ISMG INFORMATION SECURITY MEDIA GROUP

CyberEd

Cybersecurity Education, News & Insights • June 2019

Whistleblower Everett Stern: 'Do the Right Thing'

'If You See Something, Say Something' Applies to Banks, Money Laundering

p.14

What CCPA Means to Security Leaders

Attorney Sadia Mirza on the Impact of Emerging Privacy Legislation

p.20

Everett Stern
CEO & Intelligence Director, Tactical Rabbit

Letter from the Editor

Tom Field
SVP Editorial

Field is responsible for all of ISMG's 28 global media properties and its diverse cadre of senior-level editors and reporters. He also helped to develop and lead ISMG's award-winning summit series that has brought together security practitioners and industry influencers from around the world, as well as ISMG's series of exclusive executive roundtables.

Twitter: @SecurityEditor

It's been nearly seven years since HSBC was fined $1.9 billion by U.S. authorities for money laundering violations involving international drug cartels. But Everett Stern, the former employee who blew the whistle on the bank, continues to tell his story because he believes similar criminal activity is ongoing. And he has a compelling message to fraud and security leaders across all sectors:

"Do the right thing," says Stern, now the CEO of intelligence firm Tactical Rabbit. "Whatever it comes down to, you have to do it. If you see something, say something. I mean, it doesn't matter the sacrifice, especially if there's fraud."

Stern has spoken at ISMG's most recent fraud and breach prevention summits, and a transcript of an interview with him is in this latest edition of CyberEd magazine.

Also, please check out my interview with attorney Sadia Mirza of Troutman Sanders, in which she talks about the potential impact of the California Consumer Privacy Act and other pending privacy legislation.

As always, while you're here, please review the latest insights and sessions we have added to our catalog of global content. It's been a busy year for ISMG events, and I promise that you will not find a more diverse set of leaders and insights than what we offer here.

Best,

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

2019 SUMMITS

ISMG's global security summit series covers a wide range of topics, from breach prevention and response to fraud prevention and industry-specific themes.

Fraud & Breach Prevention Summit

FEB	Sydney	AUG	Seattle
APR	Dallas	DEC	Washington D.C.
MAY	Chicago Benglaru		

Cybersecurity Summit

AUG	New York
SEP	Toronto
OCT	London
DEC	Mumbai

CyberEd Talks

JAN	Mexico
APR	Chile
JULY	Brazil
OCT	Portugal

Fraud Summit

MAR	New York

Healthcare Security Summit

JUN	New York

Legal & Compliance Summit

NOV	New York

Visit **events.ismg.io** for more!

CyberEd

Editorial

Senior Vice President Editorial **TOM FIELD**
News Editor **HOWARD ANDERSON**
Director of Banking & Payments **NICK HOLLAND**
Executive Editor **MARIANNE K. MCGEE**
Executive Editor **MATHEW J. SCHWARTZ**
Managing Editor **GEETHA NANDIKOTKUR**
Managing Editor **JEREMY KIRK**
Managing Editor **SCOTT FERGUSON**
Managing Director - Asia & Middle East **VARUN HARAN**
Principal Correspondent **SUPARNA GOSWAMI**

Production

General Manager **MICHAEL D'AGOSTINO**
Vice President of Marketing **DAVID ELICHMAN**
Art Director **IAN ROBERTS**
Junior Graphic Designer **CAITLIN PERSICHILLI**

Contact

902 Carnegie Center
Princeton, NJ 08540

Toll Free: (800) 944-0401
ismg.io

ISMG INFORMATION SECURITY MEDIA GROUP

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Our 28 global media properties provide security professionals and senior decision makers with industry- and geo-specific news, research and educational events.

www.ismg.io

Table of Contents

Randy Trzeciak

Best Practices for Mitigating Insider Fraud

PRESENTED BY Randy Trzeciak, Director, CERT Insider Threat Center, CMU

The CERT Insider Threat Center at Carnegie Mellon University is one of the world's leading authorities on detecting insider fraud, and it has just released Version 6 of its Best Practices for Mitigating Insider Threats. As part of this research, the center addresses how to detect and prevent insider fraud, as well as how to map insider threat programs to existing standards, such as the NIST Cybersecurity Framework.

Attend this session to learn:

- The latest research on insider fraud;
- How "accidental insiders" are enabling fraud schemes;
- How to map your insider fraud/threat program against industry standards, including the NIST Cybersecurity Framework.

