Infosecurity Europe 2018 Highlights and Insights

Overview of Content Created by ISMG, Including:

- Video Interviews with Industry Leaders
- Articles, Photos and More from the ISMG Team
- Looking Back on the Event

iSMG
INFORMATION SECURITY
MEDIA GROUP

The Best of Infosecurity Europe 2018

Infosecurity Europe is one of the world's most important cybersecurity events. This year's conference was bigger than ever, featuring 240 sessions, more than 400 exhibitors and an estimated 19,500 attendees.

Mathew Schwartz, our European executive editor, conducted dozens of video interviews with security experts from around the globe who gathered at the event in London. His conversations covered a broad range of timely subjects, ranging from compliance with the EU's General Data Protection Regulation to efforts to fight cybercrime worldwide.

The long list of thought leaders who sat down with Mat includes:

- Jaya Baloo, CISO of KPN Telecom, who delivered a keynote presentation on quantum computing;

- Troy Hunt, an Australian data breach expert, who described the worrying rise in credential stuffing attacks;

- Thom Lanford, CISO of Publicis Group, who talked about his organization's approach to GDPR compliance;

- James Lyne of Sophos, who addressed ransomware and new criminal business models;

- Rapid7's Tod Beardsley, who offered highlights from his firm's third annual "National Exposure Index" study of open and unsecured ports on the internet.

So if you weren't able to attend this year's Infosecurity Europe conference, Mat's video interviews offer a valuable opportunity to get caught up on what the experts were talking about at this important event. This handy guide is designed to help you identify the interviews that cover those topics of greatest interest to you. \

Best,

Tom Field
SVP, Editorial
Information Security Media Group
tfield@ismgcorp.com

Visit us online for more Infosecurity Europe 2018 coverage:

https://www.databreachtoday.eu/infosecurity-europe-2018-c-510

Video Interviews

More Content

Stopping Cybercrime: Are Banks Doing Enough?

Fraud Directly Funds Organized Crime, Warns Trusted Knight's **Trevor Reschke**

Should financial services firms be doing more to combat fraud? "I absolutely think they could be doing quite a bit more," says Trevor Reschke of software vendor Trusted Knight.

WATCH ONLINE

Phishing Attacks Get More Targeted

Ironscale's **Brendon Rod** Says 70 Percent of Attacks Target 10 Mailboxes at Most

To block phishing attacks and fraudsters aiming to compromise senior managers' email accounts, organizations need to pay close attention to targeted attacks says Brendon Rod of Ironscale.

WATCH ONLINE

A Year After WannaCry: Lots of Work to Do

Carl Leonard of Forcepoint on Dealing With the Insider Threat

One year after the WannaCry attack, cybersecurity is still failing, and the likelihood of a breach has never been greater, says Carl Leonard of Forcepoint.

WATCH ONLINE

Cybercrime Trends: Cryptojacking, Fileless Attacks

Carbon Black's **Rick McElroy** Describes Latest Attacks and Threat Hunting Tactics

Attackers continue to shift their tactics to help evade improvements in defenses, says Rick McElroy of Carbon Black.

WATCH ONLINE

Behavioral Analytics: Essential for Battling Data Breaches

Juniper's **Nick Bilogorskiy** Discusses Automating Threat Hunting, Incident Response

What's behind the push for behavioral analytics?

In a video interview at the recent Infosecurity Europe conference in London, Bilogorskiy discusses:

- Threat intelligence and incident response;
- Threat hunting;
- Online attack trends, including cryptocurrency-driven threats and exploits of internet-connected devices.

WATCH ONLINE

"For responding to incidents, you need to detect them, and then you need to figure out how to mitigate them. For both of those things, you will need accurate threat intelligence",

Business Process Re-Engineering: Navigating Security Perils

Skybox Security's **Justin Coker** Outlines Top Challenges

Recent failures of IT systems at some major airports and banks are a reminder that as an organization launches a digital transformation project, or seeks to move more of its processes to the cloud, those efforts won't necessarily proceed smoothly or securely, says Skybox Security's Justin Coker.

