SUMMIT CHAIR
Nicholas Tuppen
Vice President, Global Information Security
Bank of America Merrill Lynch

2017 FS-ISAC EMEA Summit

STRENGTH IN SHARING

30 October - 1 November
etc.venues County Hall
London, England
WHO SHOULD ATTEND?

- CEO/Bank Owners, CISO, CSO, CIO, CTO and CRO
- Head of Threat Intelligence
- EVP, SVP, VP and Director of:
  - Security Operations
  - Fraud and Cybercrime
  - Investigations
  - Physical and Information Security
  - Business Continuity
  - Audit and Compliance
  - Payment and Security Risk Management
  - Payment Operations
- Payment Line of Business Managers including:
  - Online Banking
  - Online Treasury Management

WHY YOU SHOULD ATTEND

- Presentations by Senior Executive FS-ISAC members
- Concrete take-aways including case studies and best practices
- Interactive sessions that allow for strategic and solution-oriented discussion
- Actionable information and sharing designed specifically for financial services institutions
- Complimentary attendance for Premier and above members
  - All meals and events during the conference are included
- New workshops and events on the latest issues, including:
  - Breach notification (PSD2, NIS)
  - Data privacy (GDPR)
  - Extortion
  - Ransomware
  - Security assurance and certification (CBEST)
  - Shadow brokers
  - State actors
ATTENDANCE RESTRICTIONS
The 2017 FS-ISAC EMEA Summit restricts attendance to regulated financial services firms, relevant public sector entities and country-level banking associations and payments associations. If you have questions regarding eligibility, contact marketing@fsisac.com. If you are a solutions provider, please view the sponsor prospectus (fsisac-summit.com/2017-EMEA-Prospectus). Non-member registration is reserved for regulated financial institutions.

Early Bird Registration ends 23 September.

<table>
<thead>
<tr>
<th>FS-ISAC Affiliation</th>
<th>Early Bird (ends 23 September)</th>
<th>Standard Registration (after 23 September)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premier/Platinum/Gold Member</td>
<td>COMPLIMENTARY</td>
<td>COMPLIMENTARY</td>
</tr>
<tr>
<td>Basic/Core/Standard Member</td>
<td>$895 USD (£703 GBP</td>
<td>€770 EUR*)</td>
</tr>
<tr>
<td>Government</td>
<td>$995 USD (£782 GBP</td>
<td>€855 EUR*)</td>
</tr>
<tr>
<td>Non-Member/CNOP Member</td>
<td>$995 USD (£782 GBP</td>
<td>€855 EUR*)</td>
</tr>
</tbody>
</table>

*Final payment will be taken in USD. GBP and EUR prices are an estimated conversion; final price will depend on current exchange rates.

CANCELLATION POLICY
Any cancellations must be received via email to summit@fsisac.com prior to 19 September to avoid cancellation fees.

Cancellations received prior to 19 September will not be subject to a cancellation fee. Cancellations received on or after 20 September will be subject to a $200 USD (£157 GBP | €172 EUR*) cancellation fee. This applies to all members at all tiers as well as to non-member, government and CNOP registration regardless of registration fee paid.

Registrations are transferable within an organization without penalty.

ONLINE REGISTRATION
fsisac-summit.com/2017-EMEA-Attendee-Registration

FS-ISAC Summits are exclusive to FS-ISAC members, sponsors and invited guests. Only registered attendees may attend and participate and the event is closed to the media. Information shared during Summits is typically shared under the Traffic Light Protocol (TLP) Amber level unless otherwise indicated. By registering, attendees agree to abide by the Summit code of conduct outlined in the attendee materials.
location

VENUE

etc.venues County Hall
Belvedere Road, London SE1 7PB; United Kingdom
etcvenues.co.uk/venues/countyhall

For a virtual tour of etc.venues County Hall, visit this web address: etcvenues.co.uk/vr

The FS-ISAC EMEA Summit will be hosted on Level 4 of County Hall.

