STRENGTH IN SHARING


Walt Disney World Swan and Dolphin
Lake Buena Vista, FL
30 April - 3 May
WHO SHOULD ATTEND?

- CEO/Bank Owners, CISO, CSO, CIO, CTO and CRO
- Head of Threat Intelligence
- EVP, SVP, VP and Director of these areas:
  - 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 more than three dozen 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
On behalf of FS-ISAC and the 2017 Annual Summit Planning Committee, I am very pleased to welcome you to the 2017 FS-ISAC Annual Summit.

Managing risk in a constantly-changing environment is the unwavering fact of the financial sector, and 2016 is no exception. Just in the last 12 months, we’ve seen the launch of same day ACH, realization of Internet of Things (IoT) as a tangible threat, increased attacks against core payment business processes, not to mention ongoing political change worldwide or the continued focus on nation-state attacks. Our business partners, both internal and external and - most critically - our clients are looking to us more than ever to provide leadership and clarity in this time of change.

This changing landscape calls for a renewed emphasis on business alignment; by broadening our outlook, we can help ensure a resilient and secure financial ecosystem. The good news is we don’t have to handle this transformative environment alone. Over the past ten-plus years that I have been involved in the FS-ISAC, I have personally seen the organization mature from its earliest roots to the multi-national and multi-faceted organization it is now. Whether you represent a global bank, community bank, insurance company or one of our many partners in the financial services sector, the FS-ISAC Annual Summit continues to be the “can’t miss” conference to gain critical insights, collaborate with peers on emerging threats and identify cutting-edge solutions from our vendor partners.

This year is no exception. We’ve put together a program that will provide tangible and actionable information to help you continue to secure your business, your clients and your partners. By sharing our knowledge, we can make our common goals a reality and strengthen the financial ecosystem, defend our brands and institutions and preserve the trust placed in us by our clients.

Thank you for the work that each of you do to help shape our industry and your continued partnership and sharing with one another. I look forward to seeing you in Florida in May!

Matthew Harper
SunTrust Senior VP, Client Security Management

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
ATTENDANCE RESTRICTIONS

The FS-ISAC Annual Summit restricts attendance to regulated financial services firms, relevant public sector entities, and country-level banking associations and payments associations. Examiners and those responsible for informing public policy are not eligible to attend. If you have questions regarding eligibility contact marketing@fsisac.com. If you are a solutions provider, please visit fsisac-summit.com/2017-Annual-Sponsorships. Officials from the FFIEC agencies and CSBS who want to attend the Summit, please contact admin@fsisac.us.

FS-ISAC PREMIER, GOLD AND PLATINUM MEMBERS

Receive complimentary registration passes as follows below. After all complimentary passes are utilized, additional member firm staff may attend at the Standard member registration rate below.

Premier - 2 complimentary passes  
Gold - 5 complimentary passes  
Platinum - 10 complimentary passes

Early Bird Registration ends 1 April.

<table>
<thead>
<tr>
<th>FS-ISAC Affiliation</th>
<th>Early Bird (ends 1 April)</th>
<th>Standard Registration (after 1 April)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premier/Platinum/Gold Member</td>
<td>COMPLIMENTARY</td>
<td>COMPLIMENTARY</td>
</tr>
<tr>
<td>CNOP</td>
<td>$999 USD</td>
<td>$1,750 USD</td>
</tr>
<tr>
<td>Non-Member (eligible FI only)</td>
<td>$999 USD</td>
<td>$1,750 USD</td>
</tr>
<tr>
<td>Basic/Core Member</td>
<td>$999 USD</td>
<td>$1,500 USD</td>
</tr>
<tr>
<td>Government</td>
<td>$999 USD</td>
<td>$999 USD</td>
</tr>
<tr>
<td>Standard Member</td>
<td>$895 USD</td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>Guest</td>
<td>$599 USD</td>
<td>$599 USD</td>
</tr>
<tr>
<td>Monday Dinner Guest Only</td>
<td>$199 USD</td>
<td>$199 USD</td>
</tr>
</tbody>
</table>

CANCELLATION POLICY

Any member/non-member cancellations must be received via email to summit@fsisac.com.

Cancellations received prior to 24 April 2017 will not be subject to a cancellation fee. Cancellations received on or after 24 April 2017 will be subject to a $200 USD cancellation fee. This applies to all members at all tiers as well as non-member, guest, government and CNOP registration regardless of if a registration fee was paid.

Registrations are transferable within an organization without penalty.

ONLINE REGISTRATION

fsisac-summit.com/2017-Annual-Attendee-Registration
Eric O’Neill
Former FBI Operative and Subject of the Film Breach

In 2001, Eric O’Neill helped capture the most notorious spy in United States history: Robert Hanssen, a 25-year veteran of the FBI. The remarkable true events of his life are the inspiration behind the critically acclaimed dramatic thriller Breach, starring Ryan Philippe as O’Neill. The film set inside the FBI - the gatekeeper of the nation's most sensitive and potentially volatile secrets - is the story of the greatest security breach in US history.

Preceding Hanssen's arrest, O’Neill worked with the spy within the information assurance division that protected all classified FBI intelligence. O’Neill gained Hanssen's trust and used that relationship to slowly draw the traitor out of deep cover.

O’Neill began his career in the FBI as a graduate of the FBI’s Intelligence Program. He spent the first five years of his career as a special surveillance group field operative tasked to surveil and monitor foreign, national, and domestic terrorists and spies. He transitioned from field operative to direct undercover work focusing on Hanssen. Although his prior training had focused on “ghosting” targets from the shadows, he engaged his target in conversation in order to elicit information needed to catch Hanssen in the act of espionage. The singular nature of the assignment, one with little backup or support, required O’Neill to draw from deep reserves of courage and confidence within himself to battle Hanssen's mind games and aggressive probing and learn to "stop reacting to Hanssen and begin acting."

