



# RSA Conference **2017** Highlights and Insights

## Overview of Content Created by ISMG, Including:

- Video Interviews with Industry Leaders
- Audio Insights from Leading Vendors
- Articles, Blogs, Photos and More from the ISMG Team
- Looking Back on RSA Conference 2017

## The Best of RSA Conference 2017



I'm just back from RSA Conference 2017, which just might have been the biggest yet in the event's 26-year history.

It was my 10th consecutive event, and it was fun to catch up with a lot of familiar faces – some of them in new roles.

It also was interesting to see how old issues such as endpoint security and phishing suddenly have renewed interest. And newer threats such as ransomware and IoT exploits have sparked a whole new line of defenses.

Overwhelming? RSA Conference certainly can be that. From the expo floor with 500+ vendors to the sessions and the streets, packed with more than 40,000 attendees, it's like relocating to a new city for a week. Success is dependent on finding the right neighborhoods and neighbors to hang out with.

Us? We hosted clients and guests in a pair of media suites at the event, and we interviewed a select group of thought leaders in our nearby video studio.

As a media sponsor of RSA Conference 2017, ISMG was at the nexus of activity. This compilation provides a glimpse of our exhaustive RSA Conference 2017 coverage, from pre-event promotional interviews materials to excerpts of our exclusive interviews, including a one-on-one discussion with former U.S. CISO Gregory Touhill.

I've said it before, but it bears repeating: There is no way any individual could have taken in all of RSA Conference 2017. But we sure tried.

Best,

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

---

**Visit us online for more RSA coverage:**

<http://databreachtoday.com/rsa-conference>





# Video and Audio Interviews

<b>Better Bug Eradication in the Age of Agile Development</b> Chris Wysopal, Veracode .....	4	<b>Digital Evolution and Fraud Evolution</b> Ricardo Villadiego, Easy Solutions .....	14
<b>The Emergence of Analytics and Machine Learning</b> Mordecai Rosen, CA Technologies .....	4	<b>Email Security from the Trenches</b> Charles Armstrong (retired) .....	14
<b>Art Coviello on Today's Top Cyber Challenges</b> Art Coviello, RSA (retired) .....	5	<b>FTC, FCC Flex Muscles</b> Joseph Burton, Duane Morris .....	14
<b>The Need for Next-Generation Endpoint Protection</b> Dan Schiappa, Sophos .....	7	<b>Emerging Strategies for Email Security</b> Dave Wagner, Zix .....	14
<b>A New Approach to Endpoint Security Software Testing</b> Tomer Weingarten, SentinelOne .....	7	<b>Integrated Security Platform: How To Get There</b> Kevin Flynn and Ravid Circus, Skybox Security .....	17
<b>Creating New Efficiencies in Vendor Risk Management</b> Stephen Boyer, BitSight Technologies .....	7	<b>The CISO's Evolving Role</b> Vishal Salvi, Infosys .....	18
<b>Breach Response: What Lessons Has Retail Sector Learned?</b> Dan Holden, R-CISC .....	7	<b>Phishing: Inside the New Attacks</b> Markus Jakobsson, Agari .....	18
<b>The Future of Cybersecurity</b> Barrett Lyon, Neustar .....	8	<b>Litigating Cybersecurity and Privacy</b> Randy Sabett, Cooley .....	18
<b>The Evolution of Security Operations</b> Matt Eberhart, SecureWorks .....	8	<b>Mobile Devices: What Could Go Wrong?</b> David Jevans, Proofpoint .....	18
<b>SOC: Threat Discovery, Analysis, Enrichment and Automation</b> Gautam Aggarwal, NSS Labs .....	8	<b>FBI Insights on Investigating Cybercrime</b> M.K. Palmore, FBI .....	19
<b>A Common Sense Guide to Mitigating Insider Threats</b> Randy Trzeciak, CERT .....	8	<b>Cybersecurity and the New 'Adequate'</b> Rich Bolstridge, Akamai .....	20
<b>The Technology of 'Offensive Defense'</b> Avivah Litan, Gartner .....	9	<b>The Evolution of Vendor Risk Management</b> Jasson Casey, SecurityScorecard .....	23
<b>The Emergence of Managed Detection and Response</b> Don Gray and Garry Sidaway, NTT Security .....	10	<b>Behavioral Analytics: The Defender's New Edge</b> Sam Curry, Cybereason .....	23
<b>Former Federal CISO on Cyber State of the Union</b> Gregory Touhill, Brigadier General (retired) .....	12	<b>The First Step in Protecting Business Data</b> Jason Hart, Gemalto .....	23
<b>Step One: Admitting We Have a Cybersecurity Problem</b> Phil Reiting, Global Cyber Alliance .....	13	<b>Privacy Agenda: GDPR and the New Awareness</b> Michelle Dennedy, Cisco .....	23
<b>SonicWall's 2017 Threat Report</b> Bill Conner, SonicWall .....	13	<b>Why Cybercrime Business Is Still Booming</b> Ed Cabrera, Trend Micro .....	24
<b>The Power of Cognitive Security</b> Denis Kennelly, IBM Security .....	13	<b>The Impact of Trump Administration on Cybersecurity</b> Chris Pierson, Viewpost .....	24
<b>The Power of Human Intel</b> Rohyt Belani, PhishMe .....	13	<b>U.S. Rep. Michael McCaul on Homeland Cybersecurity</b> Michael McCaul, U.S. Government .....	24

