Date: ***11/12/2018*** ***Time:*** ***8:45 A.M. - 9:30 A.M.*** ***Track:*** ***Governance, Risk, and Compliance***

Connecting Large and Small Companies To Enhance Cyber Readiness

In this session learn about how the 2016 Commission on Enhancing National Cybersecurity's Cyber Readiness Institute (CRI) was created to develop best practices, tools and resources for improving the cyber-readiness of small and medium-sized businesses as well as facilitating workforce development needed to implement these cyber-risk management tools.

Speaker Info

First Name	Last Name	Company
Kiersten	Todt	Cyber Readiness Institute

Date: ***11/12/2018*** ***Time:*** ***8:45 A.M. - 9:30 A.M.*** ***Track:*** ***Security and Technology***

MISP as a General Purpose Correlation Engine

The open source software platform known as Malware Information Sharing Platform (MISP) helps teams aggregate security indicators of type "known bad". The typical usage of indicators of interest submitted to MISP is to help visualize the interrelationships between disparate discreet "events of interest". In this presentation we will show how MISP can be used as a general purpose correlation engine to correlate (at scale) observed network indicators with "all the known bad" contained with one's MISP instance. In addition we will show how MISP events can be used to correlate User Agent (UA) strings of interest with observed UA strings.

Speaker Info

First Name	Last Name	Company
Alan	Czarnecki	Nationwide Insurance

Date: ***11/12/2018*** ***Time:*** ***8:45 A.M. - 9:30 A.M.*** ***Track:*** ***Threat Intelligence***

The Resurgence of Activism and Its Impacts on the Financial Sector

Over the last few years we have seen significant increases in activism around energy infrastructure projects within the US, Canada, and Europe. This targeted activism has also taken notice of the financial companies funding these projects and leveraged this information to disrupt the projects and the banks funding them. Various techniques have been used and continue to evolve.

Join us as we review these targeted actions against financial firms, current trends within the activist community, and mitigation techniques to address being targeted.

Speaker Info

First Name	Last Name	Company
Donnie	Carpenter	FS-ISAC
Tim	Chase	GRF
Chris	Denning	GRF

Date: ***11/12/2018*** ***Time:*** ***8:45 A.M. - 9:30 A.M.*** ***Track:*** ***Security and Technology***

Case Study on the RJFS Secure Connection Project

The objective of the RJFS Secure Connection project was to provide RJ Information Security with visibility and telemetry into RJ independent advisors endpoints and an equivalent layer of security that we use with RJ advisors. In discussions with peers of RJ's, there is a large challenge having independent advisor groups agree to endpoint surveillance. The challenge lies in convincing independent advisors to allow a surveillance agent (licensed to RJ) to be deployed on an endpoint they own. It is quite a daunting task. The Secure Connection Project was a two year project to place surveillance agents on every independent advisor's endpoint. Our objective is to share the successes and challenges of the project so that other FSI firms with an independent advisory business can replicate this project successfully.

Speaker Info

First Name	**Last Name**	**Company**
Kishen	Sridharan	Raymond James Financial
Maurice	Marsh	Raymond James Financial

Date: ***11/12/2018*** ***Time:*** ***8:45 A.M. - 10:30 A.M.*** ***Track:*** ***Threat Intelligence***

BYOI: Bears Attack Banks

This threat intelligence workshop enables threat hunters, cyber-intelligence analysts and security researchers to collaborate and exchange threat hunting methodologies, behavioral queries and unique IOCs for the purpose of discovering and detecting RU and CN "bear" actors in financial environments. Tradecraft developed and shared can be used for enrichment of analytic queries, for better adversarial operational understanding and for technical APT hunting strategies specific to our sector. This is a live, working group similar to the threat intelligence sharing we love in the email exchange community.

Speaker Info

First Name	**Last Name**	**Company**
Lori	Stroud	BB&T

Date: ***11/12/2018*** ***Time:*** ***8:45 A.M. - 10:30 A.M.*** ***Track:*** ***Human Element***

Security Awareness - Make Your Voice Heard

This session will address the most relevant topics in a successful information security awareness program as determined by the Security Awareness Working Group (SAWG). Attendees will break into groups to discuss the topics and after brainstorming, present their best practices to the attendees. Findings will be documented and provided to session attendees and members of the SAWG after the Summit.

Speaker Info

First Name	**Last Name**	**Company**
Brent	Frampton	Vanguard

Date: ***11/12/2018*** **Time:** ***9:00 A.M. - 10:30 A.M.*** **Track:**

Introduction to FS-ISAC

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.