HOTEL

Park Plaza Westminster Bridge London
200 Westminster Bridge Road, London SE1 7UT; United Kingdom
parkplaza.com/london-hotel-gb-se1-7ut/gbwestmi

FS-ISAC has reserved a block of rooms at the Park Plaza Westminster Bridge London at a group rate of £179 (approximately €199 EUR) for a single occupancy room and £189 (approximately €210 EUR) for a double occupancy room. The deadline to make reservations of 29 August or until the block is sold out - which ever comes first. Space is limited, please make your reservations at your earliest convenience.

Please visit fsisac-summit.com/2017-EMEA-Hotel-Travel for more information, and to make your reservation online.
During the Solutions Showcase, members are invited to join us for hors d’oeuvres and a technology showcase where the latest technical innovations will be on display. In this relaxed setting, attendees select up to three technologies they’d like to see. These information-packed, 15-minute sessions will be presented by technology experts from our vendor sponsors, will be use-case driven and will be tailored to the unique needs of FS-ISAC members. Each sponsor will present three times to a different audience.

- Fox-IT | Evolution of the Threat Landscape: Behind the Scene
- IBM | Uncovering Fraud Faster and More Effectively
- Menlo Security | Eliminating Payment System Attacks
- Synack | Attacker Resistance: Redefining Risk from a Hacker Perspective
session descriptions

GENERAL SESSIONS

Real-Time Risk Management | Assessing endpoint risk has become increasingly complex and siloed over the past decade. Security teams and technologies alike must divide their focus between potential and active threats. Compliance efforts yield a strikingly different perspective on the state of an environment than the output of a CSIRT or hunting team. As a result, CISOs often struggle to accurately measure how secure their systems truly are, and which assets merit the most attention. This session will offer a blended approach to evaluating and monitoring endpoint security in real-time, using data points that define the risks attached to systems and their users.

Ten Changes in Cyber Regulation: Number Six Will Shock You | Global financial sector regulators are treating cybersecurity as a top priority. Their interests range from limiting the risk of systemic failure to protecting customers from fraud and privacy incidents. The last few years have been used to gather information and consolidate understanding and now new waves of prescriptive requirements are beginning to land. This fast-moving topic is challenging to regulate and this light-hearted presentation takes a click-bait fueled look at how to get the most from current and future regulation and what we can expect on the horizon.

MEMBERS ONLY

DDoS Threat*

Developing an Intel Sharing Maturity Model | Actively participating in an information sharing community like FS-ISAC is a challenging task. It requires fundamentally rethinking the confidentiality of security relevant information, and takes a lot of effort to integrate external services and processes into your own daily operations.

In order to help our members better prioritize their efforts, and to understand where they can improve the value they gain from their FS-ISAC membership, we propose developing a maturity model for participating in FS-ISAC, or in a similar information sharing initiative. This can be based on existing information security maturity models (e.g. BSIMM), as well as threat intel maturity models available, and will require member input in order to be as relevant as possible. This session is your opportunity to help create a framework that also lets us understand where our members require more support and activity.

From Compliance to Culture, from Awareness to Action*

From Secure Cloud to Competitive Advantage | In this presentation, hear about lessons learnt relating to the secure usage of cloud computing within financial institutions and in compliance with all regulations in Europe and elsewhere around the world.

Innovation Bridges | One of the greatest challenges in promoting cybersecurity resilience is bridging the gap between technology vendors, research institutions and end-users. The promotion of inclusive open innovation hubs is a necessity. In this session, learn about the current creation of a financial technology open innovation hub and the benefits of global players creating a cross-border innovation bridge.

Innovation Challenge*

Money Muling | The session will review a real case study of a criminal business – with very little technical expertise – monetizing stolen credit card data. The presenter, a former law enforcement officer, will talk to how the case was investigated, how they identified the money mule network behind the thefts, and eventually how LE arrested the perpetrators. The speaker will also take the audience through a global law enforcement exercise that examined the “cradle to grave” use of the Dark Web to buy stolen login credentials and monetize them.