## More Content

Interviews, Articles, Videos and More .....	26	ISMG Behind the Scenes .....	30
Cybersecurity Chaos Dominates RSAC Discussions .....	27		

# Welcome to ISMG Studios at RSA Conference 2017!

TOM FIELD, SVP EDITORIAL, ISMG

To me, this is what the RSA Conference is about—the deep one-on-one conversations you just can't have elsewhere.

I mean, the expo is a great place to network and get exposed to emerging technologies. The keynotes are engaging. The individual sessions are always educational and timely. But when you can coax into your private studio a true "who's who" of the information security community—people such as FireEye's Kevin Mandia, former RSA Executive Chair Art Coviello and Gartner's Avivah Litan—and engage them in candid, unscripted conversations about nation-state threats, information sharing and the convergence of fraud and security ... to me that's the true value of RSA Conference.

And, man, has ISMG got a slate of interviews for you.

We recorded roughly 35 videos at RSA Conference 2017. And truly we're talking about the A-Z of information security thought leaders, from Akamai Technologies strategist Rich Bolstridge to Zix CEO David Wagner, with a stop in the middle to discuss the future of cybersecurity with Neustar's Barrett Lyon.

I was joined by executive editors Tracy Kitten and Mathew Schwartz to conduct these interviews, and we each worked hard to entice an outspoken group of speakers to sit down with us for these one-on-ones—not just quick sound bites recorded on the expo floor with a hand-held camera, but true sit-down, face-to-face thoughtful conversations. We carefully selected our questions as well as our subjects.

## Better Bug Eradication in the Age of Agile Development

Veracode's **Chris Wysopal** Details the Latest SecDevOps Techniques



The cost upsides of writing code that's as free from bugs as possible has long been known, says Veracode's Chris Wysopal, but bugs continue to plague production code. Thanks to the rise of agile programming, however, there are new opportunities to eradicate flaws during development.

WATCH ONLINE

<https://goo.gl/QSBZ0t>

## The Emergence of Analytics and Machine Learning

CA Technologies' **Mordecai Rosen** on How to Reduce Friction in Security



As organizations struggle with finding the delicate balance of cybersecurity and customer convenience, Mordecai Rosen of CA Technologies says behavioral analytics and machine learning will help.

WATCH ONLINE

<https://goo.gl/IQqe4w>



## Art Coviello on Today's Top Cyber Challenges

Retired RSA Chair on the State of Cybersecurity in 2017

Art Coviello, retired chair of RSA, discusses the state of cybersecurity in 2017, including the threats—and threat actors—of greatest concern and the emerging security technologies that encourage him the most.

In a video interview at RSA Conference 2017, Coviello discusses:

- The impact of cybersecurity as an everyday concern;
- The evolution of security threats;
- His role as a venture capitalist and the ideas that have captured his interest.

WATCH ONLINE

<https://goo.gl/XEnGei>

---

“With the larger countries, I think we’re probably already at a state of mutually assured destruction – ‘You take out my power grid, I’ll take out your dam.’”

---





“I often tell C-level executives: Every customer action creates a fraudster reaction, and this is especially true in the digital transformation.”