Andres Rapela

The Federal Reserve's Next Steps to Advance Payments Security

PRESENTED BY Andres Rapela, AVP of Secure Payments, Federal Reserve Bank

Over the years, the Federal Reserve has worked alongside the industry to pursue real-time, safe, highly secure, efficient, broadly inclusive and ubiquitous payment services in the U.S. The U.S. payments and fraud landscape continues to shift as technology evolves and new risks emerge. During this session, attendees will learn about the Federal Reserve's work to inform fraud risk and advance the payment system's safety, security and resiliency. Attend this session to learn about the Federal Reserve's involvement in the future of the U.S. payment system.

Tim Horton

Consumer Data: Multilayered Security Gets Personal

PRESENTED BY Tim Horton, VP, Global Merchant Security and Compliance Solutions, FirstData

In today's digital environment, protecting sensitive information and sales transaction data is of critical importance. Technology and advanced loyalty programs are driving the collection of additional data, causing consumers to pay more attention to the types of data they are willing to share with merchants.

Learn why merchants must pay more attention to data security, how a multilayered approach protects both your business and customers, and why end-to-end encryption is not enough to properly secure personal data.

View this session online at **cybered.io**

Mike Greene

Compromised Credential Detection

PRESENTED BY Mike Greene, CEO & GM, Enzoic

Numerous options exist for strong authentication, but each involves introducing some form of friction into the user experience. User testing shows consumers have extremely limited tolerance for disruptions introduced by security measures, even when those measures are designed to protect personal information and valuable assets.

Enzoic built its credential screening products with the understanding that consumers use the same login credentials across multiple sites. When a user logs in, Enzoic compares their credentials against a continuously updated database of compromised credentials. This process is conducted behind the scenes and adds negligible latency to the login process.

If the user's credentials have been compromised, a range of responses can be taken: Companies may force an immediate password reset, clear credit cards on the account, require an additional authorization factor or log for additional analysis. This protects the user's account and maintains enterprise security against credential stuffing and account takeover attacks launched by cybercriminals.

View this session online at **cybered.io**

Trace Fooshee

2019 Fraud Landscape: Top 6 Trends to Watch

PRESENTED BY Kenrick Bagnall, Detective Constable - Computer Cyber Crime (C3) Intelligence Services, Toronto Police Service; Ryan Duquette, Founder and Principal - Cybercrime and Digital Investigator, Hexigent Consulting

The bad guys are winning the war on identity theft, with losses mounting for organizations across sectors. Increasingly organized criminals have plenty of weapons in their arsenals, including vast quantities of breached data and carefully cultivated synthetic identities. What are the top trends shaping the rising tide of financial fraud in 2019, and what can security professionals expect in the months and years to come?

Our speaker shares research that examines the latest trends challenging U.S. financial services providers. You'll learn:

- The latest trends in identity theft-related financial crimes, including the latest iteration of payments fraud tactics,
- Successful defensive strategies, including the latest trends in deploying omnichannel authentication hubs;
- The often overlooked role that communication plays in the customer experience.

View this session online at **cybered.io**

IT Ecosystems and the Threat From Third Parties

PRESENTED BY Todd Carroll, CISO and VP of Cyber Operations, CyberAngel

In this session, Todd Carroll, former FBI special agent, draws from his experience with the FBI and from his current role as CISO with CyberAngel to discuss:

- Case studies showing exposure of sensitive data by trusted partners in airport operations;
- The increased risk of connected storage and exposure of data trends.

