: ISMG Studio setup; below: ISMG's Mike D'Agostino snaps a picture of Allan Liska in front of his next-up graphic..



About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 34 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 and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
info@ismg.io

Sales & Marketing

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