Currently, O’Neill runs The Georgetown Group, a premier investigative and security consultancy, where he specializes in counterintelligence operations, investigations into economic espionage, cybersecurity penetrations, internal investigations, catching the trusted insider and security risk assessment consulting out of Washington, DC. O’Neill also serves as the National Security Strategist for Carbon Black, the leader in next generation endpoint protection.

O’Neill’s story is one of patriotism, of decisive action in the face of fear, and of learning to maintain confidence in ability even if it looks like success is impossible. He has told his story in national media, in print, on radio, and on television including 20/20, Nightline, Hardball with Chris Mathews, Fox News Power Player of the Week with Chris Wallace, CNN, CSPAN’s Washington Journal, NPR’s Fresh Air with Terry Gross, World News Now, MTV and Access Hollywood.

A talented motivational speaker who weaves real life experiences into a presentation that is both entertaining and rewarding, O’Neill provides practical insights into real work situations relevant to many industries. In addition to his experience in the Hanssen case, he also addresses the issues of confidence and patriotism, the threat to United States security posed by terrorism, foreign intelligence services, the cyber threat to our national infrastructure and the national conscience in a monitored society.

location

Walt Disney World Swan and Dolphin
1500 Epcot Resorts Boulevard; Lake Buena Vista, FL 32830
swananddolphin.com

The 2017 FS-ISAC Annual Summit is being held at the Walt Disney Swan and Dolphin. FS-ISAC has reserved a block of rooms at the Walt Disney World Swan and Dolphin at a group rate of $249 USD per night (plus tax). Please make sure to reserve your room now as the block will fill quickly. Reservation requests for the FS-ISAC Annual Summit will be accepted through Friday 7 April 2017. The block is available up to this date or until the block is full. Reservations requests received after 7 April are on space and price availability.

To make your reservation please use the online reservation link: swandolphin.com/groupres/2D22AC
fsisac-summit.com | fsisac.com
innovative technology showcase

You will want to make sure to add these showcases to your schedule in Lake Buena Vista. The Innovative Technology Showcase sessions are not product or sales pitches but short, bite-sized discussions around industry related topics, issues and interests. Designed to be similar to TED Talks, these eight-minute sessions offer an unique experience to hear expert dialogue from vetted and approved sponsors.

- **Attivo Networks** | What’s In Your Network? How to Find Out, What to do About it and How to Prevent it in the Future?
- **Grimm** | The Art of the Possible in Threat-Based Assessments
- **Invincia** | How Machine Learning and Artificial Intelligence Will Transform Antivirus
- **Pindrop Security** | Love and Marriage, Fraud Detection and Authentication: You Can't Have One Without the Other
- **Skycure Inc.** | New OS Upgradability for Better Android Security
- **Sqrrl** | Threat Hunting Beyond the Hype
GENERAL SESSIONS

Cloud Migration 2.0: Securing Data in Home-Built IaaS Applications | The path to the cloud may start with SaaS applications, but the destination for mature cloud programs includes IaaS and PaaS. Cloud-first companies want the performance and cost benefits of cloud for all their computing solutions. Enterprises have dozens or even hundreds of custom, home-built applications for employees, partners and customers. Between code repositories, partner portals and customer-facing systems, custom applications contain vital and sensitive data. Cloud companies invest more in infrastructure security than the vast majority of enterprises, but customers are responsible for preventing data leakage or theft. Before application teams move their home-built services to the cloud, security must ensure critical prerequisites are met. In this session, learn how CISOs are bridging the gap between application development and security teams to safely migrate their home-built applications to PaaS and IaaS environments. Specifically, learn from experiences implementing critical security capabilities like data loss prevention, activity monitoring, threat protection, and access control for custom applications in the cloud.

Coming Convergence of Cyberdefense and Information Sharing | This discussion will focus on the broader convergence of cyberdefense with automated threat sharing and response, and preview new approaches for weaving human collaboration and Machine Readable Threat Intelligence (MRTI) capability together more effectively in assessing potential impacts and defenses across sharing communities in response to cyberthreats.

Community Institution Breakfast Session | Bring your breakfast and join FS-ISAC community institution members and share in camaraderie, coffee and conversation. It’s a chance to talk about the challenges you’ve had, successes you’ve enjoyed and impressions of the Summit. This open discussion breakfast will be led by community institution Advisory Group members... enjoy a good breakfast, ask questions and share information you have with your peers.

Digital Disruption – But at What Price? | As financial institutions pursue digital strategies, their operations become part of an evolving and often poorly understood cyber-environment. In this connected ecosystem of entities, people and data, firms are using mobile/social channels to transact. This means organizational perimeters have all but disappeared. We have opened up new avenues of cost-saving, agility and speed-to-market, but at what price? Success will require focus on establishing trust as the blueprint for differentiation in a fast-paced digital world. The confidence with which organizations interact with their stakeholders via complex and evolving digital platforms will be enough to make or break a business. In this session, learn how integrating cybersecurity with digital, companies can deliver value from risk and shift from prevention to enablement. By managing traditional and digital risk, companies are well-positioned to defend their businesses, ultimately turning them into digitally trusted partners – both internally with employees, and externally with customers.

Fraud Detection and Advanced AI for Cyberthreaths | For many years, financial institutions have been on the bleeding edge of Artificial Intelligence (AI) development as they work to detect and prevent real-time payment fraud around the world. For the past 20 years, FICO has been at the forefront of these developments, working with these institutions to deploy enterprise-grade, machine-learning applications. This session will present how these real-time, self-learning anomaly detection and entity behavior analytics are now being applied to detect cyberthreats and malicious insiders in our digital ecosystem.