In a video interview at the recent Infosecurity Europe conference in London, Coker discusses:

- Visibility: Understanding an organization's attack surface;
- The challenge posed by digital transformation, mergers and acquisitions and moving to the cloud;
- Effective communication between CISOs and the C-suite.

WATCH ONLINE

CISO Thom Langford's Top Tips for GDPR Compliance

Start With ISO 27001 and a Solid Information Security Management System

Three years ago, communications giant Publicis Groupe launched its EU General Data Protection Regulation compliance project, says Thom Langford, who describes lessons learned.

WATCH ONLINE

Why Security Is Crucial for Digital Transformation Success

BlackBerry's **Florian Bienvenu** on Device Management, Collaboration, Cyber Hygiene

Organizations are increasingly turning to devices and the cloud to foster better collaboration and access to essential data. But as they do so, "the number one blocker for enabling digital transformation is security," warns Florian Bienvenu of BlackBerry.

WATCH ONLINE

Enterprise IT/OT: Better Collaboration, But Not Perfect

Groups Increasingly Share Responsibilities, Says Tripwire's **Tim Erlin**

Internet-connected devices inside the enterprise: There are many more than people might think. But they're not always under the direct control of IT departments, says Tim Erlin of Tripwire.

WATCH ONLINE

Beyond Correlation Rules: How to Build a Better SIEM

Profiling User Behavior Is Key, Says Exabeam's **Derek Lin**

Organizations have been using security information management - and later, security information and event management - for a long time. But these SIMs and SIEMS can, and must, be improved by bringing automation, orchestration and machine learning techniques and tactics to bear, says Derek Lin of Exabeam.

WATCH ONLINE

Security: Ounce of Prevention Still Worth a Pound of Cure

Check Point's **Gad Naveh** Offers Post-WannaCry and NotPetya Security Essentials

The prevalence and scale of data breaches continues to increase. "We are indeed seeing more attacks, but also the sophistication and spread of them is much larger," says Gad Naveh of Check Point.

In a video interview at the recent Infosecurity Europe conference in London, Naveh discusses:

- The rise of "gen 5" attacks that compromise entire business sectors;
- Nation-state attacks such as WannaCry and NotPetya;
- The need for a much greater focus on preventing attacks.

Organizations need to focus much more on preventing attacks, especially to combat the rise in "mega attacks that attack the whole business sector of certain states."

Better Incident Response: Let's Get Surgical

Darktrace's **Dave Palmer** on Disrupting Attacks While Maintaining Productivity

As organizations detect more breaches, incident responders are increasingly overloaded, says Darktrace's Dave Palmer.

In a video interview at the recent Infosecurity Europe conference in London, Palmer discusses:

- The evolution of incident response, especially as breach detection continues to improve;
- The increased use of orchestration - playbooks for machines to execute on incident responders' behalf - and where such automation most likely will help;
- The need to develop more surgical incident response capabilities to help maintain business productivity and system uptime.

"Only a few years ago, it wasn't that unusual to hear people say to their boards: 'We've got a clean network; there have been no infections.' And it's unimaginable to be saying that to senior leadership today."

WATCH ONLINE

How Contextual Data on Domains Helps Combat Online Attacks

Michael Jones of Domain Tools on Scoring Threats, Blocking Phishing Attacks

Studying domain ownership gives organizations "contextual data around domains that may be attacking them," says Michael Jones of Domain Tools.

WATCH ONLINE

Ransomware: No Longer Sexy, But Still Devastating

James Lyne of Sophos Rounds Up the Latest Cybercrime Trends and Defenses

We need to talk about ransomware, says James Lyne of Sophos, who emphasizes that it still represents a serious threat.

WATCH ONLINE

Fighting Malware: Why Speed Is More Important Than Ever

Lastline's **Patrick Bedwell** on Malware-as-a-Service and Breach Trends

To stop malware, it helps to spot it as fast as possible and keep tabs on what it might be trying to do, says Patrick Bedwell of Lastline.