—Ricardo Villadiego



## The Need for Next-Generation Endpoint Protection

**Dan Schiappa** of Sophos on Strategies for Advanced Threat Response



Ransomware and other advanced threats have intensified the risks for endpoint devices. And because of that, enterprises need to adopt next-generation endpoint protection, says Dan Schiappa of Sophos.

WATCH ONLINE

<https://goo.gl/PEFsqz>

## A New Approach to Endpoint Security Software Testing

**Tomer Weingarten** of SentinelOne on the Need for Change



As a result of changes in the security environment, it's time to take a new approach to endpoint security software testing, says Tomer Weingarten of SentinelOne.

WATCH ONLINE

<https://goo.gl/IM1TpZ>

## Creating New Efficiencies in Vendor Risk Management

**Stephen Boyer** of BitSight Technologies on Rethinking Strategies



As third-party vendor relationships become more complex and dynamic, organizations need to rethink the way they approach their vendor risk management strategies, says Stephen Boyer of Bitsight.

WATCH ONLINE

<https://goo.gl/ZUhuX4>

## Breach Response: What Lessons Has Retail Sector Learned?

**Dan Holden** of R-CISC on Threat Intelligence and Sharing



Dan Holden, a cybersecurity researcher and technologist, has just taken on the new role of CTO and intelligence director at the Retail Cyber Intelligence Sharing Center. What top challenges is he addressing?

WATCH ONLINE

<https://goo.gl/jM5EH3>

## The Future of Cybersecurity

Neustar's **Barrett Lyon** on How to Create What We Envision for Network Security



Thought leader Barrett Lyon recently joined Neustar as head of research and development, and he has some strong ideas on the future of cybersecurity—and how we can create what we envision.

WATCH ONLINE

<https://goo.gl/Tn6Lu4>

## The Evolution of Security Operations

**Matt Eberhart** of SecureWorks on Cybersecurity Threat Insights for Leaders



SecureWorks has released its new Cybersecurity Threat Insights Report, and Matt Eberhart, vice president, says the key takeaways are about automation, orchestrations and the evolution of the security operations center.

WATCH ONLINE

<https://goo.gl/xbTExQ>

## SOC: Threat Discovery, Analysis, Enrichment and Automation

**Gautam Aggarwal** of NSS Labs on Tackling the Challenges



What new challenges do security operations center teams face? Gautam Aggarwal of NSS Labs addresses the issues of threat discovery, analysis, enrichment and automation.

WATCH ONLINE

<https://goo.gl/6BbyrX>

## A Common Sense Guide to Mitigating Insider Threats

**Randy Trzeciak** of CERT Reviews the Latest Research



Randy Trzeciak of Carnegie Mellon University's CERT describes the latest edition of the group's common sense guide to mitigating insider threats and offers an update on his latest research.

WATCH ONLINE

<https://goo.gl/iLrB9V>





## The Technology of 'Offensive Defense'

Gartner's **Avivah Litan** on How to Boost Detection, Response

Gartner's Avivah Litan is just back from a trip to Israel, and she's particularly enthusiastic about the new topic of "offensive defense." What is the concept, and what security controls does it require?

In a video interview at RSA Conference 2017, Litan discusses:

- Israel's concept of "offensive defense;"
- Her new areas of focus at Gartner;
- What's hot in endpoint security and user and entity behavioral analytics.

WATCH ONLINE

<https://goo.gl/YYco8q>

---

"Most of the security technology today is trying to identify attack behavior, but it's not identifying the attacker behavior."

---





## The Emergence of Managed Detection and Response

**Don Gray and Garry Sidaway** of NTT Security on the Changing Security Landscape

Don Gray and Garry Sidaway of NTT Security discuss the emergence of managed detection and response and the changing security landscape.

In a video interview at RSA Conference 2017, Gray and Sidaway also describe:

- How MSSP demands have shifted in recent months to what we now call managed detection and response;
- How organization's security needs are changing;
- How NTT Security is shifting its resources to meet those changing needs.

WATCH ONLINE


<https://goo.gl/ISiLxy>

---

“It’s no longer this [approach of] ‘we’re sending an email to you,’ or ‘we’re picking up a phone.’ It’s actually ‘how do we work with you to be proactively protecting you?’”