Todd Carroll

View this session online at **cybered.io**

Tim Bedard

The State of Adaptive Authentication in the Financial Industry

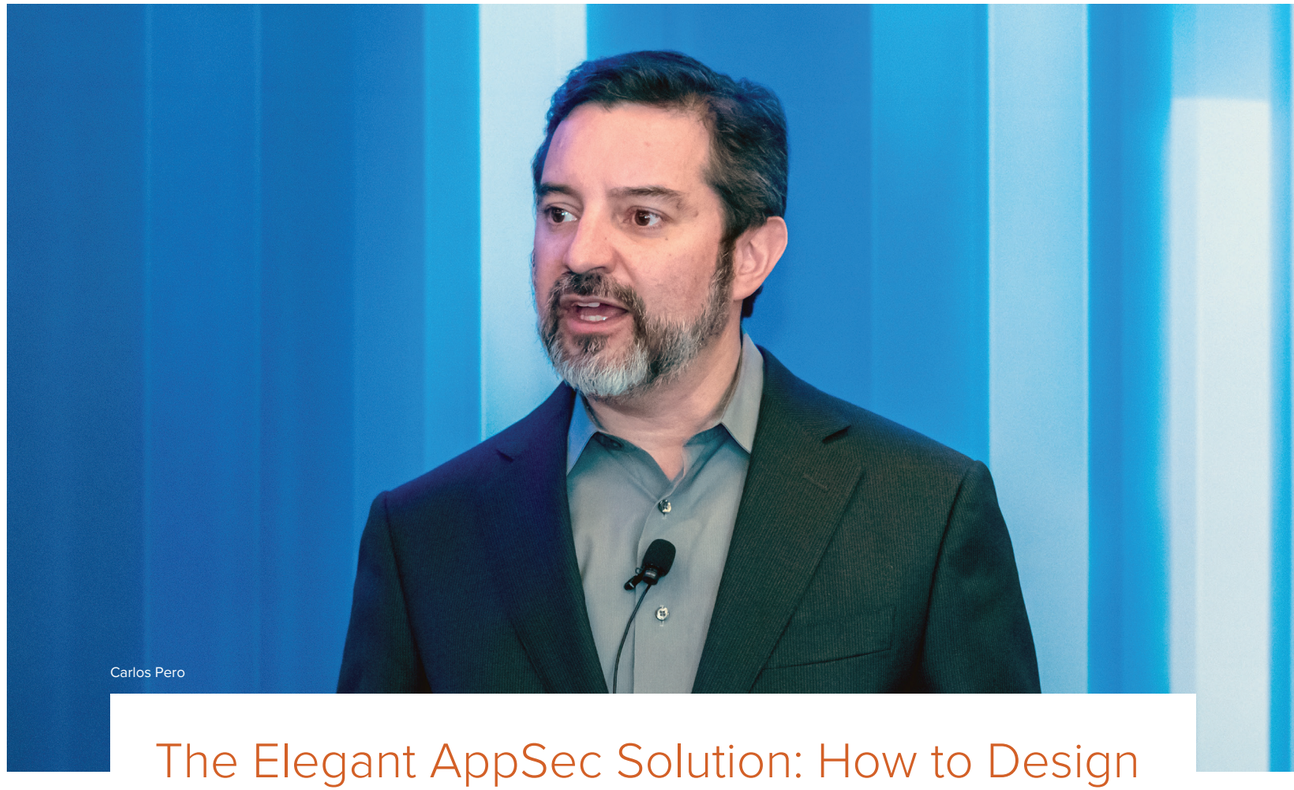
PRESENTED BY Tim Bedard, Director, Security Product Marketing, OneSpan

Fifty-four percent of survey respondents say their institutions' digital authentication measures are average or below when compared to their peers. And 55 percent rate themselves at average or below when it comes to their institution's current ability to apply the right amount of security to the right transactions at the right time. These are among the key results of The State of Adaptive Authentication in Banking survey.

In this session, learn more about the survey results and receive expert analysis about:

- How to benchmark where your organization is on the road of adaptive authentication;
- Business benefits to be gained;
- Tools, skills and partnerships to get you there.

View this session online at **cybered.io**



Carlos Pero

The Elegant AppSec Solution: How to Design a Program that Developers Will Adopt

PRESENTED BY Carlos Pero, AVP and Head of Cyber Application Security, Zurich Insurance

Application security can't continue to be the responsibility of just security experts. After all, anyone can code! And while there are certainly best practices, there is no “one size fits all.” A reasonably designed and executed program should make everyone's job easier.

Join this session for first-hand insights on:

- Security's role in application development;
- How to affect cultural change and gain developers' support for your security program.

View this session online at **cybered.io**

Whistleblower Everett Stern: 'Do the Right Thing'

'If You See Something, Say Something' Applies to Banks, Money Laundering

BY TOM FIELD | @securityeditor

It's been nearly seven years since HSBC was fined $1.9 billion by U.S. authorities for money laundering violations involving international drug cartels. But Everett Stern, the former employee who blew the whistle on the bank, continues to tell his story because he believes similar criminal activity is ongoing.

"There are clear indications it is still going on," says Stern, now the CEO and intelligence director of the Tactical Rabbit consultancy. "Nobody went to jail. Justice didn't happen. The dove did not fly across the courtroom in this case. There are banks that are constantly violating OFAC [Office of Foreign Assets Control] sanctions, getting money to terrorist organizations and drug cartels, and they're just being fined over and over ... and it seems the fines are just a cost of doing business."

