



Infosecurity Europe 2019 Highlights and Insights

Video Interviews With Industry Leaders and Review of Keynote Sessions

The Best of Infosecurity Europe 2019



Welcome to ISMG's compendium devoted to the hottest topics and most compelling speakers from Europe's premier cybersecurity event. Spanning insider threats and nonstop data breaches, to the latest business-efforts to arrest fraud, malicious insiders and advanced hack attacks, and much more, we have you covered.

As a media sponsor of Infosecurity Europe 2019, ISMG was at the center of the dialogue both at and around the event.

Once again, we returned to the Infosecurity Europe show floor with an open studio amidst the exhibitors and myriad attendees. Sitting down with dozens of the industry's leading vendors, practitioners and influencers, we gathered expert insight into the cybersecurity topics and strategies that matter most today.

All told, we conducted more than 40 exclusive video interviews with a selection of the industry's top thought leaders, including CEOs, CISOs, analysts, researchers and educators.

Conference keynote speaker Troy Hunt, founder of the Have I Been Pwned? service, analyzed for us the nonstop rise of data breaches. Distinguished security researchers – including Raj Samani, Chester Wisniewski and Tod Beardsley – detailed the latest threats and how business must respond. Other leading technology thinkers shared the latest on business adoption of machine learning and artificial intelligence, the quest to block privileged account takeovers and phishing attacks, techniques for securing supply chains, and among many other topics, digital transformation, automation, DevSecOps as well as the growing use of red teams and bug bounties.

As the preeminent cybersecurity conference in the region, Infosecurity Europe again cemented its reputation as being the place where those in Europe and the United Kingdom come to talk cybersecurity. Dive into the pages that follow for highlights from the discussion.

Best,

A handwritten signature in black ink that reads "MJ Schwartz". The "MJ" is stylized and followed by the name "Schwartz" in a cursive script.

Mathew J. Schwartz
Executive Editor, DataBreachToday and Europe
Information Security Media Group
mschwartz@ismgcorp.io

Visit us online for more Infosecurity Europe coverage:

www.databreachtoday.co.uk/infosecurity-europe-2019-c-510



Video Interviews

Act Fast: Best Practices for Arresting Spoofed Domains Corin Imai, <i>DomainTools</i>	The Need for a 'Zero Trust' Approach Pete Nourse, <i>Veriato</i>
4	15
Compliance in a Hybrid Environment Don Closser, <i>Firemon</i>	Filling the Cybersecurity Skills Gap Giovanni Vigna, <i>Lastline</i>
4	15
Empower Employees While Preventing Insider Data Breaches Tony Pepper, <i>Egress</i>	The State of the SOC Stephen Moore, <i>Exabeam</i>
5	15
Best Practices for Session-Based Fraud Detection/Prevention Tim Ayling, <i>Kaspersky</i>	The Scourge of Commodity Malware Assaf Dahan, <i>Cybereason</i>
6	16
4 Bug Bounty Myths Dispelled Laurie Mercer, <i>HackerOne</i>	Troy Hunt: Why Data Breaches Persist Troy Hunt, <i>Have I Been Pwned</i>
7	16
Enhancing Security by Red Teaming James Stranger, <i>CompTIA</i>	Improving IoT Risk Management Tim Mackey, <i>Synopsis</i>
7	16
Securing the Software Supply Chain Ilkka Turunen, <i>Sonatype</i>	Privileged Attack Vectors: Key Defenses Karl Lankford, <i>BeyondTrust</i>
7	16
Cisco on Cybersecurity: Targeting Optimal Protection Mark Weir, <i>Cisco</i>	Proactive Mitigation: A Cybersecurity Imperative Jay Coley, <i>Akamai</i>
7	17
Fusing Security With Digital Transformation for SMBs Tim Wilkinson, <i>Avast Business</i>	The Challenge of Secure Coding Jeff Williams, <i>Contrast Security</i>
8	18
The Pervasive Problem of Phishing Lior Kohavi, <i>Cyren</i>	Beyond Bug Bounties: Crowdsourced Security Testing Evolves David Baker, <i>Bugcrowd</i>
9	19
Using AI to Detect Cyber Risks David Atkinson, <i>Senseon</i>	Do You Know What Cloud Assets You Actually Have? Sam Curcuruto, <i>Expanse</i>
9	20
Life Beyond Blocking: Adopting Behavior-Based Cybersecurity Carl Leonard, <i>Forcepoint</i>	GDPR: Where Do We Go From Here? Thom Langford, <i>TL² Security</i>
9	21
Protecting Against Automated Attacks Dan Woods, <i>Shape Security</i>	The Role of DNS in Cybersecurity Stuart Reed, <i>Nominet</i>
9	21
Best Practices for Cyberattack Prevention and Response Andrew Gogarty, <i>Secon Cyber</i>	Mitigating Insider Threats With IAM Andrew Clarke, <i>One Identity</i>
10	21
Network Security Policy Management: Seeking Visibility Jeffrey Starr, <i>AlgoSec</i>	Reinventing Application Security Bob Egner, <i>Outpost24</i>
10	21
Step Away From the Artificial Intelligence John Matthews, <i>ExtraHop</i>	Hacked With Words: Email Attack Sophistication Surges Michael Flouton, <i>Barracuda</i>
10	22
Cloud and Container Adoption: The Visibility Imperative Marco Rottigni, <i>Qualys</i>	Risk and Resilience: Finding the Right Balance Nik Beecher, <i>Leonardo</i>
10	22
Addressing the Human Element in Cybersecurity James Mackay, <i>MetaCompliance</i>	Cyberattack Risk: Scans Find Big Businesses Exposed Tod Beardsley, <i>Open Ports</i>
11	22
How IT, OT Teams Can Collaborate Kim Legelis, <i>Nozomi Networks</i>	How to Block Advanced Threats John McClurg, <i>Blackberry Cylance</i>
12	23
Top Drivers for Privileged Account Management Grant Burst, <i>Wallix</i>	Are You APT-Ready? The Role of Breach and Attack Simulation Tim Ager, <i>Cymulate</i>
13	24
The Expanding Digital Attack Surface Brent Davidson, <i>ZeroFOX</i>	Beyond Opportunistic: How the Threat Landscape Is Evolving Chester Wisniewski, <i>Sophos</i>
14	25
Cybersecurity's Automation Imperative Richard Walters, <i>Censornet</i>	
15	