Speaker Info

First Name	Last Name	Company
Jane	McKenna	FS-ISAC
Michael	Petrik	FS-ISAC

Date: ***11/12/2018*** **Time:** ***9:45 A.M. - 10:30 A.M.*** **Track:** ***Cloud***

Microservice Security: An Analogous Look at Cloud Architecture

Security architecture has been drastically changed by the utilization of public clouds. As banks move into the cloud they move from a perimeterized security model to a deperimeterized one. The difficulty, cost and strategies must all be re-evaluated. This session takes a comparative look at traditional datacenter architecture and cloud-based microservice architecture as well as a look at some standard tools for the cloud.

Speaker Info

First Name	Last Name	Company
Cheney	Hester	Fifth Third Bank

Date: ***11/12/2018*** **Time:** ***9:45 A.M. - 10:30 A.M.*** **Track:** ***Threat Intelligence***

A Beginner's Guide to Creating a Threat Intel Program

Everyone talks about threat intel but no one really talks about how they built up their program. In this discussion, we'll take a stroll down memory lane with the masterminds behind CTI (Mike and Russell) and go step by step on how Kaiser Permanente created their threat intel program and how it's saved our bacon on more than one occasion!

Speaker Info

First Name	Last Name	Company
Mike	Slavick	Kaiser Permanente
Russell	Culpepper	Kaiser Permanente

Date: ***11/12/2018*** ***Time:*** ***9:45 A.M.*** - ***10:30 A.M.*** ***Track:*** ***Resiliency and Recovery***

Complicated, Complex, Robust and Resilient – Decoding These Needed but Often Misunderstood Concepts to Increase Your Information Security Posture

Are you often bombarded with the buzz terms complicated, complex, robust and resilient? Too often these terms are usec interchangeably to the detriment of those speaking. This presentation will first decode this lexicon; and then provide you a framework to develop and integrate strategies for achieving the two very different yet highly desired qualities of both robustness and resilience into your information security programs. Learn practical actions you can immediately take back to your organization and understand a framework to evaluate your strategies to ensure you have full alignment to tackle both your robustness and resilience goals.

Speaker Info

First Name	**Last Name**	**Company**
Ian	Schneller	Bank of America

Date: ***11/12/2018*** ***Time:*** ***11:15 AM*** - ***12:00 PM*** ***Track:***

Tipping the Scales: Using Asymmetrical Thinking to Change the Rules in Your Favor

Is it possible to acquire the ability to mastermind the kind of agile business practices and innovative thinking that separate the great companies from the mere good ones? Is it possible to devise new ways to out-think your competition? Yes, or at least Jeffrey Baxter, national security expert and founding member of Steely Dan, thinks so. There are plenty of self-proclaimed "out-of-the-box" thinkers in this world, but Baxter has a proven track record in this arena. His experience and expertise span the gamut, from the music and media to US security and government agencies.

What makes it different is that Baxter doesn't just avoid the box – for him, there is no box. Stripping down the 19th-century business model to show how outdated flaw – such as the rigid, hierarchal and policy-driven roles for workers and management have limited companies abilities to "grow" – Baxter illustrates how new technologies, practices and ways of thinking are (and can) reaping huge benefits for organizations and individuals. These new models foster and stimulate a more agile and creative action and reaction to today's modern, rapidly changing and competitive world that corporate management and governments of the past would have a hard time understanding and recognizing, much less anticipating.

Speaker Info

First Name	**Last Name**	**Company**
Jeffrey	Baxter	

Date: ***11/12/2018*** ***Time:*** ***12:00 P.M.*** - ***12:30 P.M.*** ***Track:*** ***Cloud***

From Prevention to Protection: Data as the New Security Perimeter

The traditional security model was invented for a world where IT services controlled data behind the enterprise perimeter. With the rise of cloud and mobile, organizations must shift from a prevention to a protection model. In this session explore tactical approaches that can be used to secure collaboration services such as Box and Office 365 at a global scale. Gain an understanding of how this new IT security strategy has driven both business agility, cost savings and an alignment with business needs.