Next-Gen Security Intelligence and Operations Centers - From Training to Cognitive | Discover how the next generation of SOCs are being built. Moving away from classic IT “moat and castle” approaches towards end-to-end incident handling, cognitive computing and even military grade cybertraining. The session will start with a brief intro to today’s approach and examples, including how financial services firms are building next-generation SOCs to handle every aspect from prevention to detection, mitigation, incident response, data sharing and media handling. Learn first-hand from experiences training security teams and doing live SOC simulations. Discover how cognitive computing is evolving into a game changer for security teams fighting fraud and cybercrime. Finally, a discussion around current threats facing the financial industry in areas such as IoT and the latest trends from cybercrime groups using the dark web, including real world examples of how companies are dealing with these security issues.

Opportunities and Challenges in Engineering Mobile Centric, Omni-Channel Identity for Password Replacement | Banks and transaction processor application owners are inundating IT and security teams for new requests for identity related projects (such as biometrics), yet the ability for the organization to execute on these requests takes a very long time and costs a lot of money. At the same time, the mobile device is presenting many new opportunities to eliminate passwords and to simplify the identity customer experience across web, mobile, branch and phone channels. This panel will discuss how organizations have made sense of this complex maze, and discuss the next generation of identity architectures being introduced to dramatically reduce internal costs, increasing delivery response times for thousands of use cases and future proofing their environment from vendor lock-in.
Build Your Cyber A-Team and Strengthen the Cybersecurity Workforce | Building and maintaining a strong cybersecurity team can be challenging. Employers often struggle to find candidates with the right skills and spend months training them, only to lose them to a competitor. Fortunately, new standards have prompted the creation of programs, tools and guides that can help. In this session, participants will be guided through the tools, templates and information that DHS has developed for organizations as they address cybersecurity workforce planning, recruitment, retention and training issues. Additionally, learn about the National Cybersecurity Workforce Framework and how you can use it to strengthen the cybersecurity workforce!

SWIFT's Customer Security Program - Supporting the Community in Strengthening Security | Cyber-attacks are growing in number and sophistication and attackers are focusing more deeply inside banks. Recently publicized cases show attackers have started by exploiting security weaknesses within institution's local environments to steal valid operator credentials to their local payment infrastructure. They input seemingly legitimate payment instructions with those valid credentials and hide the evidence of fraud. Combating fraud is a challenge for the whole industry – there are no quick fixes. The threat landscape adapts and evolves by the day, and while customers are responsible for protecting their own environments, SWIFT’s Customer Security Program (CSP) has been established to support customers in the fight against cyber-attacks. This session will provide an overview of the program, the successful milestones already achieved and how we continue to jointly work to mitigate the risks of these ever-increasing threats.

The Three T's of Cybersecurity | Talent, tools and techniques... represent the three T's of cybersecurity. Obviously, the scarcity of talent represents a significant challenge to any enterprise managing a security program. So, which of the T's is the most important? Learn the answer from an industry veteran who will share many examples of unconventional controls that yield favorable business results.

Avoiding APT Misattribution with Indicators of Deception | Advanced persistent threat (APT) cyber-attacks—orchestrated by sophisticated criminal groups or by state-sponsored hackers—always employ a level of deception by misdirecting pursuers into misattribution. Cybersecurity researchers are already burdened by their competitive commercial landscape in post-incident reporting and today's media outlets often prioritize speed and sensationalism that may cause cyber-attacks to be attributed too quickly. To the benefit of APTs this pressure can lead to misattribution caused by poor due diligence enabled by analytical errors and shortsightedness. Consequently, cybersecurity researchers need a logical approach to discover indicators of deception (IoD) and avoid APT misattribution. Because APTs easily and effectively employ deception to evade responsibility and retribution, the trend will likely continue due to ever competing financial and political-military interests. This session aims to enhance cybersecurity researchers’ ability to identify IoD and confirm the misdirection – even under rapid publication deadlines.

Board Reporting is Not Boring | Many boards discuss cybersecurity with management when cyber-attacks are widely reported or when the financial institution experiences an attack. However, routinely discussing cybersecurity issues in board and senior management meetings will help the financial institution set the tone from the top and build a security culture. In this panel presentation, learn what some community institutions are doing to inform and educate their boards.

Building a Risk Assessment Process for Small Institutions | Safeguarding an institutions critical information assets and systems has never been more important in the age of evolving cyber threats. Enterprise risk management (ERM) is a fundamental approach for the management of an organization. IT enterprise security risk assessments are performed to allow organizations to assess, identify and modify their overall security posture and to enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an attacker’s perspective. In this presentation, learn how small institutions have built an effective risk assessment program and increased the overall security culture in their organizations.

Edgile | Case Study on Governance Refresh | The recent updates to the FFIEC Management and Information Security Handbooks necessitate a highly organized level of alignment. Not to mention today’s cyberthreats require this level of coordination and collaboration. This presentation details a case study on operationalizing information risk management policies across three lines of defense using a service catalog. Learn how the service catalog approach allows organizations to clearly define roles and responsibilities between front line risk takers, second line risk oversight and third line audit providing accountability and enabling a glide path for a maturity roadmap to incrementally improve the service capabilities over time.

Cybersecurity: Threat Landscape and Internal Audit | This session will focus on how an internal audit of your organization can provide details on coverage of cybersecurity. Topics that will be discussed include: the cyberthreat landscape – actors and methods, current cyberthreat trends, knowing the enemy, insider threat, “attacker already has access”, cyber-attacks, internal audit best practices, information security auditor engagement model, “defense in depth” audit coverage and audit coverage mapped to key risks.