More Content

10 Highlights: Infosecurity Europe 2019 Keynotes	26
--	----

Welcome to ISMG Studios at Infosecurity Europe 2019

MATHEW SCHWARTZ, EXECUTIVE EDITOR, ISMG

Information Security Media Group's editors staffed our exclusive video studio on the Infosecurity Europe show floor, where we produced more than 40 interviews with the global cybersecurity industry's leaders. Joining me to conduct these interviews was my colleague Nick Holland. Among the conversations were one-on-ones with Infosecurity Europe keynote speakers and hall of fame honorees, sponsors and speakers, covering topics ranging from regulations and breach trends to the latest technology and CISO business strategies.

Act Fast: Best Practices for Arresting Spoofed Domains

Corin Imai of DomainTools on the Quest to Block Bad Domains



Organizations are increasingly relying on threat intelligence to help them better identify malicious behavior before it hits the network - or users encounter it - including using domain name system analysis to track emerging campaigns, says Corin Imai of DomainTools.

WATCH ONLINE

Compliance in a Hybrid Environment

Don Closser of Firemon Shares Insights on New Issues in New Era



How can organizations deal with compliance issues in a hybrid environment? Don Closser of Firemon discusses compliance in the age of cloud computing.

WATCH ONLINE



Tony Pepper,
CEO, Egress

Empower Employees While Preventing Insider Breaches

Make Technology Your Last Line of Defense, Says **Tony Pepper** of Egress

Carelessness and a lack of awareness are root causes of insider breaches. So says Tony Pepper, CEO of Egress, based on the findings of a study his company conducted of CISOs and employees to trace the cause of insider breaches resulting from both intentional and unintentional loss.

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

- Key findings from the Egress research, including a significant CISO/employee disconnect;
- The mandate for a more people-centric approach to security - and what it looks like;
- Targeting the insider threat by using machine-learning capabilities to better spot anomalies;
- Right-sizing encryption and ensuring technology provides a last line of defense.

“Quite frankly, the market has never really deeply understood what's causing these breaches of data security, and, more importantly, why are they actually going in the wrong direction - why are data security breaches going up, when it seems like investment in IT and IT security is going up as well?”

WATCH ONLINE



Tim Ayling
Global Vice President - Fraud Prevention Solutions, Kaspersky

Best Practices for Session-Based Fraud Detection/Prevention

Kaspersky's **Tim Ayling** on Session-Based Tools Serving as 'Early Warning' System

Numerous industries, including financial services, rely on transaction-based controls to help spot and block fraud. But increasingly, organizations are also using session-based fraud detection and prevention, says Kaspersky's Tim Ayling.

“Transaction monitoring works - it works quite well. But nevertheless, there's still a lot of fraud out there.”

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

- Why and how adoption of session-based fraud detection has been increasing across multiple sectors;
- Top factors examined by session-based fraud analysis;
- How much fraud is acceptable - and how many industries understand that it cannot be eradicated.