---



A portrait of Mordecai Rosen, a middle-aged man with grey hair, smiling. He is wearing a dark pinstripe suit jacket over a white button-down shirt. A small lapel microphone is clipped to his shirt. The background is a blue screen with a stylized world map.

“Analytics helps you  
balance between  
low friction and high  
security, based on  
continuous analysis.”

—*Mordecai Rosen*





## Former Federal CISO on Cyber State of the Union

### Gregory Touhill Reflects on Challenges for New Administration

Brigadier General (retired) Gregory Touhill was the first federal CISO of the United States. Fresh from that role, he opens up on the state of federal cybersecurity and what the new administration should do to enhance protections.

---

“We’ve already put together a pretty good flight plan. I’d like to see the new administration follow through and execute.”

---

In a video interview at RSA Conference 2017, Touhill discusses:

- His tenure as federal CISO;
- The state of federal cybersecurity;
- The draft cybersecurity executive order awaiting the president's signature.

WATCH ONLINE

<https://goo.gl/bg89WY>

## Step One: Admitting We Have a Cybersecurity Problem

**Phil Reiting** of Global Cyber Alliance on Tackling Risk Management



Phil Reiting, CEO of the Global Cyber Alliance, a group he describes as a "coalition of the angry," describes how it has channeled this anger into action and tells why he believes the U.S. is in step one of a 12-step cybersecurity program.

WATCH ONLINE

<https://goo.gl/7D8Adj>

## SonicWall's 2017 Threat Report

SonicWall CEO **Bill Conner** Highlights Key Research Findings



Bill Conner of SonicWall outlines the key findings of the company's latest threat report, which pinpoints where cybercriminals have made advances in the past year.

WATCH ONLINE

<https://goo.gl/YjBNXw>

## The Power of Cognitive Security

**Denis Kennelly** of IBM Security Describes a Cognitive Security Operations Center



In today's threat landscape, why do we need a "cognitive" security operations center? Denis Kennelly of IBM Security defines the term and makes the case for taking action.

WATCH ONLINE

<https://goo.gl/yYctas>

## The Power of Human Intel

**Rohyt Belani** of PhishMe on the Not-So-Weak Link



Conventional wisdom has long held that humans, because of the mistakes they make, are the weakest links in the security chain. But that's not so, says Rohyt Belani of PhishMe, who explains why.

WATCH ONLINE

<https://goo.gl/ulpXSZ>



## Digital Evolution and Fraud Evolution

Ricardo Villadiego of Easy Solutions on Financial Fraud



Easy Solutions' Ricardo Villadiego addresses how the digital revolution, millennials and the widespread use of online communications affect financial fraud.

WATCH ONLINE

<https://goo.gl/JQILci>

## Email Security from the Trenches

Ex-CIO Charles Armstrong on How to Defend Against the Threats Common to All Sectors



As former CIO of a large government agency, Charles Armstrong is painfully aware of email security issues. Now, as an independent consultant, he's helping organizations defend against them.

WATCH ONLINE

<https://goo.gl/o2nSD6>

## FTC, FCC Flex Muscles

Attorney Joseph Burton on the Impact of Regulators Involved in Cybersecurity



The FTC and FCC are among U.S. regulators now starting to flex their muscles when it comes to enforcing cybersecurity standards, says attorney Joseph Burton. What enforcement trends might we expect to see in 2017?

WATCH ONLINE

<https://goo.gl/IUppBJ>

## Emerging Strategies for Email Security

Zix CEO Dave Wagner on New Threats and the Solutions to Defend Against Them




In the age of ransomware and business email compromises, email security has taken on new significance. And Zix, the email security provider, has rebranded itself to respond. Dave Wagner, Zix CEO, discusses the latest threats and defenses.

WATCH ONLINE

<https://goo.gl/uHUnxQ>



A man with dark hair, wearing a dark suit jacket over a light blue button-down shirt, is shown from the chest up. He is looking slightly to his left and gesturing with his right hand, which is raised with fingers spread. The background is a blurred city skyline with various skyscrapers and a body of water, suggesting an office or conference room setting.

**“It’s all coming back to the security operations center, and the state of the union for them is: ‘Guys, let’s keep it simple ...’”**

***–Gautam Aggarwal***



“The human is not really the weakest link if they’re conditioned the right way. They can be a strong asset—something traditional law enforcement and intelligence agencies have known in the physical world.”