DMARC Quick Start Guide | This session is a practical discussion on the implementation of DMARC for financial institutions. Learn actionable items to assist in implementation and adoption as well as best practices for a smooth transition.
Ducking Threats Globally - Threat Management for the Global Organization | Threat management has evolved becoming a critical component of a mature security program. For many businesses, this means that threat intelligence processes and systems must expand beyond domestic headquarters. This session will discuss successes and lessons learned in taking a cutting-edge threat intelligence platform used in one country and expanding its accessibility, user base, architecture and processes to support around-the-clock operation, analysis and control deployment in multiple geographic office locations. Topics discussed will include architecture considerations, legal and compliance hurdles, cultural nuances, process design and tangible results.

Deloitte | Financial Services Cyber-Regulations and RegTech: Emerging Trends, Opportunities and Risks | Increasing regulatory and threat environments are driving organizations to demand more from their cybersolutions. While new rules and regulations such as those from the New York State Department of Financial Services, Federal Financial Institutions Examination Council and the EU’s General Data Protection Regulation are requiring more prescriptive frameworks than existing regulations, increasing cybersolution complexity. This presentation will explore topics such as what impacts the new regulations have on existing operations; how CISOs and CROs should work together to stay focused on the organization’s risk and threat tract while remaining compliant; and what is adhering to these new regulations going to cost.

KnowBe4 | Financial Services Social Engineering and CEO Fraud: the $3.4 Billion Mistake | Social engineering methods and the “evil genius” of CEO fraud are costing businesses billions of dollars with little chance of recovery. Ransomware is one of the top three most dangerous security threats and continues to proliferate despite the best efforts of endpoint security and gateway solutions to block them. How do you manage the ongoing problem of users falling for social engineering attacks and what are the most effective methods for securing your organization to combat cybercrime? This presentation will cover how financial institutions can stay ahead of social engineering traps and lower risk.

From Consumer to Producer: Taking Your Community Institution to the Next Level | Are you interested in doing more than consuming intelligence, and learning how to join the fight against malware and other threats? It is vital to the health of a sharing community that everyone do what they can to contribute, but many of us are not sure how or where to start. Well, with very little time and commitment we can generate valuable data as well as sharpen our senses in defending our own institutions. This session will share some simple ways to take your institution from a threat intelligence consumer to a threat intelligence producer by covering topics like data visualization (email and web), malware and endpoint analysis, network forensics and honeypots.

Myths of Cybersecurity | This presentation will shed light on some of the various myths amongst information technology professionals and others about cybersecurity controls and how effective they are in reality. Some misconceptions are dangerous to organizations in that they may believe a control or set of controls make them safe from malware and other forms of maliciousness. This presentation will clarify and correct some of these common misconceptions. Participants should leave the session with a better understanding of what certain common controls do for them and what they don’t do.

Non-Conventional Data Gathering Using Huginn and Elasticsearch | Today’s InfoSec world is a fast-paced society in which vast data is available at people’s fingertips. Searching, organizing and deleting relevant information from this data is the key to succeeding in accurately stopping threats in a timely manner. This session will discuss and showcase the dual-usage of Huginn and Elasticsearch to implement the automatic monitoring of several sources of useful unstructured information at a minimal cost to the organization.

Steganography-Stealing Data in Plain Sight | Stealing data is easier than you think and could happen right in front of you. Concealing data within multimedia, operating systems and network traffic provides covert transfer of valuable data. The art of sending covert messages has been around for thousands of years and modern technology has facilitated the ability to hide messages (and data) in common media to avoid detection. As technology changes, the methods of stealthy communications seems to get easier to conduct but harder to detect. This presentation will explore various approaches to hiding data and covert communications. It will explore the tools and techniques used to hide this data in common transport carriers as well as provide a broad understanding of how these methods work. Armed with this information, participants will be better able to identify where they may be at risk for data exfiltration via steganography.

The Challenges and Success of Employing an Information Security Analyst in a Community Bank | An information security analyst should be the “champion” of information protection for his or her community bank. To be effective and make their voice credible, the analyst must understand their bank’s significant business operations and the related technology and information assets which must be protected. He or she should approach every day with the mindset that the bank must do all it can to protect its information assets and those of its customers. This doesn’t necessarily mean saying “NO”, but rather finding solutions that balance business needs with security and regulatory requirements. Practically speaking, the analyst must have an equal “voice at the table” and be willing and able to stand firm and communicate to management if security or related compliance is jeopardized at the expense of advancing business objectives.
The Life of a Trade from InfoSec Perspective | This presentation will walk through and highlight the internal and external systems used as well as what information is shared to create a trade in the securities industry.

Interset Software | Use Case: How One Global Bank Utilized Security Analytics to Mitigate Fraud | Fraud costs financial services companies hundreds of millions of dollars every year. Existing detection products are unable to surface fraud on a broad spectrum. Security analytics offers a new approach to fraud detection for both employees and online. This presentation will detail the implementation of a fraud detection project featuring the use of advanced security/behavioral analytics. Learn how a security analytics product can be utilized successfully, best practices and lesson learned from the project deployment and ongoing operations.

Where Privacy and Security Intersect | Information security and information privacy are not the same. Regulations are looking towards a risk assessment, which looks at the threats, vulnerabilities and the likelihood that those events will represent a risk to the organization based on their likelihood and impact. One of the largest risks today is that of unauthorized information disclosure. There are an increasing number of privacy concerns that security managers need to start becoming familiar with. While they don’t need to become attorneys, they need to realize the requests that various legal entities will request. Keeping a secure system is a great step, but if privacy isn’t part of the decision process, the secure system stays secure only for so long. Understanding the privacy requirements helps the security manager prioritize their efforts. When security ultimately fails, whether due to a technical or process-based reason, the privacy protections help limit the exposure of the incident.