Speaker Info

First Name	**Last Name**	**Company**
Rajiv	**Gupta**	McAfee

Date: ***11/12/2018*** ***Time:*** ***12:30 P.M.*** - ***1:30 P.M.*** ***Track:***

Lunch with the Sponsors

Speaker Info

First Name	**Last Name**	**Company**

Date: ***11/12/2018*** ***Time:*** ***1:30 P.M.*** - ***2:15 P.M.*** ***Track:*** ***Resiliency and Recovery***

Preparing for a Systemic Attack on Power, Communication and Financial Services

Leaders from finance, communication and electricity sectors will discuss the Tri-Sector Crisis Response Playbook and discuss an ongoing partnership development to reduce the impact of critical infrastructure attack. An event of high severity activates the Tri-Sector Playbook for early coordination among the three critical infrastructure sectors, to share situational awareness and courses of action development and selection. The crisis rhythms of the three sectors will also be discussed.

Speaker Info

First Name	**Last Name**	**Company**
Kathryn	Condello	CenturyLink
Brian	**Tishuk**	FS-ISAC
Scott	Aaronson	Edison Electric Institute

Date: ***11/12/2018*** ***Time:*** ***1:30 PM*** - ***2:15 PM*** ***Track:*** ***Governance, Risk, and Compliance***

Key Policy Issues From Info Sharing to Cyberwar

Learn about key emerging policy issues in cyberwar, internet governance and information sharing. This session will treat you to a deep-dive on polices specific to cyberwar, internet governance and information sharing. Learn how critical infrastructure companies cannot protect themselves from adversarial nation-states without federal assistance and advocates that the US government should create a classified network to share information on cyberthreats with private companies critical to the economy.

Speaker Info

First Name	**Last Name**	**Company**
Robert	Knake	Council on Foreign Relations

Date: ***11/12/2018*** ***Time:*** ***1:30 P.M.*** - ***2:15 P.M.*** ***Track:*** ***Governance, Risk, and Compliance***

Don't Break the Bank: Achieving Compliance

Compliance regulations such as SWIFT and GDPR can be challenging to understand and implement. Many of these regulations have cybersecurity requirements that are focused on protecting critical banking infrastructure with aggressive timelines - and without disrupting the very business-critical systems you're trying to protect. Jumping from one set of requirements to another, and to subsequent internal and external audits, can feel like a never-ending cycle.

In this session, Faraz Aladin, director of product management at Illumino shares his thoughts about different approaches to handling the unique challenges a security practitioner in financial services can expect. This session reviews:

- Top challenges facing global banking
- Approaches to protecting the digital "crown jewels"
- How to future-proof for evolving requirements

Speaker Info

First Name	**Last Name**	**Company**
Faraz	Aladin	Illumio

Date: ***11/12/2018*** ***Time:*** ***1:30 P.M.*** - ***2:15 P.M.*** ***Track:*** ***Security and Technology***

Reframing the 4 W's of PAM using Federated Insights

Security professionals have tools, but less joined up visibility mixed with the highest levels of scrutiny over our programs. The reality is, we can no longer sustain success with traditional firefighting monitoring approaches. Organizations must proactively focus efforts across the enterprise on areas of greatest return and impact to drive risk reduction. This session will reframe PAM and explore what data-driven and federated insights you can glean from data about where the problem lies and how to fix it.

Speaker Info

First Name	**Last Name**	**Company**
James	Doggett	Panaseer

Date: ***11/12/2018*** ***Time:*** ***1:30 P.M.*** - ***2:15 P.M.*** ***Track:*** ***Security and Technology***

Enabling Agile Development Velocity Through DevSecOps and Zero Trust

Many companies are exploring the opportunity to increase development velocity and agility while maintaining a sufficient level of security. In this presentation, learn how a Fortune-500 sized company was able to completely replace the customer-facing application through a combination of scale-out, service-based architecture, DevSecOps transformation, zero-trust adoption, open source focus and an "everything as code" methodology allowing the application to scale from 50K users to 15+ million users in three years.

Speaker Info

First Name	**Last Name**	**Company**
Benjamin	Agner	Aflac

Date: ***11/12/2018*** **Time:** ***1:30 P.M. - 3:15 P.M.*** **Track:** ***Governance, Risk, and Compliance***

Cyber Defense Matrix Workshop

This is a workshop to continue developing and aligning security capabilities, products and functions to the Cyber Defense Matrix. During this workshop, participants will learn more about the Cyber Defense Matrix, but more importantly, contribute to a body of work that practitioners can use to quickly determine gaps that they may have in their security program and discover solutions that fill those gaps.