WATCH ONLINE

Geopolitical Instability Is CISOs' Latest Challenge

KPN Telecom's **Jaya Baloo** on Technology, Politics and Software Vendor Bans

The latest challenge to face chief information security officers: Keeping their organizations secure while at the same time navigating geopolitical instability, says Jaya Baloo of KPN Telecom.

WATCH ONLINE

Buzzword Bingo: Quantum, AI, Blockchain, Crypto

Thales e-Security's **Jon Geater** Separates Hype From Utility

Quantum computing, blockchain, crypto, internet of things: There's a lot of hype around these technology areas, says Jon Geater of Thales e-Security. So it's essential to pierce the hype and see what's useful and applicable for practitioners, he stresses.

In a video interview at the recent Infosecurity Europe conference in London, Geater discusses:

- What quantum computing, artificial intelligence, blockchain and other hot topics mean for information security in the real world;
- Why these technologies are being forced into focus now;
- Takeaways for practitioners.

WATCH ONLINE

"It's important to cut through ... the kind of general sense of doom that we hear about how the robots are going to take over the world or about how cryptocurrency is going to replace all governments period."

Data Breach Trends: Attackers' Dwell Time Decreases, Mostly

But Some EMEA Organizations Weren't So Lucky, Says Mandiant's **Mike Trevett**

There's data breach good news and bad news for organizations in Europe, the Middle East and Africa, says Mike Trevett of FireEye's Mandiant. In general, attackers are dwelling in networks for less time before being discovered, except for some particularly long-lasting breaches in EMEA, he says, drawing on the most recent M-Trends report from Mandiant.

In a video interview at the recent Infosecurity Europe conference in London, Trevett discusses:

- Data breach trends;
- Attackers' preference of conducting reconnaissance and data exfiltration;
- The prevalence of repeat attacks - victims getting hit multiple times;
- How cyberattack volumes from Iran and North Korea have been increasing, with attacks from Russia and China emaining constant.

WATCH ONLINE

Credential Stuffing Attacks: How to Combat Reused Passwords

Troy Hunt Describes Efforts to Build and Store Better Passwords

For attackers, "credential stuffing" is the gift that keeps on giving, says information security researcher Troy Hunt, founder of the free Have I Been Pwned? breach-notification service.

WATCH ONLINE

Nation-State and Cybercrime Gangs: Lines Blur

CrowdStrike's **Zeki Turedi** Discusses Pseudo-Ransomware, False Flags, Leaked Toolkits

In the past 12 months, there's been a blistering series of high-impact attacks, including a marked increase in pseudo-ransomware attacks and supply chain subterfuge. "It's been a very interesting year from a cyber perspective," says Zeki Turedi of CrowdStrike, who highlights "the blurred lines between statecraft and criminal organizations."