In an interview, Stern discusses:

- Why he continues to tell the HSBC story;
- The impact this saga had on him personally;
- Lessons to be learned from his experience.

Stern is CEO and intelligence director of Tactical Rabbit, a private intelligence agency that provides clients with actionable business intelligence. He made international headlines as a government whistleblower who helped uncover one of the largest banking scandals of all time. When Stern joined HSBC Bank in 2012, he discovered that the bank was facilitating the transfer of hundreds of millions of dollars by terrorist organizations and major drug dealers, in clear violation of U.S. law. Stern quit HSBC and filed a whistleblower claim with the SEC. In late 2012, in part as a result of Stern's efforts, HSBC agreed to pay a record $1.9 billion in fines to U.S. authorities. Stern later founded Rabbit Capital Management, an investment advisory firm, and Tactical Rabbit, a consultancy. He has been featured in dozens of news articles and broadcasts, and appeared in a Netflix documentary, "Dirty Money," on Wall Street and corporate greed.

Everett Stern
CEO & Intelligence Director, Tactical Rabbit

View this session online at **cybered.io**

Everett Stern

The Struggle

TOM FIELD: Everett, you have been on television, in print, in publications talking about your work as a whistleblower. People see you as a champion, as someone that saw something that was wrong and stood up for it. What don't people see about your experience as a whistleblower?

EVERETT STERN: They don't see the sacrifice and the pain and the loss and losing everything. I mean, after the HSBC scandal, I lost everything. I mean, I was even sleeping on a cot in this 400 square foot apartment. People don't see that. They don't see the struggle. They just see years later, after starting and running a successful company, they just see the success part of it. They don't see the struggle to get there.

What they also don't see is right before you blow the whistle, or in my case I started passing the information to the CIA about three weeks in on the job, so I was doing this consistently throughout my tenure at HSBC. So I didn't quite blow the whistle. I don't really consider myself a whistleblower. I did the right thing. I did it multiple times. But right before my email to the CIA three weeks in, there was a moment where I was laying in bed, tossing and turning, trying to figure out whether or not to pull the trigger and to actually send that email and do the right thing, and decide I'm going to take a stand for what's right. What got me to do it was that success poem by Emerson.

My dad gave me the success poem. I don't remember the whole thing, but I remember at the end it says that you're successful if you can leave this world a better place by a redeemed social condition, and that's the true meaning of success. I decided, "You know what? I'm going to go for it."

I remember, it was like 2:00 in the morning, that's when I sent the email to the CIA. That's what started me down a path and the bank down a path, of the largest fine in U.S. history of $1.92 billion.

Why Continue?

FIELD: The case is years over now. Players have moved on, you've moved on. As you say, the bank got the biggest fine in US history. What inspires you to continue to go out and tell this story?

STERN: Because I believe it's still going on. There are clear indications it's still going on. Nobody went to jail. Justice didn't happen. A dove did not fly across the courtroom in this case. There are banks now that are constantly violating OFAC sanctions, that are getting money to terrorists and drug cartels, and they're just being fined over and over. Not just HSBC, but other banks, like Standard Charter and Capital One.

I mean, there are numerous banks that are being engaged in this. It seems to be that these fines are just the cost of doing business, and it's not just the cost of doing business anymore. The U.S. government right now has taken the stance of just issuing these fines, and what the U.S. government doesn't understand is that if the next 9/11 happens, that's what's going to cause the next financial crisis.

By the government not putting bankers in jail, what they're trying to do is prevent that financial crisis. But again, circling back to 9/11 or terrorism, wars cost money. If we shut off the money supply, then we'll win. That's what the government is kind of missing here. They just keep fining because they're afraid of this financial crisis that is going to happen because the terrorists keep getting the money.

Bombs, bullets. These things cost money. It's disgusting to me, to go back to your question even further as to why I keep being so outspoken about this. Every time I see a vet with his arm blown off from some IED on the side of the road in Iraq or Afghanistan, that is coming from Hezbollah, where they're designing the IEDs, and HSBC has been found guilty and has admitted to financing Hezbollah to create these types of bombs to blow up our troops. We're talking thousands of American soldiers that have been killed or maimed, and it's continuing to go on.