CONCURRENT SESSIONS

A Collaborative Approach to Third-Party Risk Management: A Case Study | In this session, hear about a best practice framework for reducing the potential risk from third-party vendors by developing a collaborative, ‘synapse’ ecosystem that helps companies both big and small effective manage their vendors. This approach reduces both time to completion and overall cost of evidence collection as well as greatly reducing the risk posed by third-parties.

Adversary-Centric Threat Hunting and Mitigation | There are a variety of ways to go threat hunting in an environment. Leveraging threat intelligence to mimic adversaries observed attacking the environment or suspected to have an interest in attacking the environment can be a very effective counter to threats both observed and yet to be seen. This session will focus on a method of threat hunting that involves simulating attacker activity, scouring logs for evidence of that activity and then searching iteratively across the environment for signs of that activity. Additionally, going a step further will discuss how to develop countermeasures and mitigations against such tools and attacks can carry this approach into a quasi-red team activity.

An Enhanced Approach to Cybersecurity Risk Assessments: Using Advanced Adversary Simulations to Drive Real World Results | In this session, learn the benefits of combining a risk assessment with advanced adversary simulation. Hear how leading organizations can evaluate both the maturity and the effectiveness of their information security program to drive an outcome that is a more comprehensive cybersecurity risk assessment and empirical evaluation of their attack resiliency, driving enterprise-wide results.

Autism and Cybercrime - Profiling Offenders by Behaviors | More than half of cyber-offenders are determined to be on the Autistic Spectrum. The nature of their disorder and the one-dimensional, black and white environment of the internet makes technology an attractive draw for people who find the real world difficult to navigate. They find that, due to the nuances of their disorder and their skill set, they can veer into criminal activity without thought for the consequences. A lot of high-profile hacking cases have determined the offender(s) to have an autistic disorder. In this presentation, learn how this conclusion has been arrived at via a study being conducted in the UK with the support of the UK government and law enforcement.

Betrayal-as-a-Service: Trends in Insider Threat | Insider threat is a trending avenue for malicious actors. Insiders can provide the necessary information and insight into increasingly complex systems, as illustrated by the Bangladesh bank hack in early 2016. Additionally, government agencies are enacting costly regulations, requiring the establishment of corporate insider threat programs. Yet there is no universal definition nor response to 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 indicators of insider threat outside your networks. Also, this session will explore cost effective solutions to implementing continuous monitoring and response to insider breaches, while protecting and respecting the individual privacies of your employees.

Building the Right Team: Successfully Intertwining Cybersecurity and the Legal Team | You’re the security professional who just told the general counsel about a successful cyber-attack on your organization. Who takes the next step, you or legal? Which of you owns the incident response plan? Who is going to contact the CEO? Who is going to brief the Board? What are you required by law to do next? What should you do next? This session will discuss the role the legal department needs to play as part of cyberthreat detection, response planning and execution as well as how to develop a sustainable and cost-effective intelligence-led solution to cyberdefense.

Closing the Vault: Defending Your Organization Against Cybercrime-as-a-Service | Cybercrime-as-a-service (CaaS) is an important trend in deep web forums because it puts
cybercriminal tools and services in the hands of a wider range of threat actors—even the nontechnical, such that anyone can become a cybercriminal with minimal investment. Enterprise networks have become targets for evolved versions of CaaS, including Ransomware-as-a-Service and even Espionage-as-a-service. This session will provide insight that information security and IT leaders need to know to protect their organizations’ critical assets by outlining a typical attack chain and identifying different entry points and evasion techniques utilized by malicious actors. Learn specific steps that information security leaders can implement to guard against evolved threats and the role that innovative technologies, such as machine learning, can play in defending against even hard-to-detect threat components such as exploit kits.

Cloud Security - Lessons Learned | The agility and cost advantages of migrating to public and hybrid cloud environments as well as consuming software-as-a-service are causing significant shifts in how financial institutions (FIs) consume and manage information technology. One of the biggest question marks for FIs is how to support and maintain security and compliance requirements in the cloud. This session will provide lessons learned from real-world cloud implementations, present a framework for secure cloud computing and outline best practices for cloud security with a particular focus on how cloud security differs from data center best practices.

Community Institution Discussion Forum | An open-floor, panel-led session discussing the successes, trials and pitfalls unique to community institutions. This discussion-driven forum is specifically tailored for community banks and credit unions, with discussion topics sourced from both the panel and the audience. Discussion will include building and maintaining a healthy information security program, threat intelligence for community institutions, risk management and much more.

Cyber-Intelligence Meets Information Sharing | Cyber-intelligence is a crucial component of any cybersecurity program as well as the need to share threat data across verticals. In this session learn the difference between threat data and threat intelligence and more importantly the who/what/when/where/how of sharing that threat data so your defense can be another companies’ offense.

Cybersecurity Scorecard: Does Your Organization’s Security Posture Stand Up? | The financial industry has a higher cybersecurity maturity than other industries, yet it often fails to prevent modern cyber-attacks, including attacks involving ransomware and polymorphic malware. These failures are spawning more public scrutiny and increased regulatory oversight. To better prevent these attacks, organizations must be able to quickly identify them and close security gaps within their environments. Creating a more mature security posture begins with an honest assessment of where your organization currently stands. This session will detail how organizations can lower their liability against regulatory pressure, reduce security threats to their enterprise, ensure data-security and regulatory accountability and the pressures organizations face when balancing security risks and regulatory mandates. Attendees will leave the session empowered to construct a cybersecurity “scorecard” for their organization, measuring the true regulatory and security postures of their enterprises.

Cybersecurity: Why are We Failing? | Security technology vendors are failing! Despite the increased investments in technology, we continue to see high-volume, high-impact breaches. This presentation will look at evidence from real breaches to try and understand why technology-only approaches to protecting our key assets are failing. Additionally, there is a lot to learn from the military’s approach to effective intelligence gathering, human conditioning and how to operationalize them. This session will also look to translate these lessons to the realm of cybersecurity.