WATCH ONLINE

Email-Borne Security Threats: Sophistication Increases

Barracuda's **Hatem Naguib** on Ransomware, Phishing, Cloud Account Takeover

Email attacks continue to bite businesses, says Natem Naguib of Barracuda, who talks about the latest sophisticated strategies.
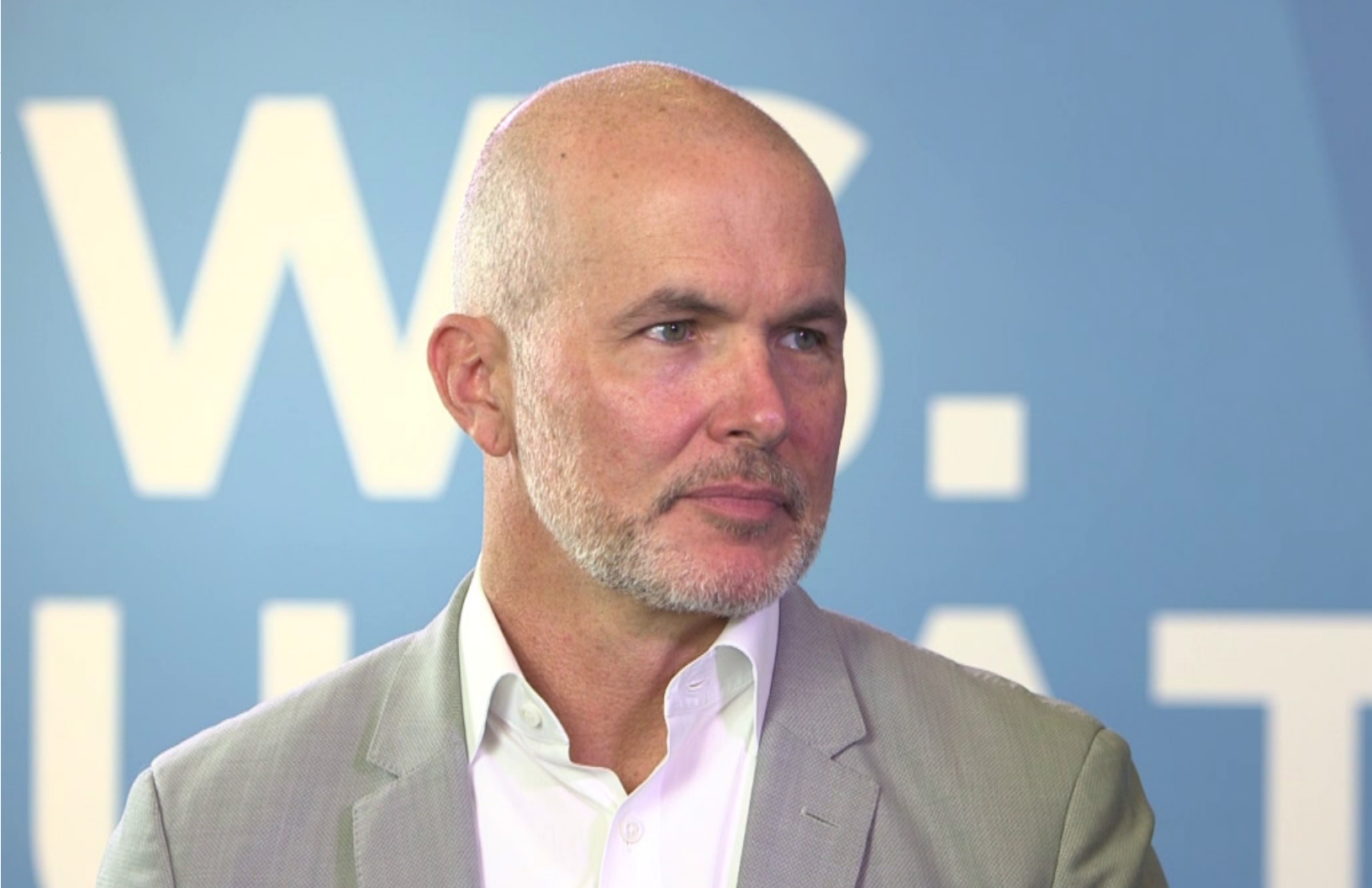
WATCH ONLINE

Data Governance Best Practices in the GDPR Era

Matt Lock of Varonis on the Need to Have a Baseline for Data Access Behavior

Organizations that must comply with the EU's General Data Protection Regulation are now compelled to ensure they're handling personally identifiable information in a legal manner, says Matt Lock of Varonis.

WATCH ONLINE

Improving Network Visibility

Wallace Sann of ForeScout on Keeping Up With the Growth of Network-Connected Devices

The explosion in the growth and diversity of devices linked to networks as a result of the internet of things and BYOD makes it more challenging to manage network security, says Wallace Sann of ForeScout.

In a video interview at the recent Infosecurity Europe conference, Sann discusses:

- The convergence of IT and OT;
- The difficulty in identifying all devices on a network;
- The impact of cloud computing on visibility issues.

WATCH ONLINE

Why Data Classification Has Gone Mainstream

Regulations Such as GDPR Drive More Classification, Says **Tony Pepper** of Egress

Driven by the EU's General Data Protection Regulation and other regulations, as well as the move to the cloud, more organizations are turning to data classification, says Tony Pepper, CEO of Egress.