Again, this is a situation where it's so frustrating for me because I keep blowing the whistle every single day. It's not just blowing the whistle once, but every single day. Even now, nobody is listening. What people don't understand is that everything comes down to the dollar. Terrorist organizations want to use the U.S. dollar. That's the ultimate currency to actually buy equipment, buy bombs, and to be able to wage war against the United States. They're using our own currency against us.

> **"Do the right thing. Whatever it comes down to, you have to do it. If you see something, say something."**

'Do the Right Thing'

FIELD: Everett, you spoke at our Chicago Fraud and Breach Prevention Summit. If there's one take away from your session, what would that be?

STERN: Do the right thing. Whatever it comes down to, you have to do it. If you see something, say something. I mean, it doesn't matter the sacrifice, especially if there's fraud. ... What a lot of people don't understand is that when it comes fraud or violations in money laundering compliance, they think, "Oh, it's no big deal." ... People have to link money to terrorism, drug cartels, crime, death. It's not so simple. It's not just a white collar crime. A white collar crime is not just white collar – it's red collar; it's blood. ■


Tommy McDowell

Retail Breach Response

PRESENTED BY Tommy McDowell, VP of Intelligence, RH-ISAC

Target. Home Depot. Starwood. These retail and hospitality giants have been in the data breach headlines in recent years. And in response, the industry formed the Retail and Hospitality Information Sharing and Analysis Center to be a central hub for sharing sector-specific cyber security information and intelligence.

This session addresses:

- RH-ISAC's mission and accomplishments;
- The 2019 threat landscape;
- Top lessons learned from the headline breaches.


Dan Fitzgerald

The Future of Cloud Security Programs

PRESENTED BY Dan Fitzgerald, CISO, McKinsey & Company

This session features stories, practical experiences, anecdotes and a bit of humor about creating and managing cloud security programs and the journey to DevSecOps.

The session covers:

- Key components of cloud security programs and the basics of DevSecOps;
- Real-world challenges and practical solutions for creating cloud security programs;
- Challenges of standardizing cloud infrastructure at scale and how to overcome them;
- The changing nature of security teams in cloud settings;
- Action planning and applied discussion questions for participants.

What CCPA Means to Security Leaders

Attorney Sadia Mirza on the Impact of Emerging Privacy Legislation

BY TOM FIELD | @SecurityEditor

Post-GDPR, the California Consumer Privacy Act was the first piece of U.S. legislation to emerge – but it's hardly the last. Attorney Sadia Mirza of Troutman Sanders talks about the potential impact of CCPA and other pending privacy legislation.

"2018 was a huge year for privacy," Mirza says. "It's important to follow what's going on in California right now because it's going to be shaping a lot of the other laws that are going to be popping up in the United States."

In an interview, Mirza discusses:

- GDPR's impact on U.S. legislation;
- Key tenets of CCPA;
- What security professionals need to know about pending privacy bills.

Mirza, a cybersecurity, information governance and privacy attorney at Troutman Sanders, focuses her practice on the financial services industry.

Following in GDPR's Footsteps

TOM FIELD: We hear a lot about post-GDPR in the U.S. and about the rise of CCPA in California. I know they're part of your interest, but what is the emerging privacy legislation that really has got your attention these days?

SADIA MIRZA: I think you hit it right on the spot. The California Consumer Privacy Act really did follow in the GDPR's footsteps. As I'm sure you know, 2018 was a huge year for privacy. The GDPR rolled out, and then with the California Consumer Privacy Act, California quickly followed suit right afterward.

It's really important to follow what's going on in California right now, because it's going to be shaping a lot of the other laws that are going to be popping up in the United States.

Just for some background, the California Consumer Privacy Act's goal is to expand the privacy rights for California residents by giving consumers, California residents, access to their personal information. Of course, under certain circumstances, consumers will have the ability to delete their personal information, request that businesses opt out from the sale of their personal information, and things along those lines. So it really does mimic some of the GDPR data subject rights that we saw over there.

The California law is going to come into effect in January 2020. But there are many amendments in the works right now. So companies can start taking steps toward compliance. But they should keep in the back of their minds that things may change over the next few months and just keep an eye on what's happening.

Why this is important is because ... the last time I checked, there were about 16 states that had proposed their own version of a CCPA law, so we've been calling them the CCPA copycat laws.

With all these variances across the states, similar to what we saw with data breach notification obligations, companies need to be staying ahead of that to make sure that they're going to be able to comply when the time comes.