—*Rohyt Belani*







## Integrated Security Platform: How to Get There

Skybox Security's **Kevin Flynn and Ravid Circus** on the Business, Security Benefits

Increasingly, security leaders want to migrate from disparate point solutions to integrated security platforms. Kevin Flynn and Ravid Circus of Skybox Security lay out the business and security benefits.

In a video interview at RSA Conference 2017, Flynn and Circus discuss:

- How the enterprise and security team benefit from consolidation;
- The necessary tools and skills to get there;
- A case study of integration in action.

WATCH ONLINE

<https://goo.gl/sMqG66>

---

“Security is hard – on a large network, it’s complex. And the bad guys like complexity. So the more you can simplify your architecture, simplify your organization, simplify your management ... the better [you are] against the bad guys.”

---



## The CISO's Evolving Role

**Vishal Salvi** of Infosys on the Maturity of Security Leadership



Vishal Salvi is a security leader who has worked in business, left to be a consultant, and now returned to business again. What new perspectives does he bring to his role as CISO at IT services firm Infosys?

WATCH ONLINE

<https://goo.gl/l9kBwp>

## Phishing: Inside the New Attacks

Agari's **Markus Jakobsson** on How the Attackers are Getting Stealthier



Immediately after the 2016 U.S. presidential election, there was a phishing attack that impressed experts with its ingenuity. Markus Jakobsson of Agari discusses this and other recent attacks—and what we must learn from them.

WATCH ONLINE

<https://goo.gl/N0AvaG>

## Litigating Cybersecurity and Privacy

Attorney **Randy Sabett** Shares Insights from Breach, Data Privacy Cases



Cybersecurity attorney Randy Sabett finds himself involved in many lawsuits tied to breach response and data protection. What tips can he share from cases he has litigated?

WATCH ONLINE

<https://goo.gl/5bthXB>

## Mobile Devices: What Could Go Wrong?

Proofpoint's **David Jevans** on Mobile Risks and Phishing Exploits



In the enterprise of ubiquitous mobility, there are overlooked BYOD risks from the mobile apps and the unsecured networks employees use. David Jevans of Proofpoint shares how to mitigate these risks.

WATCH ONLINE

<https://goo.gl/uxcTTk>



## FBI Insights on Investigating Cybercrime

### M.K. Palmore on How to Work Better with Law Enforcement

As one of the FBI's top cybercrime investigators in San Francisco, M.K. Palmore helps many enterprises respond to ransomware and other cyber intrusions. What lessons can he share from investigations?

In a video interview at RSA Conference 2017, Palmore discusses:

- The types of cases he investigates;
- What he has learned about threats and threat actors;
- How security leaders can work more effectively with investigators.

WATCH ONLINE

<https://goo.gl/Dr07tF>

---

“We are pretty good at identifying who’s at the other end of the keyboard, but if we can’t get cooperation and assistance from the governments and places where we find these people, then it’s kind of all for naught.”

---





## Cybersecurity and the New 'Adequate'

Akamai's **Rich Bolstridge** on Expectations for Banks of All Sizes

The threat landscape for financial institutions has changed considerably since the DDoS attacks of 2012. Rich Bolstridge of Akamai Technologies tells how the definition of "adequate cybersecurity" has also shifted.

In a video interview at RSA Conference 2017, Bolstridge discusses:

- The evolution of the financial threat landscape;
- What "adequate" security is today;
- The unique security challenges facing community institutions.

WATCH ONLINE


<https://goo.gl/1j62tH>

---

"If you over the last three or four years built out a security posture that was at the 'elevated' level, now – with the threats increasing over time – you're barely maintaining an adequate security defense for even a 'guarded' environment."

---



A man with short, curly grey hair and glasses, wearing a green button-down shirt, is smiling and looking towards the camera. He is seated in front of a large screen displaying a vibrant image of the Golden Gate Bridge in San Francisco. The bridge's red-orange structure is prominent against a blue sky and water. The lighting is bright, coming from the top of the frame.

“There’s an interesting kind of trickle-down where the [phishing] tools that are developed for the nation-state attacks then get repurposed and used against enterprises, and then after a while they’re used against consumers.”