Deconstructing Elite Credential Theft Services | Several high-intensity criminal operations dominate the field of credential theft malware, which drives account takeover fraud affecting financials worldwide. Key threats in this area Trickbot, Dridex, Vawtrak, Ramnit, Ursnif and others. This presentation will examine the current characteristics of these organizations and the trajectory of fraud they enable.

Demystifying Lateral Movement - A Pragmatic Approach | After obtaining an initial foothold on an environment, sophisticated attackers need to embark in lateral movement (LM) tasks to be successful in identifying and exfiltrating sensitive information. Being a buzzword, LM is sometimes perceived as a magical thing attackers perform as part of a breach without really understanding it. As defenders, we need to have a clear understanding on how LM can be achieved. This presentation will describe how an attacker can perform LMs and what can cyberdefenders do to prevent and detect it.

Disruptive Defense | It is said that the definition of insanity is repeating the same actions and expecting different results. So, how can we break away from Fiserv “group think” to make it harder for attackers? Is the best defense a good offense? Should we follow the Chinese model of collecting threat intelligence? Join this session to hear from a panel, including industry leaders, who will discuss disruptive defense techniques, some of which may be politically incorrect. Audience participation will be encouraged.

Fighting Cybercrime in a Cloud-Based World | With the move to the cloud, criminal organizations are not changing their targets, but they are evolving their behavior. This session will discuss the evolution of cybercrime and disruptive malware impacting financial institutions and their customers. Learn more about these evolving threats and how using creative legal strategies, with an increased focus to locate the criminal organizations and produce actionable criminal referrals to law enforcement, is helping to facilitate arrests of these criminals. Join this session to learn how Microsoft and FS-ISAC are working to help your organization guard against cybercrime.

Financial Data Protection, Visibility and Control: Security for Regulated Data, Cloud and IoT | A significant challenge in the financial sector is protecting highly regulated, structured and unstructured data. This data is highly sought after by criminals, yet the ubiquitous sharing of it across platforms and enterprises is essential for financial companies to
conduct business. This means, unlike most other industries, finance has one of the largest attack surfaces. What is needed is a control that can easily plug into the financial ecosystem and seamlessly provide visibility, control and protection for the most sensitive data. See how top financial companies are approaching some of these challenges within their organizations and understand how a data-centric information protection strategy can enable secure sharing of critical data not only within your own organization but also between consumers, banks, payees, vendors and beyond.

Finding Signal in the Noise: Leveraging Fraud Analytics to Identify Emerging Fraud Schemes | The diversity of available payment types has led to an evolution of how cybercriminals exploit payment systems for financial gain. These new payment types as well as new technologies developed to combat fraud have led to innovative fraud schemes that require new methodologies to uncover them. Building on sessions from the past three summits, this talk explores how big data analytics can be applied to transactional data to uncover emerging fraud schemes. These analytics allow for the quicker identification of compromised merchants and lead to proactive measures to stop payment card fraud before it occurs. This presentation will provide numerous case studies and detailed methodologies that attendees can leverage in examining their own data.

How to Showcase Your Intelligence Program to Your Board with a Live Attack | Show your board how tactical intelligence can stop an active attack. This presentation will show you an incredibly impactful way to showcase what an attack looks like, how easy it is to execute and the importance of intelligence in the defense of the network. This session will showcase an incredibly impactful way to highlight the importance of intelligence to an organization by showing how intelligence is used to detect a live attack. A demonstration and all material will be available so you can do this for your executives/board.

Hunting for Security Threats, Lessons Learned from Three Years Building Hunt Teams | During this session learn about building "hunt" capabilities that search for security breaches including those around SWIFT vulnerabilities. Hunt teams are relative newcomers within the security operations domain. Many companies say they are doing "hunt" but when one digs deeper the capabilities are ad hoc, with no measurable indicators of success nor formal organizational support. That means hunt teams are growing in popularity and use without a "gold standard" for how they work. In this session, lessons learned will be shared transparently so the audience can learn from past experiences. You will leave with a better understanding of what a hunt can be (if run successfully) and a broader view of the ecosystem of breach hunting technology and organizational considerations.

Lessons Learned: How to Ramp Up Your Application Security Program | Most financial services organizations today understand the serious implications of a data breach. At the same time, most may not be funneling enough money or resources toward application security – an initiative that could greatly reduce the risk of a data breach. This disconnect can stem in part from simply not knowing where to start. In this session, learn about getting started with application security, getting teams on board with application security, integrating security into development processes, measuring AppSec success and managing and maturing an application security program.

Leveraging Threat Intelligence for Small to Mid-Sized FIs 2.0 | Back due to popular demand, this standing room only session is returning for 2017. In this discussion session, hear industry experts share their experiences in utilizing threat intelligence (TI) and automation. Special attention will be given to the unique ways a small or midsize FI can collaborate and participate in TI sharing with the larger community, including building an effective TI program on a shoestring budget, technology implementation (Punch+, STIX, etc.) and more.

Odinaff: High Stakes Cybercrime | Since January 2016, campaigns involving malware called Trojan.Odinaff have targeted financial organizations worldwide. The attacks are extremely focused on organizations in banking, securities, trading and payroll sectors. The attacks also share links to the Carbanak group, which specializes in high-value attacks against financial institutions and has been implicated in a string of attacks against banks and PoS intrusions. This session will discuss the attacker’s method of operation and the malware identified during investigation.

Operationalizing the Cyberdefense Matrix | This is the third part in a series about the Cyberdefense Matrix (CDM) and how it can be used to understand, strengthen and mature one’s security program. This session covers how to operationalize the CDM to organize the security team and consistently determine what are the ideal handoffs among business partners. In addition, learn how the CDM can explain and deconflict some of the latest security trends, including microsegmentation, behavior analytics and solutions to destructive attacks.