Sadia Mirza
Attorney, Cybersecurity, Information Governance and Privacy Practice Group, Troutman Sanders

Breach Notification

FIELD: What is the interest of security professionals in all this legislation? What do they need to know?

MIRZA: Washington recently did something that I think was noticeable; they amended their data breach notification obligation. What they did was they strengthened it in the sense that it expanded the definition of personal information.

It will be considered a data breach if there's a compromise of first name, last name, with something like a full date of birth. Historically, that's not really what constituted a data breach, at least not in Washington. It was more limited to the historical, like first name, last name in combination with a Social Security number, or some kind of a government identifier.

So the number of incidents that will qualify as a data breach is going to increase. We saw this happening in Washington, and ... North Dakota is kind of following in those similar footsteps.

I don't think it would be very surprising to see other states trying to amend their data breach notification laws to strengthen them or expand the definition of personal information or shorten the notification deadlines.

To your question, I think why it's important is because when you're having these incident response plans in place, that document is the guiding document to help you respond, assess and detect your security incident. You need to be complete. You need to have that in place so that you can meet these notification obligation deadlines.

The shortest deadline right now, I believe, is Puerto Rico, where it's 10 days; Washington amended it to 30 days. But if you don't have a good incident response plan in place, which speaks to the information security professionals, you're not going to be able to meet those deadlines. And that's why it's important to focus on this.

FIELD: Sounds like it's a good time for the privacy officers and the security officers to have some lunches together.

MIRZA: Yes, it's a good time. It's a very busy time; all the legislation is keeping everyone really busy. It's tough sometimes to stay ahead of it because there are constantly amendments being proposed. You just have got to stay ahead of it.

FIELD: Is there emerging international legislation you're watching as well?

MIRZA: I really do focus on U.S. privacy law right now. My focus at this point is the California Consumer Privacy Act and the various state laws that are popping up along those lines.

But yes, the GDPR really stole the show last year, so that's probably what people are still taking a look at. ■

The Next Perfect Storm: Are You Ready for the Convergence of IoT, Blockchain, Better Data Analytics and AI?

PRESENTED BY Laszlo Gonc, Practicing Chief Healthcare CISO, and Cybersecurity and Transformation Strategist & Evangelist

Tremendous technology changes in recent years have made exponential leaps in the way we communicate, interact and transact with each other. The internet of things has brought about the potential for embedded low-cost sensors on everything around us, on us and even in us. Blockchains and smart contracts with advances in encryption tools will provide for the immutable trust and transparency required to build the foundation of Web 3.0. The collection of all this data will provide startling context to how we behave and make decisions through better data analytics.

Advances in artificial intelligence through machine learning will change the way we interact with machines, our environment and each other forever. What does this mean to your business? In this session you'll learn:

- The technology risks and security challenges to your organization;
- How to protect your company against the new cyberattacks;
- How these technologies impact your organization on its road to digital transformation.

New Targets On Cybercriminals' Radar

PRESENTED BY Shaked Vax, Trusteer Products Strategist, IBM Security

Cybercrime has targeted bank and payments solutions for a long time, but in the past few years, targeted industries have expanded to airlines, insurance, travel, retail and other sectors. CISOs and fraud-fighting leaders who have been focused on insider threats are finding they need to consider the fraud darknet ecosystem and actors as part of their strategy development considerations.

This session:

- Identifies new industries targeted by cybercrime and fraud and key MOs used to attack them;
- Presents opportunities for advancing digital cybercrime protection while improving the customer experience at the same time through implementation of new digital trust strategies.

View this session online at **cybered.io**

Randy Sabett

GDPR, CCPA and Security in the New Privacy World

PRESENTED BY Randy Sabett, Special Counsel, Cyber/Data/Privacy Practice Group, Cooley LLP

U.S. organizations were barely GDPR compliant in 2018 when California unveiled its own privacy legislation, the California Consumer Privacy Act, which goes into effect on Jan. 1, 2020. This is just one of several privacy laws being enacted across the U.S., and it poses many questions about the role of security to enable privacy – and the role of security leaders to enforce it.

Join this session for an exclusive legal overview of:

- What's covered and who's covered under CCPA;
- GDPR Article 32 security requirements;
- The answer to the question: "If I'm GDPR-compliant, aren't I CCPA-compliant?"
- What happens if I'm not secure?