—Markus Jakobsson







## The Evolution of Vendor Risk Management

Jasson Casey of SecurityScorecard on Giving Enterprises New Tools, New Views



Entities across all industry sectors appreciate the need for ensuring secure relationships with their third-party service providers. Jasson Casey of SecurityScorecard discusses new solutions for achieving those secure relationships.

WATCH ONLINE

<https://goo.gl/cZbBII>

## Behavioral Analytics: The Defender's New Edge

Cybereason's Sam Curry on the Promise of New Technology Solutions



As a veteran security practitioner, Sam Curry of Cybereason is tired of the attackers having the advantage. He wants to see the tables turned, and he believes behavioral analytics just might be the technology to make it happen.

WATCH ONLINE

<https://goo.gl/OSsGMb>

## The First Step in Protecting Business Data

Jason Hart of Gemalto on the Importance of 'Situational Awareness'



The best starting point for effectively safeguarding data and protecting against breaches is to clearly understand what kind of data an organization has, where it's located and the risks, says Jason Hart of Gemalto.

WATCH ONLINE

<https://goo.gl/zir6YO>

## Privacy Agenda: GDPR and the New Awareness

Cisco's Michelle Dennedy on Why Everyone Is Talking About Privacy



Europe's GDPR has business leaders everywhere talking about privacy. But are they having the right conversations? Michelle Dennedy, chief privacy officer at Cisco, offers her perspective.

WATCH ONLINE

<https://goo.gl/b9yQrz>



## Why Cybercrime Business Is Still Booming

Trend Micro's **Ed Cabrera** on Ransomware and Business Email Compromise Trends



Evil hackers with monomaniacal intentions have long dominated pop culture sensibilities. But when it comes to for-profit hacking, cybercrime predominantly remains a business-driven concern, says Trend Micro's Ed Cabrera.

WATCH ONLINE

<https://goo.gl/9R8syH>

## The Impact of Trump Administration on Cybersecurity

**Chris Pierson** of Viewpost on the Outlook for 2017



Chris Pierson of Viewpost offers an assessment of the impact the Trump administration could have on cybersecurity in the government and private sectors and sizes up the role of emerging technologies.

WATCH ONLINE

<https://goo.gl/AC1u0L>

## US Rep. Michael McCaul on Homeland Cybersecurity

What the Trump Administration Can Do to Improve the Nation's Cyber Defense



U.S. Rep. Michael McCaul says Washington must accept that we are losing on the global cyber battlefield. But the Homeland Security Committee chairman contends the Trump administration has the opportunity to turn the tide by prioritizing cybersecurity and investing the right resources in partnerships and defense.

LISTEN ONLINE

<https://goo.gl/8SJOJC>



**“We’re seeing more and more regulators wanting to see this kind of information and hold organizations accountable because of the types of breaches and losses that have happened.”**

***—Stephen Boyer***



## More RSA Conference 2017 Content from ISMG



### [The Rise of Software-Defined Secure Networks](#)

ISMG • AUDIO INTERVIEW • MIHIR MANIAR, JUNIPER NETWORKS



### [Why Most Cybersecurity Startups Won't Survive](#)

ISMG • AUDIO INTERVIEW • RAIMUND GENES, TREND MICRO



### [The Security Business Case for User Behavior Monitoring](#)

ISMG • AUDIO INTERVIEW • DOUG COPLEY, FORCEPOINT



### [Trapping Hackers Via BEC Attacks, Email Spoofing](#)

TRACY KITTEN • AUDIO INTERVIEW • JOE STEWART & JAMES BETTKE, SECUREWORKS



### [Javelin: Card-Not-Present Fraud Jumped 40% in 2016](#)

TRACY KITTEN • AUDIO INTERVIEW • AL PASCUAL, JAVELIN STRATEGY & RESEARCH



### [What's Ahead for Trump on Cybersecurity Initiatives?](#)

TRACY KITTEN • AUDIO INTERVIEW • ARI SCHWARTZ, VENABLE

### [11 Takeaways From RSA Conference 2017](#)

MATHEW SCHWARTZ • ARTICLE

### [RSA Conference Journal: First Days' Highlights](#)

TOM FIELD • VIDEO

### [RSA 2017: Voices of InfoSec Thought Leaders](#)

ERIC CHABROW • SECURITY REPORT

### [Data Integrity in the Era of Fake News](#)

ERIC CHABROW • SECURITY REPORT

### [RSA Conference Update: Talking Phishing](#)

TOM FIELD • VIDEO

### [Post-Quantum Crypto: Don't Do Anything](#)

MATHEW SCHWARTZ • ARTICLE

### [Microsoft Advocates 'Digital Geneva Convention'](#)

JEREMY KIRK • ARTICLE

# Cybersecurity Chaos Dominates RSA Conference Discussions

US Election Interference Highlights Ongoing Dangers, Industry Leaders Say

BY MATHEW SCHWARTZ



Actor John Lithgow addresses RSA Conference 2017.