Portraits of the New Cyberdefender: Behind the Looking Glass | How do security teams change skill-sets and mindsets to defend themselves in the new threat landscape? Created from more than a year of in-depth interviews, this session will present five detailed profiles of the cybersecurity organization, including how teams are structured, staffed, trained and motivated. Learn how teams are weaving in more human and threat intelligence - from understanding the adversary, infrastructure, tools and tactics used into the workflows of security operations at a practical level to the benefits and challenges.

Security Insiders: Talent Attraction, Retention and Development | This session will provide tips and tricks about how you can attract, retain and develop talent for information security positions. Learn how to attract interns, entry level and experienced hires including tips for female and diverse hiring, retention and development. Attendees will walk away from the session with tips to take back to their organizations.

Subdomain Infringement: When Your Own Domain is Used Against You | Infringing subdomains are extremely dangerous and destructive to your brand and security posture, enabling phishing, account takeover and fraud from your own registered domain. This session will cover how subdomain
infringement works, how prevalent this threat is using five leading financial services companies as real examples, and how FIs can detect and prevent subdomain infringement.

The DNC Attack - Exclusive Insights and Case Study | The hack of the Democratic National Committee (DNC) during the course of the US Presidential Election was perhaps one of the most consequential cyber-intrusions of all time. Hear the exclusive inside story of that event upon completion of a compromise assessment, which resulted in their discovery and public attribution of Russian government intrusions and follow-on incident response investigation. Practical lessons learned from the incident will be shared with you that are invaluable for defending your networks against these types of attacks.

The Dynamic Duo: Threat Intelligence and Security Operations; They Don't Have to be Together to be Great, Do They? | In this panel presentation, representatives from three major banks will present their views and experiences on the collaboration between threat intelligence and SOC functions. They will discuss what is being done to foster collaboration, innovation and partnership to protect their respective organizations, including going beyond the IOC’s and how the SOC gives back.

Updates on Cyber Regulations | The session will provide a walk-through of recent regulatory changes and explore suggestions on how best to approach the process of compliance with these regulations. Following a similar path as the NY Department of Financial Services with their proposed cybersecurity regulations – the Office of the Comptroller of the Currency (OCC), the Federal Reserve System (FED) and the Federal Deposit Insurance Corporation, released enhanced cybersecurity management standards for large and interconnected entities under their supervision. These regulations address five categories of cybersecurity: cyberrisk governance, cyberrisk management, internal dependency management, external dependency management and incident response and cyber resilience and situational awareness.

Ushering in the Era of Big Data Security Analytics | Security leaders have accepted a realistic but pessimistic outlook – the question is not “if” but “when” their organization will be breached. Those tasked with protecting valuable assets have operated with tools that are incapable of recognizing threats to what they’re actually defending: the data! But today, advances in big data analytics, behavior analysis and unsupervised machine learning are enabling real-time detection of threats that were invisible to legacy security tools such as insider threats, fraud, cyber-attacks and abuse of privileged access. This panel presentation will feature insights into new analytical capabilities that predict, prevent, detect and contain threats with unprecedented accuracy.

Why the World’s Leading Banks are Inviting Hackers to Help Protect Their Applications and Networks? | Hackers who help protect billion dollar accounts rather than pilfer them? What has led to this previously unimaginable adoption of crowdsourced security testing by the world’s largest financial services institutions? This session will discuss how global banking and financial services institutions are embracing hacker-powered, crowdsourced security initiatives to help secure even the most sensitive applications and network environments. In this session, case study examples will be used to show how some of the world’s largest banking organizations are currently utilizing crowdsourced teams of trusted ethical hackers to: detect and report holes in critical financial/banking applications and networks to protect highly confidential and valuable information proactively; understand how areas of weakness and subsequent exploitation relates to overall business risk and how vulnerabilities can be prioritized for remediation accordingly; and gain a true understanding of how an adversary views your networks and digital applications.

Will the Real Cyber-Attack Please Stand Up? | Experts say the next black market is digital certificates. But most organizations don’t fully understand how these digital assets are used in cyber-attacks. In this panel discussion, leaders in FS-ISAC member firms will represent both true and false aspects of current advanced cybercrime that misuse certificates, and the audience will test their knowledge using interactive polling. Each panelist will represent a possible attack characteristic—only one will be accurate and the others will highlight common misconceptions. After the audience submits their vote through interactive polling, the “real” cyber-attack will stand up and provide real-world guidance on how to detect, prevent and remediate this type of advanced cyber-attack.

"You're Going to Need a...": Security and Risk Management Lessons from Jaws | The classic 1975 film, Jaws, presents a unique and fascinating perspective on security threats, risk management and incident handling. The session will examine key scenes from the iconic movie and apply them to real-world security threats that are facing financial institutions. Attendees will leave with a fresh perspective on applying security practices to their organizations. Remember, "it's only an island when you look at it from the water."

*Sessions subject to change.
silver sponsor
solutions showcase

Join us for complimentary snacks, refreshments and a technology showcase where the latest technical innovations in cyber-awareness, proactive security and defense will be on display. In this relaxed setting, attendees may select up to three solutions they would like to see. These information-packed, 15-minute sessions will be presented by technology experts from our solution providers, be use-case driven and tailored to the unique needs of FS-ISAC members.