View this session online at **cybered.io**

Malicious Bot Attacks: The New #1 Cyber Threat

PRESENTED BY Carl Gustas, Solutions Engineer, Cequence Security

This session addresses the automation landscape as it pertains to nefarious actions against hyper-connected organizations. It discusses what bots were initially designed for and what they've evolved to. And it describes the negative effects automation can have on organizations, their business logic, infrastructure and security practices. Plus, the session outlines the tools commonly used by enterprise organizations and the pitfalls and challenges surrounding them.

Carl Gustas

View this session online at **cybered.io**

Premium Memberships

See why a Premium Membership is a must-have resource at thousands of organizations worldwide.

1 UNLIMITED ACCESS TO EXCLUSIVE CONTENT

Only premium members have unrestricted access to our entire educational resource, including: exclusive breaking news, in-depth interviews, industry research, live expert Q&A sessions, ISMG summit session recordings, on-demand webinars, and our full archive of over 800 webinars.

2 CONTINUALLY EXPANDING CURRICULUM

Gain unrestricted access to an expanding curriculum, including recordings from all ISMG summits throughout the year. With daily breaking news updates, executive interviews, and new on-demand courses, no education solution is nearly as comprehensive. This continually growing resource ensures you have the latest information available as you need it.

3 EVENT PROCEEDINGS AT YOUR FINGERTIPS

Only premium members gain access to recorded sessions from in-person events, including all ISMG summits. Couldn't attend a summit? Want to revisit your favorite presentation? Each summit has over 10 hours of education. Presentation materials are also available for each session throughout the year.

4 ON-DEMAND CONVENIENCE

The ability to access the training you need exactly when you need it is essential when it comes to your professional responsibilities. On-demand viewing and downloadable presentation materials allow you to access education around your availability, not ours. Whether you have 15 minutes before a meeting, 30 minutes on your lunch break, or even during your daily commute, our education is always at your fingertips.

5 CONTINUING PROFESSIONAL EDUCATION (CPE)

Responding to regulators, senior management and certifying associations can become a hassle. Our transcript tracking feature lists date, title and hours of all credit-eligible webinars, articles, interviews, handbooks and other content accessed. This transcript can be broken down by topic, and attendance certificates can be emailed or printed directly from our system, making it easy to keep track and report on your continued education.

6 ACCESS TO EXPERT SPEAKER FACULTY

Our faculty of over 100 experts consists of industry practitioners and regulators who have been essential in successfully implementing the very same initiatives you are responsible for. These experts not only contribute through interviews and webinars, but also interact directly with premium members through insider access to live Q&A webinars and in-person executive roundtable meetings and ISMG summits.

RECENTLY RELEASED SESSIONS	SPEAKER(S)	TOPIC
2019 Fraud Landscape: Top 6 Trends to Watch	Trace Fooshee	Fraud
The Elegant AppSec Solution: How to Design a Program that Developers Will Adopt	Carlos Pero	Application Security
The Future of Cloud Security Programs	Dan Fitzgerald	Cloud Security
New Targets on Cybercriminals' Radar	Shaked Vax	Cybercrime
GDPR, CCPA and Security in the New Privacy World	Randy Sabett	Compliance
Compromised Credential Detection	Mike Greene	Authentication
The State of Adaptive Authentication in the Financial Industry	Tim Bedard	Authentication
IT Ecosystems and the Threat From Third Parties	Todd Carroll	Third-Party Risk Management
HSBC Whistleblower on Uncovering Fraud	Everett Stern	Fraud Management & Cybercrime
Consumer Data: Multilayered Security Gets Personal	Tim Horton	Risk Management
Retail Breach Response	Tommy McDowell	Information Sharing
The Next Perfect Storm: Are You Ready for the Convergence of IoT, Blockchain, Better Data Analytics and AI?	Laszlo Gonc	Technology
Best Practices for Mitigating Insider Fraud	Randy Trzeciak	Fraud
Incident Response Plans: Global Compliance Mandates and Obligations	Sadia Mirza Darrin Kimes	Incident Response
Malicious Bot Attacks: The New #1 Cyber Threat	Carl Gustas	Endpoint Security

JOIN NOW AND GET INSTANT ACCESS

Gain unrestricted access to an expanding curriculum, including recordings from all ISMG Summits throughout the year. **Visit www.cybered.io/memberships**

Gain unrestricted access to an expanding curriculum, including recordings from all ISMG Summits throughout the year.

Visit cybered.io
@cyberedio
CyberEd.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY CyberEd.io

ISMG
INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io