Ask not what cybersecurity can do for you, but what you can do for cybersecurity.

Amidst the increasing security chaos facing individuals and organizations, one of the dominant themes at RSA Conference 2017 in San Francisco was the need for information security professionals to do more, both for helping to bring order to that chaos, as well as by influencing public policies that could foster long-term relief.

But first, this year's RSA Conference launched with a riot of light and sound: a DJ, drummer, followed by hip hop duo Black Violin's dueling violins and conference-branded wristbands that pulsed colors in time to the music.

Actor John Lithgow next appeared on stage to deliver a crescendoing monologue celebrating cybersecurity professionals and their contributions to making the world a better place.

But if cybersecurity might have previously seemed to be an abstract subject for so many non-practitioners, last year the idea of using hacking "to disrupt a mainstream election became front page news," said Zulfikar Ramzan, the CTO of RSA, in a keynote speech.

"There is no doubt in my mind that the Russia government attempted to influence our elections," said U.S. Rep. Michael McCaul, R-Texas, the chairman of the House Homeland Security Committee and an original co-chair of the Cybersecurity Caucus, in a speech at RSA. "Frankly, it didn't matter to me that it was



---

## "Chaos isn't just something perpetrated by the bad guys."

---

Democrats or Republicans being targeted. These were Americans, first, in the crosshairs of the Kremlin."

McCaul said that he'd previously "pushed President Obama and candidate Trump" to take a stronger stand in response to the Russian interference, "but I was disappointed in their response."

### PUSH TO SIMPLIFY

There are more than a few lessons to be learned from such interference. "It demonstrates our problem isn't limited to the initial cyberattacks we face," RSA's Ramzan said. "Our problem is the long tail of chaos they create. But chaos isn't just something perpetrated by the bad guys; chaos is something woven into the fabric of life, business, government, in nature."

Accordingly, Ramzan said organizations must attempt to simplify their IT operations—he's a fan of consolidating vendors—as well as attempt to tame chaos and finally to "plan for the chaos you cannot control." From an incident-response perspective, he said focusing on availability, budget and collaboration remains essential.

In a message that seemed tailor-made to address current political discussions in the United States, and reflecting the intense, historic

link between Silicon Valley and immigrant innovators, Ramzan also called on the community to ensure that it doesn't "alienate people on the basis of gender, race and culture."

### POLICY INPUT REQUIRED

Multiple speakers called on attendees to use their information security expertise and experience to help actively make the world a better place, amid a backdrop of driverless cars, smart sensors everywhere and the so-called "going dark problem" facing law enforcement and intelligence agencies.

"We technologists need to get involved in policy," Bruce Schneier, CTO of IBM's Resilient Systems, said during a debate about whether internet-connected devices should be regulated to ensure they're secure. "We're never going to get the policies right if the lawmakers continue to get the technology wrong."

Getting involved doesn't necessarily mean having to change jobs, he said, but rather to provide expertise as needed. "We technologists need to get involved ... on Congressional staffs, in federal agencies, at NGOs, part of the press," Schneier said. "We need to build a viable career path for public technologists, just as there is now for public interest law."

### CALL FOR A 'DIGITAL GENEVA CONVENTION'

The call for cybersecurity experts to help bring order to chaos—and for information security professionals to do more—continued in a speech delivered by Brad Smith, Microsoft's president and chief legal officer.

U.S. Rep. Michael McCaul, R-Tex. delivers keynote address.







Professor Susan Landau of Worcester Polytechnic Institute speaks up during the cryptographers panel.

"We are the world's first responders," he said. Complicating that job, however, is the fact that "every company has at least one employee who will click on anything."