Amazon Web Services | Security Essentials When Migrating to the Cloud
BitSight Technologies | How to Get Control of Third-Party Risk
Denim Group | DevOps and Software Risk for Highly Regulated Industries
Digital Defense, Inc. | Industry Best Scan Engine Effectively Powers IT Security Automation Platforms
Early Warning | Minimizing Fraud and Risk at New Account Onboarding Through Advanced Identity and Authentication Solutions
Endgame | How to Identify and Eliminate the Blind Spots for a Drama-Free Security Program, Effective Against the Next ‘Next Generation’ of Attacks
Fireglass | Any Website, Every Email, 100% Secure
Flashpoint | Business Risk Intelligence: Shaping the Future of Enterprise Protection
ForeScout | IoT Security: How to Make the Invisible Visible
Gurucul | Borderless Behavior Analytics - Top 10 CSO and CISO Insights
Kenna Security | Intro to Kenna: A Risk-Based Approach to Vulnerability Management
Level 3 Communications | Mirai Botnet: A Timeline Through the Eyes of the Customer and Provider
Menlo Security | Isolation as the New Security Standard for Bank Security
Netskope | How The Cloud Allows Ransomware to Hide in Plain Sight
NuData Security | Passive Biometrics Beats Fraudsters by Using Their Own Behavior Against Them
Optiv | Defuse the Data Bomb
Preventy | Say Goodbye to Vulnerability Backlogs: Using RASP to Reclaim Control and Reduce Risk
Security Compass | Building a Blueprint for Financial Industry Security
The Media Trust | You Have Threat Intelligence in Your Arsenal, So What?
TITUS | Identify and Protect Sensitive Data Across the Enterprise
TopSpin Security | Using Deception to Hunt Cyber-Attackers
UpGuard, Inc. | Cyber-Insurance as Part of a Business Resilience Strategy
Varonis | The Enemy Within: Detecting and Mitigating Insider Threats
Wombat Security Technologies | Preparing End-Users Beyond the Phish
<table>
<thead>
<tr>
<th>Sunday, April 30</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4:00-6:00 p.m.</td>
<td>Beach Blast</td>
</tr>
<tr>
<td>6:00-7:00 p.m.</td>
<td>Welcome Reception</td>
</tr>
<tr>
<td>7:00-9:00 p.m.</td>
<td>Sponsored Member Dinners</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monday, May 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7:00 a.m.-8:00 p.m.</td>
<td>Registration</td>
</tr>
<tr>
<td>7:00-8:00 a.m.</td>
<td>Board and Member Breakfast**</td>
</tr>
<tr>
<td>8:00-9:30 a.m.</td>
<td>Board Meeting**</td>
</tr>
<tr>
<td>9:30 a.m.-12:00 p.m.</td>
<td>Members Meeting*</td>
</tr>
<tr>
<td>12:00-1:15 p.m.</td>
<td>Members Birds of a Feather Lunch*</td>
</tr>
<tr>
<td>1:15-2:00 p.m.</td>
<td>Desserts in Sponsor Hall</td>
</tr>
<tr>
<td>1:15-2:00 p.m.</td>
<td>FS-ISAC 101 with Desserts</td>
</tr>
<tr>
<td>2:00-2:30 p.m.</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td><strong>2:30-3:30 p.m.</strong></td>
<td>Keynote</td>
</tr>
<tr>
<td>3:45-4:45 p.m.</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>5:00-6:00 p.m.</td>
<td>Solutions Showcase***</td>
</tr>
<tr>
<td>6:00-7:00 p.m.</td>
<td>Networking Reception in Sponsor Hall</td>
</tr>
<tr>
<td>7:30 p.m.</td>
<td>EPCOT Gala Dinner Event and Illusions After Hours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tuesday, May 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7:00 a.m.-7:15 p.m.</td>
<td>Registration</td>
</tr>
<tr>
<td>7:00-7:45 a.m.</td>
<td>Breakfast</td>
</tr>
<tr>
<td>7:45-8:00 a.m.</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>8:00-8:45 a.m.</td>
<td>General Session</td>
</tr>
<tr>
<td>8:45-9:15 a.m.</td>
<td>General Session</td>
</tr>
<tr>
<td>9:15-9:45 a.m.</td>
<td>General Session</td>
</tr>
<tr>
<td>9:45-10:15 a.m.</td>
<td>Networking Break in Sponsor Hall</td>
</tr>
<tr>
<td>10:15-11:15 a.m.</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>11:30 a.m.-12:30 p.m.</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>12:30-1:45 p.m.</td>
<td>Innovative Tech Lunch</td>
</tr>
<tr>
<td>1:45-2:45 p.m.</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>3:00-4:00 p.m.</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>4:15-5:15 p.m.</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>5:30-6:30 p.m.</td>
<td>Solutions Showcase***</td>
</tr>
<tr>
<td>6:30-7:30 p.m.</td>
<td>Networking Reception in Sponsor Hall</td>
</tr>
<tr>
<td>7:30 p.m.</td>
<td>Sponsor Dine-Around</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wednesday, May 3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7:00 a.m.-6:00 p.m.</td>
<td>Registration</td>
</tr>
<tr>
<td>7:00-8:00 a.m.</td>
<td>Breakfast/Community Institution Session</td>
</tr>
<tr>
<td>8:00-8:15 a.m.</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>8:15-8:45 a.m.</td>
<td>General Session</td>
</tr>
<tr>
<td>8:45-9:15 p.m.</td>
<td>General Session</td>
</tr>
<tr>
<td>9:30-10:30 a.m.</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>10:45-11:45 a.m.</td>
<td>Solutions Showcase***</td>
</tr>
<tr>
<td>12:00-1:30 p.m.</td>
<td>Lunch in Sponsor Hall - Summit Wrap-Up with Door Prizes</td>
</tr>
<tr>
<td>1:30-5:00 p.m.</td>
<td>Members Technical Forum*</td>
</tr>
</tbody>
</table>

* closed to ALL Sponsors
** closed to all sponsors except affiliate board advisors
*** closed to all sponsors except silver sponsors speaking during this session

Agenda is subject to change. For an up-to-date agenda, visit fsisac-summit.com/2017-Annual-Agenda