WATCH ONLINE

4 Bug Bounty Myths Dispelled

HackerOne's **Laurie Mercer** Takes Down Common Misconceptions



Bug bounty myths: All such programs must be public, run nonstop, pay cash to bug-spotters and allow anyone to join. Laurie Mercer says that, in fact, bug bounty and vulnerability disclosure programs are often run as private, invitation-only and time-limited endeavors. In addition, while the average program reward is \$600 for finding a significant bug, sometimes simply publicly thanking bug hunters or offering cool swag can suffice as rewards.

WATCH ONLINE

Enhancing Security by Red Teaming

James Stanger of CompTIA on Improving Security Controls



James Stanger, chief technology evangelist at CompTIA, explains why red teaming can prove highly beneficial in improving organizational security controls. In a video interview at the recent Infosecurity Europe conference, Stanger discusses the role of red teams, and how security teams can make the transition from a compliance-based mentality to a focus on detecting traces and signatures.

WATCH ONLINE

Securing the Software Supply Chain

Ilkka Turunen of Sonatype on Addressing Vulnerabilities



What steps can be taken to eliminate vulnerabilities in the software supply chain? Ilkka Turunen of Sonatype offers practical insights. Turunen discusses why the way software is built is problematic, security issues raised by the reliance on open source code and the need for faster reaction time to supply chain attacks.

WATCH ONLINE

Cisco on Cybersecurity: Targeting Optimal Protection

Mark Weir Talks Threats, Skills Development and Incident Response Priorities



Cybersecurity truism: Defending organizations against attackers is more challenging than ever. "The complexity and sophistication of the threats has increased," says Mark Weir, Cisco's director of cybersecurity for the U.K. and Ireland. "What we're seeing a lot of at the moment as well is intellectual property theft."

WATCH ONLINE

A portrait of Tim Wilkinson, a middle-aged man with short brown hair, wearing a dark blue blazer over a light blue and white checkered shirt. He is looking slightly to his right with a thoughtful expression. The background is dark and out of focus, with some horizontal light streaks.

Tim Wilkinson
Sales Leader UK&I, Avast Business

Fusing Security With Digital Transformation for SMBs

Tim Wilkinson of Avast Business Discusses Strategic Efforts

Digital transformation impacts the way that organizations deal with cybersecurity risk, says Tim Wilkinson of Avast Business, who provides advice how to place security at the center of the transformation.

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

- Why the move toward digital transformation presents greater challenges in terms of security;
- What organizations need to do to put security at the center of their digital transformation efforts;
- How organizations can stay one step ahead.

WATCH ONLINE

“The challenge is how do we make the digital transformation a reality while maintaining the trust of our customers?”

The Pervasive Problem of Phishing

Lior Kohavi of Cyren Discusses How Attacks Are Becoming More Evasive



Phishing attacks are becoming actively evasive, says Lior Kohavi of Cyren, who discusses countermeasures.

WATCH ONLINE

Using AI to Detect Cyber Risks

David Atkinson of Senseon Discusses Key Benefits of Artificial Intelligence



Artificial Intelligence is coming of age as a key tool in the security analyst's arsenal, says David Atkinson, founder and CEO of Senseon, who highlights key benefits of the technology.

WATCH ONLINE

Life Beyond Blocking: Adopting Behavior-Based Cybersecurity

Forcepoint's **Carl Leonard** Says More Real-Time Response to Behavior Required



To arrest incoming malware, users browsing to bad sites or phishing attack attempts, among other threats, many cybersecurity tools are designed to block or allow specific activities based on prescribed rules, says Carl Leonard of Forcepoint.

WATCH ONLINE

Protecting Against Automated Attacks

Dan Woods of Shape Security on How Enterprises Should Mitigate Risks



Dan Woods, vice president of Shape Security, outlines what enterprises can do to protect themselves against automated attacks.

WATCH ONLINE

Best Practices for Cyberattack Prevention and Response

Secon Cyber's **Andrew Gogarty** Describes High-Impact Risk Reduction Strategies



Organizations that want to ensure they have a solid cybersecurity strategy must ensure they rigorously pursue best practices, monitor their infrastructure, eliminate vulnerabilities as well as prepare for the worst, says Andrew Gogarty of Secon Cyber.

WATCH ONLINE

Network Security Policy Management: Seeking Visibility

AlgoSec's **Jeffrey Starr** Says IT Environments Ever More Heterogeneous and Complex



Visibility, or a lack thereof, continues to challenge organizations as they attempt to protect their businesses by knowing which systems, applications and data they have, says Jeffrey Starr of AlgoSec, who details how centralized visibility, control and automation can help.

WATCH ONLINE

Step Away From the Artificial Intelligence

ExtraHop's **John Matthews** Decries AI Buzzwords in the Era of Machine Learning



Machine learning is a proven technique for helping organizations to improve their security posture because it helps automate whatever can be automated. "Machine learning is a way to use technology that allows you to do more with less," says John Matthews, CIO of ExtraHop Networks.