Speaker Info

First Name	Last Name	Company
Sounil	Yu	Bank of America

Date: ***11/12/2018*** **Time:** ***2:30 P.M. - 3:15 P.M.*** **Track:** ***Cloud***

Assessment and Compliance for the Financial Services Cloud

Over the past five years, cloud computing has revolutionized how organizations do computing. Computing has gone from being a capital-intensive effort to buy and build computer systems and networks, to being a "virtual" activity using remotely accessible resources. The session focuses on hardening cloud implementations to withstand attacks from advanced, professional and nation-state attackers. In this presentation, discuss the limitations of the current assessment and compliance frameworks with regard to cloud, best practices to look for when assessing cloud cybersecurity and the elements to included within standards for cloud cybersecurity assessment and compliance.

Speaker Info

First Name	Last Name	Company
Christopher	Williams	Leidos Cyber
Siobhan	Moran	Leidos Cyber

Date: ***11/12/2018*** **Time:** ***2:30 P.M. - 3:15 P.M.*** **Track:** ***Human Element***

Five Ways to Keep Your Security Talent Happy

In this session learn how to recruit security talent that matches the mission and culture of your security organization; ways you can get new hires productive and engaged in their first few weeks and months; how you can foster an environment that encourages learning and collaboration; what things can silently frustrate your team to the point of leaving; how to measure your team's performance (and when not to); and how to provide growth opportunities for your team - both inside and outside your organization.

Speaker Info

First Name	Last Name	Company
Bruce	Potter	Expel
Mase	Issa	Expel

Date: ***11/12/2018*** ***Time:*** ***2:30 PM - 3:15 PM*** ***Track:*** ***Security and Technology***

Playing the Hand You're Dealt: Investigating SARs Without Showing Your Cards - How AML Investigations to Decrease Risk Add Cyber Risk

Unauthorized disclosure of a SAR filing is a federal criminal offense. Online research and investigation is an inherent part of creating a SAR and an ever present risk of attribution. Analysts and investigators need a browser that reduces exposure risks and conceals their identity. This session discusses and demonstrates how AML analysts and investigators use a cloud browser to access the web from any machine, any network without compromising their computer, network or organization. See how AML teams operate more efficiently when using a compliance-friendly browser built in the cloud, provided as a service offsite and centrally managed by IT. This session will include demonstrations of non-attribution capabilities.

Speaker Info

First Name	Last Name	Company
Kevin	Yu	Authentic8

Date: ***11/12/2018*** ***Time:*** ***2:30 P.M. - 3:15 P.M*** ***Track:*** ***Governance, Risk, and Compliance***

Mitigating Unknown Third- and Fourth-Party Risk

This session reviews a vendor risk management program and looks at how it implementation has addressed risk to critical infrastructure third- and fourth-party partners. Hear new ideas about how to reduce vendor security risk, including best practices, program optimization and financial sector partnership.

Speaker Info

First Name	Last Name	Company
Amera	McCoy	CME Group
Bethany	Netzel	CME Group

Date: ***11/12/2018*** ***Time:*** ***3:30 P.M. - 4:15 P.M.*** ***Track:*** ***Human Element***

Collaboration Between Cyber Threat Intelligence and Proactive Human Threat Prevention

Typically, insider threat programs focus on detecting current insider threat activity or responding to incidents after they have occurred. The key to disrupting and preventing damage from malicious insiders is getting in front of unrealized insider threat behavior. This presentation will examine the development and execution of a joint effort between an organization's cyberthreat intelligence and human threat prevention teams to focus on identifying potential risks before the malicious actor has an opportunity to strike. Explore the development of the program, key initiatives crucial for success, an overview of challenges and obstacles and a summary of lessons and best practices in building the effort.

Speaker Info

First Name	Last Name	Company
Michael	Kosak	Bank of America
Ed	Traywick	Bank of America

Date: ***11/12/2018*** ***Time:*** ***3:30 P.M. - 4:15 P.M.*** ***Track:*** ***Security and Technology***

Securing Open Banking with FIDO Authentication Standards

This session provides in-depth insights into understanding how FIs can use FIDO strong authentication to stop attacks against user credentials, while also meeting the security and convenience requirements of open banking.