Ransomware and WannaCry: Sharing Experiences of the Critical Success Factors. Now What's Next? | This session features a panel discussion with key specialists from financial services, including a brief presentation on the history of ransomware, key insights into the threat, the impact of ransomware and how best to defend against it. Learn about trends and developments, the main challenges of ransomware, the human factor, destructive wiper attacks, what could be on the horizon and more.

CONCURRENT SESSIONS

A Collaborative Approach to Third-Party Risk Management | Governing and managing third- and fourth-party vendor relationships continues to be complex and significant given all of the new global regulations, technologies and standards. Financial organizations want to protect themselves and their customers from vendor threats, but are challenged with how to do it in a scalable and cost-effective way. In this session, attendees will learn: industry best practices on developing a third-party risk program and how to incorporate a collaborative approach that will save you time and money.

*Please check back for more detailed information on this breakout session.
As the security industry has continued to
Defending Against Phishing: Preparing and Using Human
2018 exercise.

In 2016, more than 1,800
Cyber-Attack against Payment Systems (CAPS), EMEA

Betrayal-as-a-Service: Trends in Insider Threat |
This session will highlight the shift in insiders’ due to
anonymization and shifting demographics; discuss the
coming trends of incremental insider threat; and highlight the
role that threat intelligence plays in monitoring and identifying for indicators of insider threat outside your networks. Also, this presentation will review cost effective solutions to implementing continuous monitoring and response to insider breaches, while protecting and respecting the privacy of your employees.

CISO Case Study: Teaching Old Data New Tricks | Security officers and teams need to communicate with many different business functions to explain risk and justify priorities. Usually this means taking data that is technical and about security and compiling it into an engaging and empowering read for non-technical individuals. This is not without its challenges. Hear how you can give different stakeholders the visibility they need into security-relevant data, so that they understand, support and assist in protecting your business.

Cyber-Attack against Payment Systems (CAPS), EMEA 2017 After-Action Report | In 2016, more than 1,800 financial institutions registered for the CAPS table-top exercise in EMEA, APAC and the Americas. This after-action report will focus on the observations about the aggregated anonymous results from the EMEA region. The 2017 exercise scenario features a cyber-attack against ACH corporate trade payments that do not use SWIFT messaging. The first part of the session will be a review of data with observation, followed by an interactive discussion on observations, feedback and recommendations for the 2018 exercise.

Defending Against Phishing: Preparing and Using Human Sensors | As the security industry has continued to under invest in the human element of security, phishing has become the top attack vector for cybercriminals. Breaches continue to occur in record numbers, detection takes an excessively long and the most preferred targets are an organization’s human assets. Empowering human assets to provide vetted intelligence to your incident response teams is often overlooked. In this presentation, learn about recent phishing attacks, how businesses can reduce susceptibility to human-targeted attacks by providing immersive simulated phishing and how to empower users to be human sensors that can recognize and report suspected attacks, thus reducing the attack detection window.

FS-ISAC 101 | This session is an interactive workshop on FS-ISAC services. It provides an overview of FS-ISAC, how to use the portal, filter alerts, and participate in appropriate special interest groups.

Hot Topic!* Keeping Up with FinTech: Security Testing in a Fast-Paced World | The rapid rise of FinTech and new application-driven financial products increases the threat surface for malicious actors. Gartner states that 90% of all applications are not secure, raising the risks for potential security vulnerabilities and exploits. This session will highlight the overall security challenges in a fast-paced FinTech world; provide a guide to automated security testing to keep up with that pace; address automation for stress testing financial transaction networks and web facing content, application security defect prevention and automation for discovering third-party integration risks; and how to prioritize actions to get started by independently benchmarking your security maturity against financial service organizations around the world.