WATCH ONLINE

Cloud and Container Adoption: The Visibility Imperative

Marco Rottigni of Qualys on Business Best Practices for Digital Transformation



As organizations pursue digital transformation initiatives backed by new application deployment techniques, they must ensure that security, operations and development teams fully coordinate, says Marco Rottigni of Qualys.

WATCH ONLINE



James MacKay,
Chief Revenue Officer, MetaCompliance

Addressing the Human Element in Cybersecurity

James Mackay of MetaCompliance Discusses Building Better Risk Awareness Among Employees

James Mackay of MetaCompliance explains techniques for educating and motivating employees to be more aware of cyber risks.

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

- How the human element in cybersecurity is changing;
- Common trends witnessed when it comes to the human risk element;
- What has worked most effectively in educating and motivating employees to be more cyber risk aware.

“Ninety percent of breaches are happening as a result of a phishing attack.”

WATCH ONLINE



Kim Legelis,
CMO, Nozomi Networks

How IT, OT Teams Can Collaborate

Kim Legelis of Nozomi Networks on Industrial Cybersecurity Teamwork

How can IT and OT teams collaborate to address urgent cybersecurity issues? Kim Legelis of Nozomi Networks offers insights.

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

- Changes in industrial cybersecurity in recent years;
- How organizations are protecting themselves;
- How IT and OT teams can improve collaboration.

“IT security is about confidentiality, integrity and availability. In the OT side of the business, it’s about availability, availability and availability.”

WATCH ONLINE

A portrait of Grant Burst, a man with a beard and mustache, wearing a black polo shirt. He is looking slightly to the left of the camera with a neutral expression. The background is a dark blue, out-of-focus pattern of light streaks.

Grant Burst,
Pre-Sales Engineer & Cybersecurity Expert, Wallix

Top Drivers for Privileged Account Management

Grant Burst of Wallix Says Operational Technology Driving More PAM Rollouts

When it comes to drivers for implementing and maintaining privileged access management programs, Wallix's Grant Burst says that demonstrating compliance and safety remain top priorities.

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

- Key business challenges being faced by his customers;
- Best practices for outsourcing PAM projects;
- The importance of securing critical assets.

“When we're looking at the OT [operational technology] sector, when we're looking at power, water, manufacturing, these are all solutions that we never even thought about before needing this.”

WATCH ONLINE



Brent Davidson,
VP, International, ZeroFOX

The Expanding Digital Attack Surface

Brent Davidson of ZeroFOX Discusses New Cybersecurity Threats

The attack surface is expanding across social media channels and via employee risk. Brent Davidson of ZeroFOX discusses risk mitigation strategies.

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

- A new category of cybersecurity risks in the digital realm;
- The implications of these new digital risks;
- Risk mitigation strategies.

WATCH ONLINE

“From a cyber perspective, the digital channels are now inbound vulnerability risks for organizations.”

Cybersecurity's Automation Imperative

Censornet's **Richard Walters** on the Role of Autonomous Security



With cybersecurity becoming ever more difficult to monitor and manage, and product and data overload triggering cyber fatigue among cybersecurity professionals, organizations must adopt more autonomous approaches, says Richard Walters of Censornet.

WATCH ONLINE

The Need for a 'Zero Trust' Approach

Pete Nourse of Veriato Discusses Shifting to a New Mindset



The perimeter is now both external and internal, which is why organizations must move to a "zero trust" model, says Pete Nourse of Veriato.

WATCH ONLINE

Filling the Cybersecurity Skills Gap

Giovanni Vigna of Lastline Describes New Ways to Acquire Fresh Talent



Gamification can play an important role in addressing the cybersecurity skills shortage, says Giovanni Vigna of Lastline.

WATCH ONLINE

The State of the SOC

Stephen Moore of Exabeam Outlines Key Security Operations Center Challenges



Managing a security operations center is fraught with challenges, says Stephen Moore of Exabeam, who outlines the findings of a new "State of the SOC" report.

WATCH ONLINE

The Scourge of Commodity Malware

Assaf Dahan of Cybereason Analyzes Techniques



Assaf Dahan, head of threat research for Cybereason, describes why most malware can be attributed to a small number of techniques.

WATCH ONLINE

Troy Hunt: Why Data Breaches Persist

More Data, Use of the Cloud and IoT Presage Even More Big, Bad Breaches



Bad news for anyone who might have hoped that the data breach problem was getting better. "I'm just seeing a massive rate recently of breaches" of many different styles and sizes across seemingly every sector, says Troy Hunt, the Australian security researcher who created the free Have I Been Pwned? breach-notification service.

WATCH ONLINE

Improving IoT Risk Management

Tim Mackey of Synopsys on the Need to Tackle Security at the Design Phase



Managing risk for internet of things devices must start early in the design phase, says Tim Mackey of Synopsys, who offers insights on key risk mitigation steps, including building a threat model.