In a video interview at the recent Infosecurity Europe conference in London, Pepper discusses:

- Protecting unstructured data;
- Starting small: Why it's never too late to start classifying data;
- How regulations, including GDPR, are leading more organizations to classify data.

WATCH ONLINE

Incident Response Challenge: Knowing What to Prioritize

IBM's Mike Spradbery on Triage, Machine Learning, Tennis

Much of the push for bringing artificial intelligence - often better known as machine learning - tactics to bear in information security has been to help security experts know where to focus and to much more quickly glean this information, says Mike Spradbery of IBM.

WATCH ONLINE

Challenges for SOCs: People, Process, Technology

Cyberproof's Adrian Bisaz Describes How Security Operations Centers Must Evolve

Running a security operations center today remains a "challenging operation," not only when it comes to the required technology, but also people and processes, says Adrian Bisaz of Cyberproof.

WATCH ONLINE

Battling Alert Fatigue

Robert Hamilton of Imperva on the Role of Artificial Intelligence

Security alert fatigue is a growing concern, leading to difficulties sorting out false positives from alerts worth investigating, says Robert Hamilton of Imperva.

WATCH ONLINE

Defenders Must Think Like Attackers

Online Attacks Increasingly Target Users, Warns Proofpoint's **Adenike Cosgrove**

Never underestimate the human factor in attacks. Indeed, especially as organizations shift more resources to the cloud, many of today's top attacks - from malware to phishing - will require some level of interaction from victims. But attackers, using services such as LinkedIn and Google, and becoming better and better armed.

In a video interview at the recent Infosecurity Europe conference in London, Cosgrove discusses:

- How threat actors are increasingly targeting people, not infrastructure;
- The gap between how security teams view their organization and how attackers approach their targets;
- How to stop today's increasingly specialized, socially engineered cyberattacks across email, social media channels and cloud applications.

READ ONLINE

How Orchestration and Automation Help Incident Responders

IBM Resilient's **Allen Rogers** on Breach Response Essentials for the GDPR Era

The EU's General Data Protection Regulation is already having an impact on how organizations approach data breach detection and remediation, says Allen Rogers of IBM Resilient.

In a video interview at the recent Infosecurity Europe conference in London, Rogers discusses:

• Faster response to breaches or suspected breaches;
• The automation and orchestration imperative;
• How breach notification requirements, including GDPR, will increasingly impact organizations' approaches to privacy and breach response.

WATCH ONLINE

GDPR: UK Privacy Regulator Open to Self-Certification

Focus on Continuous Compliance and Breach Response, Experts Say

Organizations in Europe may eventually be able to self-certify that they are compliant with the EU's General Data Protection Regulation, an official at the U.K.'s independent privacy watchdog said.

READ MORE

10 Hot Sessions: Infosecurity Europe in London

Cybersecurity Conference Tackles Cybercrime, AI, Breach Response, Privacy, GDPR

Hot topics at this year's Infosecurity Europe conference in London ranged from artificial intelligence and breach response to GDPR and battling cybercriminals and nation-states.

READ MORE

Visual Journal: Infosecurity Europe 2018

Cybersecurity Conference Tackles GDPR, Cybercrime, Nation-State Attacks and More

Here are visual highlights from this year's event, which featured 240 sessions, 400 exhibitors and an estimated 19,500 attendees.

WATCH ONLINE

About ISMG

Information Security Media Group (ISMG) is the world's largest media organisation devoted solely to information security and risk management. Each of our 28 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

BANK**i**NFO SECURITY®   CU**i**NFO SECURITY® *Just for Credit Unions*   GOV**i**NFO SECURITY®   HEALTHCARE**i**NFO SECURITY®

*i*nfoRisk® TODAY   CAREERS**i**NFO SECURITY®   Data Breach. *Prevention. Response. Notification.* TODAY   Cyber**Ed**.*io*

*i*SMG
INFORMATION SECURITY
MEDIA GROUP