Know Thy Enemy: Views from the Deep and Dark Web Underground | The deep and dark web (DDW) is a rich source of data full of black market products and services, weapons and training manuals, malicious TTPs and dialogue between threat actors. Threatening activity from the most difficult to access and high-risk areas in the DDW can harm an organization’s business, stakeholders, employees and customers.

This session will outline some of the challenges involved in effectively tracking and monitoring threats on the DDW including dispelling common myths surrounding attackers operating within these communities and providing insight into their mindsets and motivations through examples from past and current events.

Lessons Learned from the Frontlines: Responding to WannaCry and Petya* Offline and Local: The Hidden Face of Cybercrime | The conventional wisdom is that cybercrime is a largely anonymous activity that exists essentially in cyberspace. The supposed anonymity of attackers feeds into a narrative that cybercrime is strange, new, ubiquitous and ultimately very difficult to counteract. The central purpose of this presentation is to dispute this view. Where one looks for it, there is actually a strong offline and local element within cybercrime, alongside the online dimension. In order to investigate this claim and its implications for policing, the core of this presentation is dedicated to a case study from Romania.

Positive Regulatory Engagement over Regulation: The Changing Nature of the Relationship | Cyber-resilience is a sector top priority and regulators want to be part of the solution not the problem. Rather than dictating compliance regulators are looking to collaborating on security. This session explores how coordination of cybergroups are proving to be a vehicle for open and productive collaboration. Learn about how CBEST helped modify the intrusive nature of the testing and has changed the relationship that firms’ cybersecurity teams have with their regulators, reinforcing the desire for a collaborative over a compliance based approach to securing the sector.
Quantifying Cyber-Risk Using Threat Objectives Lifecycle Approach | This presentation will describe a threat objectives approach in quantifying cyber risk and effectively engaging business, management and governance structures in assessing the cyber threat landscape.

Red Teaming the C-Suite: The Ultimate InfoSec Awareness Program | The sad truth is that cybersecurity awareness programs can be stale, boring and ineffective leaving many employees and managers to grudgingly complete their annual training requirement without really understanding the importance of good cyber hygiene. And while you may hold periodic tabletop exercises to test your cybersecurity incident response plan, often the C-Suite is not fully engaged. Red teaming the C-Suite will bring buy-in from your company’s executive leadership team by making cybersecurity personal and tangible, not some abstract discussion point in a slide deck. This presentation will look at ways your internal cybersecurity team can conduct red team exercises on a budget that will engage your C-Suite and hopefully increase their awareness and advocacy (funding!) for your cybersecurity program.

The Year in Cyber: Annual Review and Predictions | What has 2017 brought to the finance sector? The repurposing of sophisticated tools for high-scale ransomware attacks, suspected nation-state watering hole campaigns across regions, copycat DDoS extortionists, network-based ATM attacks, and other threats. It also saw the growth of FS-ISAC in the region, bringing new products to members and services like the Weekly Watch Reports and the new EMEA Business Resilience Council. Join FS-ISAC Staff and members in a discussion over what the past year has seen and where the threat landscape is headed in the near future.

Trends, Predictions and Real-World Tradecraft. The Lessons Learnt in Responding to the Most Advanced Attacks*

What's in Your Digital Footprint? | Organizations have spent massive amounts of money to protect the perimeter of their networks, but if your business exists on the internet, there really is no perimeter. This session will discuss recent attacks on internet-facing assets, such as those on Polish banks in February, as well as critical vulnerabilities that can turn web servers into your worst enemy, like the Apache Struts vulnerability in March. Business and cybercrime are not slowing down – learn how you can be prepared to address these types of threats.

Workshop to Help Members Overcome FS-ISAC Information Overload*

keynote

KEREN ELAZRI
Author

Keren Elazari is an internationally recognised researcher, author and speaker on all matters cyber security and hacker culture. Since 2000, Keren has worked with leading security firms, public organisations, Big 4 and Fortune 500 companies. Her independent research about cyber security has been featured by Scientific American, WIRED magazine, TED.com, VICE Media and more.