WATCH ONLINE

Privileged Attack Vectors: Key Defenses

BeyondTrust's **Karl Lankford** on Mitigating the Unmanaged Privilege Threat



Attackers crave insider-level access to IT infrastructure, and to get it, they regularly target insiders - and especially anyone with "super user" or admin-level access - to steal their credentials, says Karl Lankford of BeyondTrust.

WATCH ONLINE



Jay Coley,
Security Director, Akamai

Proactive Mitigation: A Cybersecurity Imperative

Jay Coley, Akamai on Blunting Hackers by Blocking Emerging Types of Attacks

A top cybersecurity imperative for organizations is to "take proactive mitigation before an event even occurs," says Akamai's Jay Coley.

In a video interview at Infosecurity Europe conference, Coley discusses:

- Emerging attack trends;
- The need for more automated responses;
- With attack types always evolving, how defensive capabilities must evolve.

WATCH ONLINE

"Attackers really have to see a return on investment when they're operating. So the more frequent attacks we see are the ones still having a good return on investment for their efforts. When the attacks become less effective, they start to drop off."



Jeff Williams,
Co-Founder & CTO, Contrast Security

The Challenge of Secure Coding

Jeff Williams of Contrast Security on Why Application Security Is So Critical

In today's highly connected, cloud-based environment, application security is more critical than ever, says Jeff Williams of Contrast Security, who explains why.

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

- Why application security is so important right now;
- What kinds of apps are the most vulnerable to attack;
- The definition and role of DevSecOps.

WATCH ONLINE

“Frankly we’re not very good at writing secure code.”



David Baker,
CSO, Bugcrowd

Beyond Bug Bounties: Crowdsourced Security Testing Evolves

Bugcrowd's **David Baker** on Targeted 'Researcher Grants,' Waning 'Crowd Fear'

Crowdsourced bug bounty programs help organizations identify severe flaws in their IT infrastructure, apps or other code. Now, that model is being used to help organizations perform more widespread security testing, including penetration testing as well as deep dives by single researchers, says Bugcrowd CSO David Baker.

“Traditionally ... you've had a large group of people sort of gamified - the first one to find a bug gets paid, and so that tends to work very well.”

In a video interview at Infosecurity Europe conference, Baker discusses:

- The state of the crowdsourced security testing market;
- The evolution in trust as well as reward mechanisms;
- The role of penetration testing.

WATCH ONLINE

A portrait of Sam Curcuruto, a man with short dark hair and a light beard, wearing a light pink button-down shirt. He is looking slightly to his left with a neutral expression. The background is a dark blue with abstract, glowing light patterns.

Sam Curcuruto,
Director, Product Marketing Solutions, Expanse

Do You Know What Cloud Assets You Actually Have?

Sam Curcuruto of Expanse on the Role of Cloud Governance in Maintaining Control

Many organizations struggle to understand what cloud assets they actually have. Sam Curcuruto of Expanse explains the role cloud governance plays in gaining better clarity and control.

In a video interview at Infosecurity Europe conference, Curcuruto discusses:

- The level of disconnect between what cloud assets organizations think they have and how many are actually there;
- Examples of this discrepancy;
- How cloud governance can help address the problem.

WATCH ONLINE

“Because everything is so decentralized in IT ... they have essentially pushed a lot of those different security controls out of IT and they’re now in the hands of other groups, like DevOps or even individual developers.”

GDPR: Where Do We Go From Here?

Consultant **Tom Langford** on How the Regulation Has Reframed the Global Privacy Discussion



Even though the EU's General Data Protection Regulation went into full effect more than one year ago, there's still room for privacy improvement, says Thom Langford, founder of the consultancy (TL)2 Security.

WATCH ONLINE

The Role of DNS in Cybersecurity

Stuart Reed of Nominet on Improving Visibility



DNS is cybersecurity's best-kept secret for eliminating threats, says Stuart Reed of Nominet, who explains the value of analyzing traffic.

WATCH ONLINE

Mitigating Insider Threats With IAM

Andrew Clarke of One Identity Discusses the Need for Automated Identity Management



Provisioning and deprovisioning employee credentials is a critical component of mitigating insider threats, says Andrew Clarke of One Identity, who discusses the importance of identity and access management.

WATCH ONLINE

Reinventing Application Security

Bob Egner of Outpost24 on DevSecOps and Secure Coding



Bob Egner of Outpost24 discusses the challenges involved in improving application security and whether DevSecOps is a "silver bullet."