Smith said the solution involves—at least in part—individuals, governments and organizations all doing more, and said there is an opportunity for the new U.S. president to help drive such discussions. In particular, Smith called for a Digital Geneva Convention, backed by a new, international cybersecurity agency, modeled on the International Atomic Energy Agency, which seeks to promote the peaceful use of nuclear energy, while discouraging its military use.

### CRYPTOGRAPHERS ANALYZE ELECTION INTERFERENCE

Numerous conference speakers pointed to the U.S. election interference as an example of why cybersecurity professionals are needed more than ever before, while noting that such interference was not exactly surprising.

Chris Young, senior vice president and general manager for Intel Security - a.k.a. McAfee - noted that at the 2016 RSA Conference, he'd posed the question of what might happen if a cybersecurity attack disrupted the U.S. election. Without contesting the results of the 2016 election, he noted that "cyberattacks played a role" and called out the danger for everyone when hacking could be used "to assassinate character."

Such interference has happened before. "Using stolen documents to influence an election is not a new development," said Israeli cryptographer Adi Shamir, the "S" in the RSA asymmetric

cryptographic algorithm, during an opening day cryptographers' panel discussion. Both the United States and Israel's national intelligence agency, the Mossad, have done so before, for example in 1956, when a speech denouncing Stalin was leaked, helping spark an anti-communist revolution that overthrew the Stalinist party and government in Hungary.

"That's why I'm shocked, shocked, by what the Russians are doing," said Shamir, who's a professor of computer science at the Weizmann Institute in Israel. "Let's remember that they're not alone."

Such attacks work better against some targets more than others. "As we know, the Hungarian Revolution wasn't very effective," said co-panelist Susan Landau, a professor of cybersecurity policy and computer science at Worcester Polytechnic Institute. "This type of attack works best against democracies, and against open societies and wired societies."

### PUSH FOR PAPER BALLOTS

To defend against potential interference or voting machine hacking, co-panelist Ron Rivest - the "R" in the RSA algorithm, and a professor at the Massachusetts Institute of Technology - recommended that for future U.S. elections, every vote should generate a paper ballot.

Although there's no evidence that any 2016 U.S. presidential election voting machine results were hacked, having paper ballots would have allowed all voting results to be audited and verified. "Usually you try to convince the losers that they lost fair and square," Rivest said. "Now you're trying to convince the winner that they won fair and square." ■



# Behind the Scenes: ISMG at RSA Conference 2017

Information Security Media Group, Media Partner at RSA Conference 2017, 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 editors being recorded;  
Right: Ed Cabrera, Chief Cybersecurity Officer, Trend Micro speaks with ISMG Executive Editor Mathew Schwartz.



Above: Stephen Boyer, CTO, BitSight with ISMG SVP Tom Field;  
Right: Video crew sets up for the day.









Left: ISMG's Tom Field prepares to interview Tomer Weingarten, CEO of SentinelOne; below: ISMG Executive Editor Tracy Kitten preps for an interview.



Left: Ricardo Villadiego, CEO, Easy Solutions discusses his interview with ISMG SVP Tom Field; above: ISMG Executive Editor Mathew Schwartz on camera; Bottom right: ISMG SVP Tom Field chats with David Elichman, ISMG's Marketing Director.







Above: ISMG at RSA 2017. From left: Kristin Lopez, Tom Field, CEO Sanjay Kalra, Mathew Schwartz, Gina Stillman and GM Mike D'Agostino.



Above: Video crew member prepares for an interview; Left: ISMG sales VP Max Steiger enjoys a conversation with Dan Schiappa, GM of Sophos' end-user and network security groups.





Above: Gregory Touhill, former U.S. CISO, talks with ISMG's Mike D'Agostino and Tom Field; below, ISMG team at their W Hotel media suite: from left, Kristin Lopez, Tom Field, Mike D'Agostino, Tracy Kitten, Max Steiger, David Elichman, Gina Stillman, Mathew Schwartz.







## 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@ismgcorp.com

## Sales & Marketing

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

BANK  INFO SECURITY® CU  INFO SECURITY® Just for Credit Unions GO  INFO SECURITY® GOVERNMENT  HEALTHCARE  INFO SECURITY®

 infoRisk  
TODAY

 CAREERS  INFO SECURITY®

 Data Breach  
Prevention, Response, Notification. TODAY

 **ISMG**  
INFORMATION SECURITY  
MEDIA GROUP