Keren holds a CISSP certification and Masters in Security Studies from Tel Aviv University – where she is a senior researcher at the Balvatnik Interdisciplinary Cyber Research Center, And the Founder of BsidesTLV. Keren is also a faculty member of Singularity University, a private Silicon Valley think tank.

In 2014, Keren was the first Israeli woman to speak at the prestigious TED conference. Keren’s TED 2014 talk Hackers: the Internet’s immune system was viewed by millions online, translated to 30 languages, selected for TED.com ‘Most Powerful Ideas’ and Inc.com ‘Top TED Talks for Entrepreneurs’.

MISSION STATEMENT

The Financial Services Information Sharing and Analysis Center (FS-ISAC), established in 1999, is a non-profit, member-driven corporation. FS-ISAC’s mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector’s ability to provide services critical to the orderly function of the global economy. FS-ISAC shares threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid response communications for both cyber and physical events, conducts education and training programs and fosters collaborations with and among other key sectors and government agencies. Learn more at fsisac.com

*Please check back for more detailed information on this breakout session.
## Agenda

### Monday 30 October

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>0800-2100</td>
<td>Registration</td>
</tr>
<tr>
<td>0900-1000</td>
<td>Breakfast</td>
</tr>
<tr>
<td>1000-1015</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>1015-1100</td>
<td>Keynote</td>
</tr>
<tr>
<td>1100-1130</td>
<td>General Session</td>
</tr>
<tr>
<td>1145-1230</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>1230-1330</td>
<td>Networking Lunch</td>
</tr>
<tr>
<td>1230-1330</td>
<td>FS-ISAC 101</td>
</tr>
<tr>
<td>1330-1415</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>1415-1445</td>
<td>Networking Break</td>
</tr>
<tr>
<td>1445-1530</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>1530-1600</td>
<td>Networking Break</td>
</tr>
<tr>
<td>1600-1700</td>
<td>Silver Solutions Showcase*</td>
</tr>
<tr>
<td>1700-1800</td>
<td>Reception</td>
</tr>
<tr>
<td>1800-2100</td>
<td>All Hallow’s Eve Dinner Event</td>
</tr>
</tbody>
</table>

### Tuesday 31 October

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>0830-1800</td>
<td>Registration</td>
</tr>
<tr>
<td>0830-0930</td>
<td>Breakfast</td>
</tr>
<tr>
<td>0930-0945</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>0945-1045</td>
<td>General Sessions</td>
</tr>
<tr>
<td>1045-1115</td>
<td>Networking Break</td>
</tr>
<tr>
<td>1115-1200</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>1200-1330</td>
<td>Innovative Technology Showcase Lunch</td>
</tr>
<tr>
<td>1330-1415</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>1415-1530</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>1530-1600</td>
<td>Networking Break</td>
</tr>
<tr>
<td>1600-1700</td>
<td>CISO Panel</td>
</tr>
<tr>
<td>1700-1800</td>
<td>Trick or Treat Reception</td>
</tr>
</tbody>
</table>

### Wednesday 1 November

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>0800-1745</td>
<td>Registration*</td>
</tr>
<tr>
<td>0800-0900</td>
<td>Breakfast*</td>
</tr>
<tr>
<td>0900-1215</td>
<td>Member Sessions*</td>
</tr>
<tr>
<td>1215-1330</td>
<td>Birds of a Feather Lunch*</td>
</tr>
<tr>
<td>1330-1715</td>
<td>Member Sessions*</td>
</tr>
<tr>
<td>1715-1745</td>
<td>Reception*</td>
</tr>
</tbody>
</table>

* closed to Sponsor Attendees with the exception of companies sponsoring this event

Agenda is subject to change. For an up-to-date agenda, visit [fsisac-summit.com/2017-EMEA-Agenda](http://fsisac-summit.com/2017-EMEA-Agenda)