WATCH ONLINE

Hacked With Words: Email Attack Sophistication Surges

Barracuda's **Michael Flouton** on Social Engineering, Account Takeover and More



Ask 10 email users if the use of email as an attack vector has stopped, and all 10 would surely agree: No way. "It's insidious because email just works; these attacks continue to be effective," says Michael Flouton of Barracuda Networks. "And it's really just related to our natural curiosity and humanity's willingness to take risks and click on things and explore new opportunities."

WATCH ONLINE

Risk and Resilience: Finding the Right Balance

Leonardo's **Nik Beecher** Details Digital Transformation Best Practices



Finding the right balance between risk and resilience is a challenge for every cybersecurity project, and that's why such efforts must be driven by CISOs and CIOs, says Nik Beecher, vice president of cybersecurity and ICT solutions at Leonardo.

LISTEN ONLINE

Cyberattack Risk: Scans Find Big Businesses Exposed

Open Ports and Servers Plague Some UK Firms, Warns Rapid7's **Tod Beardsley**



Britain's biggest businesses continue to inappropriately expose a number of servers and services to the internet, putting the organizations and the data they store at risk, according to a new study by security firm Rapid7.

LISTEN ONLINE



John McClurg,
VP of Security & Trust, BlackBerry Cylance

How to Block Advanced Threats

Focus on 'Total Cost of Control,' Says BlackBerry Cylance's **John McClurg**

After years of organizations being stuck in a reactive security posture, proactive prevention is finally possible thanks to machine learning backed by artificial intelligence math models, says John McClurg of BlackBerry Cylance.

In a video interview at Infosecurity Europe conference, Coviello discusses:

- Gaining defense in depth while avoiding "expense in depth";
- The increasing juxtaposition of physical security and cybersecurity, especially driven by IoT;
- The promise of artificial intelligence math models and machine learning applications;
- The latest on BlackBerry's acquisition of Cylance.

It's important to "leverage math models instead of signatures and wield the strength of deep learning and neural networks to actually keep pace at the rate of which we see threats morphing today."

WATCH ONLINE



Tim Ager,
VP Sales EMEA, Cymulate

Are You APT-Ready? The Role of Breach and Attack Simulation

Cymulate's **Tim Ager** Discusses Security Control Validation in the Age of Advanced Attacks

With the volume of data breaches and cyberattacks continuing to rise, organizations are increasingly relying on breach and attack simulation tools to provide more consistent and automated validation of controls, says Cymulate's Tim Ager.

In a video interview at Infosecurity Europe conference, Ager discusses:

- The state of data breaches and cyberattacks, including advanced persistent threats;
- The rise of breach and attack simulation tools, and why Gartner is tracking them;
- Handling advanced attacks in today's resource-constrained environment.

“By the year 2021, analysts are predicting that cybercrime will be worth about \$6 trillion worldwide. So it's an arms race that I would argue that organizations are losing right now, and I think there are many reasons for that.”

WATCH ONLINE



Chester Wisniewski,
Principal Research Scientist, Sophos

Beyond Opportunistic: How the Threat Landscape Is Evolving

Chester Wisniewski of Sophos Describes the 'Blended Threat'

The threat landscape continues to evolve, says Chester Wisniewski of Sophos. "The more professional, the more skilled criminals out there are moving, seemingly, away from this 'spray and pray' mass exploitation approach and getting more targeted. It's what I call a blended threat," he says.

In a video interview at Infosecurity Europe conference, Wisniewski discusses:

- How ransomware attackers are shifting from email distribution to directly infecting servers;
- Why identity and authentication is increasingly a social problem;
- As attackers shift tactics, identifying which processes and security policies to adjust.

"It begins out opportunistic, meaning they may just be scanning the internet for people that are running a particular kind of database that has a vulnerability or they may be looking for insecure open remote access things like RDP."

WATCH ONLINE

10 Highlights: Infosecurity Europe 2019 Keynotes

Maersk on NotPetya Cleanup, Troy Hunt on Kid-Perpetrated Data Breaches, and More

BY MATHEW SCHWARTZ | [@euroinfosec](#)

Data breaches, incident response and complying with the burgeoning number of regulations that have an information security impact were among the top themes at this year's Infosecurity Europe conference in London.

Keynote speakers focused on changes in the cybercrime landscape, how big businesses continue to get hacked by children – and what that implies about the state of corporate cybersecurity defenses – as well as complying with European privacy and data security regulations, among many other topics.

Here are 10 highlights from a selection of the keynote presentations at this year's Infosecurity Europe.

Cyberattacker Hype Continues

Data breach expert Troy Hunt, who runs the free Have I Been Pwned? breach notification service, called out a lack of precision when some officials and law enforcement agencies approach cybercrime.

As an example, he referenced the early, official response to the October 2015 TalkTalk breach. "There was a quote from a detective who said: 'We think it's Russian Islamic cyber jihadis.' It's a true quote; you can Google it," Hunt said.

"And the thing that struck me at the time: You're basically just picking scary words and combining them all together. And I hope I didn't upset anyone by saying that these words are scary, but obviously they're just trying to string together something that makes impact," he said. "Now as it turns out, the only part of this which was actually accurate was the cyber bit, and even that I'm not so sure about."

Big Businesses Keep Getting Hacked by Kids

The TalkTalk breach turned out to be the work of a 17-year-old, resulting in what the telecommunications giant said was £77 million (\$97 million) in cleanup costs.

"How does a 17-year-old child do £77 million worth of damage to a massive multinational?" Hunt asked. "Kids and the damage they do via data breaches is massive, and there's a huge amount of communication between literally children about how to break into websites and do this sort of damage."

To illustrate the challenge, Hunt played a clip of video on YouTube in which a young-sounding narrator walks through how to use an automated tool to exploit SQL injection flaws, which he appears to pronounce not as "ess-que-el," as professionals say, but rather as "squirrel." In other words, the kid apparently has no idea about the concepts underpinning structured query language. Regardless, he appears to know how to wield an automated hacking tool to remotely dump databases.

Large Darknet Markets Disappearing

Cybercrime markets reachable via the darknet – aka using the anonymizing Tor browser to browse .onion sites devoted to cybercrime – are dying out, politics and technology expert Jamie Bartlett said in his keynote presentation.

In his talk – "Discovering the Digital Underworld: Privacy, the Dark Web, Tech & Democracy" – Bartlett detailed how many sellers have been favoring "smaller markets that are single vendors rather than large marketplaces that are easier for the authorities to manipulate."

That's been a long-forecasted consequence of police successfully busting so many of these large marketplaces.

Beyond simply rolling up the administrators and top sellers, Bartlett said such sites have also been undercut by authorities creating accounts on these sites and using them to write fake reviews.



Troy Hunt

Markets Shift From Drugs to Data

Initially, darknet markets focused almost exclusively on bringing together sellers and buyers of narcotics, Bartlett said. But that's changed. "Now it's really more about stolen information."

What should organizations from which such data might have been stolen do about it? In response to an audience question about subscribing to darknet intelligence feeds, Bartlett said he thought that if the price was right, that was an excellent idea.

"It's very good for your company to get an early heads-up if your data is being sold there," he said. Even if it was just corporate email addresses or names showing up on darknet markets, monitoring for that occurrence "just gives you a little bit of a head start in case this kind of thing happens."

Maersk: Transparency Helped Save the Day

Transparency was a repeat theme at this year's Infosecurity Europe, including during the keynote presentation delivered by Adam Banks. Banks is the CTO and CIO of Danish shipping giant A.P. Møller-Maersk, which got hit hard by the NotPetya malware outbreak that began on June 27, 2017.

Banks said Maersk's systems were fully patched, and that the malware infected every system that it touched. "This piece of malware was designed specifically to destroy data processing capability," as well as "to destabilize the government by

destabilizing the tax flow," he said. "Of the 7,000 companies that file tax returns in Ukraine, 7,000 were hit."

In Maersk's case, he said, the malware successfully infected every Windows system – all primary, secondary and backup systems – in just seven minutes, before lying dormant for 53 minutes, and then irreversibly crypto-locking everything, including all primary, secondary and backup system, including DHCP and Active Directory servers.

Banks said about 9,000 people worked 20-hour days for nearly three months to get Maersk back up and running again.

Ultimately, the outbreak cost Maersk about \$350 million, including lost revenue. But Maersk earned plaudits for its transparency during the crisis. Banks said this was also key to keeping the shipments flowing. Notably, Maersk secured agreements with every country that it ships to, allowing the firm to retro-file all customs forms once its systems were back up and running. As a result, Maersk still got 95 percent of the goods it was shipping to the right place, on time.

What about the other 5 percent? "I had to go and apologize to the head of Toyota, because we shipped his cars to Australia instead of Europe," Banks said.

GDPR Still Looms Large

Regulations – including the EU's General Data Protection Regulation, which went into full effect in May 2018 – remain a dominant concern for organizations.



Panel: "Navigating Complex Regulatory Oversight to Ensure Privacy, Security and Compliance"



Titta Tajwe

In a keynote panel, "Navigating Complex Regulatory Oversight to Ensure Privacy, Security and Compliance," representatives from the Bank of England, Penguin Random House UK, News UK and the U.K. Information Commissioner's Office talked about the upside – and occasional downsides – of dealing with regulations.

Although moderator Brian Honan, president of BH Consulting in Dublin, focused the discussion on the broader regulatory landscape – including the updated EU ePrivacy Directive – panelists and audience questions kept returning to GDPR.

Broadly speaking, however, panelists highlighted how many regulations, including GDPR, have helped to improve their organization's security posture.

"With the EU GDPR, it really helped for executives to understand what needs to happen to protect the data of your customers," said Titta Tajwe, CISO of News UK. "So it did allow the CISOs to get the budget they needed to do the work they'd already been asking for, for a long, long time."

PCI Is Outdated

But Tajwe said not all regulations are so useful, singling out the Payment Card Industry's Data Security Standard, for example, as being little more than an unhelpful "tick-box exercise."

"At [retailer] John Lewis, I had responsibility for PCI and GDPR, etc., and I can honestly say that the PCI schema was almost a

distraction, because what we found was it was very prescriptive," said the Bank of England's Steve Wright. "It almost wasn't appropriate for our environment," he said, noting that the retailer had "to almost reverse-engineer the those controls to ensure compliance."

"Does more complex regulation improve security or not? It depends on the regulation," said Deborah Haworth, head of information security for Penguin Random House UK. "Regulation that prescribes things for you and removes a company's opportunity to operate under its own board's direction is never going to improve security, because everything becomes 'is it black or white' or 'are we right or wrong?'"

Wright, who's now the Bank of England's GDPR and CISO adviser, said that PCI initially got the industry "to collectively really pull our socks up," but is much too prescriptive for current requirements.

"The challenge is that we need regulation, we need regulators, I get that," he said. "But it is a real challenge, almost a paradox, because you can't dictate too much, but you need to be in a position to self-certify or self-attest that we are doing enough."

"We always tell every organization, get the basics right," said Peter Brown, the ICO's group manager for technology policy. But he noted that for large organizations especially, much more extensive risk measures might be required.

Start Here: You've Been Breached

In terms of basic challenges, "90.8 percent of breaches is still human error," which highlights a lack of data "accountability, ownership and responsibility," said the Bank of England's Wright.

"My approach to this has been to build what I call a defensible position. So almost take the assumption that you've been breached, and it doesn't matter what regulation you fall under, you're going to be asked to justify some of the decisions that were made, that led up to that, and the only way you can do that is by looking at your risk assessment, and understanding where your data is, what you're doing with the data," he said.

"Then you're going to build up a really defensible position for when the proverbial hits the fan ... and you're going to be able to defend yourself," Wright said, regardless of whatever any specific regulation requires.

Cambridge Analytica Likely Failed – This Time

The conference also focused on more big-picture questions of the intersection of technology and society. Bartlett, who previously led the Center for the Analysis of Social Media at U.K. think tank Demos, said one of the biggest threats to democracy is the use of micro-targeting to influence voters. That was the model practiced by Cambridge Analytica, which he said may – or may not – have helped President Donald Trump win three crucial swing states in the 2016 election, each by less than one percentage point.

The micro-targeting being practiced by Cambridge Analytica "was pretty industry standard – lots of people were doing the same thing," he said. "They were probably just slightly better at doing data analytics than the Clinton team was. But this misses the point. Our elections are changing fundamentally."

Thanks to advances in data science, he said, organizations can use "data science and subtle nudges" to micro-target smaller and smaller groups of people. "This is not really what elections are supposed to be about," he said.



Steve Wright



Jamie Bartlett

Instead, elections are supposed to be about grand visions: Who best to govern the country, and what will they bring?

Election Dystopia Looms

Bartlett warned that unchecked election micro-targeting could lead to widespread disenchantment with the electoral system. Ahead of last month's European Parliament elections, for example, British people were being shown political advertisements saying that the EU was trying to ban Brits from drinking tea. (Spoiler alert: Such claims were false.)

"How will an election look 10 to 15 years from now, if we carry on down this same path? That's not really about this election," he said, but rather about the future of elections.

Bartlett offered a vision of what data science might do in the future, based on using smart refrigerator data to correlate an individual's normal dinnertime – say between 6 p.m. and 6:30 p.m. – with social media monitoring that reveals they tend to produce slightly angrier tweets around then, likely due to their being hungry. Meanwhile, data scientists might have concluded that people

who are slightly angrier are more open to messaging by political candidates espousing law-and-order messages.

"So lo and behold, when you open your smart fridge at 6:50 pm, Jacob Rees-Mogg is going to pop up with a message for you and for you alone," he said, referring to the Tory British MP who often espouses far-right viewpoints.

What's the fix? For starters, greater transparency. "The problem is that the rules that we've created just aren't in keeping with the technology that we have, and that's what's causing so much of the tension," Bartlett said. "Our rules at the moment are essentially designed for an age of television and billboard advertisements, not direct, micro-targeted adverts."

What might new rules look like? Bartlett said he'd like to see records kept of every advertisement directed at every individual, backed by automated software to ensure that everyone plays by the same rules, including being transparent about the source of every advertisement, all governed by a regulator that is completely independent from the government. ■

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

+ 44 (0) 203 769 5562 x 216
(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