Speaker Info

First Name	**Last Name**	**Company**
Brett	McDowell	FIDO

Date: ***11/12/2018*** ***Time:*** ***3:30 P.M. - 4:15 P.M.*** ***Track:*** ***Fraud***

Automated ATO: The Rise of Single Request Attacks

Account takeover is growing. Attackers swoop in after credential spills and use software to automatically match breached email addresses with the top 10 most common passwords. While this approach, known as a single request attack. may appear unsophisticated, attackers commonly use headless browsers, execute JavaScript like a legitimate human user, and present dynamic client and network fingerprints. This session reviews real-world case studies where ATOs have been scaled via single request attacks. These case studies unpack the compounding effect caused when businesses use depreciated mitigation strategies and profiles the growing incentive attackers have across other use-cases and verticals. The session scrutinizes past approaches to curbing ATO and explains why single request attacks have increased and examines tested pathways toward mitigating and preventing single request attacks.

Speaker Info

First Name	**Last Name**	**Company**
Kevin	Gosschalk	Arkose Labs

Date: ***11/12/2018*** ***Time:*** ***3:30 P.M. - 4:15 P.M.*** ***Track:*** ***Governance, Risk, and Compliance***

Security Frameworks versus Assessment Tools

There is a plethora of confusion and misstatements about security frameworks and assessments. Many times, security professionals will refer to the FFIEC's Cybersecurity Assessment Tool as a framework, which it is not. Many financial institutions are not aware of the value of the NIST Cybersecurity Framework, which is not an assessment tool. This session will offer a brief explanation of the difference between a security framework and a security assessment tool, the panelists will outline which framework or tool their community institution uses, the decision behind their selection and the pros and cons of that decision.

Speaker Info

First Name	**Last Name**	**Company**
Barb	Groskinsky	American Community Bank & Trust
Heather	McCalman	FS-ISAC
Ken	Shaurette	FIPCO

Date: ***11/12/2018*** ***Time:*** ***3:30 P.M.*** - ***4:15 P.M.*** ***Track:*** ***Threat Intelligence***

Predicting the Punchline: Joker's Stash Timeline Analysis

Worldpay's Cyber Fraud Intel and Disruption program arms the fraud and risk departments with actionable intelligence by monitoring the ecosystems of the largest black market carding shops. A historical fusion analysis on the criminal carding market "Joker's Stash" was done to uncover key indicators about the actor's release activity. These indicators predicted a new mass breach to be released by Joker on May 10, 2018 at 11:00 pm ET. The ability to align the fraud and intelligence teams in advance allowed for a swift response to yielding successful identification of the common point of purchase in record time.

Speaker Info

First Name	Last Name	Company
Matthew	Heath	Worldpay

Date: ***11/12/2018*** ***Time:*** ***3:30 P.M.*** - ***5:30 P.M.*** ***Track:*** ***Governance, Risk, and Compliance***

How am I doing? The Benchmarking Workshop

This workshop explores the need for benchmarking to assist with regulation and board presentations. Learn about drafting benchmarking metrics in relation to the Cyber Defense Matrix as well as what else is needed for success.

Speaker Info

First Name	Last Name	Company
Sounil	Yu	Bank of America
Ryan	Bowling	Bank of America

Date: ***11/12/2018*** ***Time:*** ***4:30 P.M.*** - ***5:30 P.M.*** ***Track:*** ***Security and Technology***

Establish Digital Trust with a Frictionless User Experience

How can you establish trust over digital channels to seamlessly welcome in both new and existing users? The answer lies in how the risk of digital identities are assessed. To help identify actual users in a digital channel, organizations will need strong digital identity risk assessment capabilities that examine each user’s digital patterns and that can detect potential malicious actors more accurately. In this session, learn how solutions can help you authentically and quickly establish a trusted and frictionless digital relationship between you and your users.

Speaker Info

First Name	Last Name	Company
Shaked	Vax	IBM Security

Date: ***11/12/2018*** ***Time:*** ***4:30 P.M.*** - ***5:30 P.M.*** ***Track:*** ***Threat Intelligence***

Doing More with Less: Using Automation to Operationalize Cyber Threat Intel

Cyberthreat intelligence programs have become increasingly popular in enterprise organizations, yet most companies are not even close to maximizing its potential. Cyber-intelligence teams must process millions of incidents, datapoints, alerts and indicators of compromise to identify cyberthreats targeting their organization; but this process can become incredibly overwhelming and burdensome to manage. To maximize the value of threat intelligence, companies must leverage tailored collection techniques and automation of common threat mitigation steps. This interactive session demonstrates how to operationalize threat-intelligence programs.

Speaker Info

First Name	**Last Name**	**Company**
Guy	Nizan	IntSights

Date: ***11/12/2018*** ***Time:*** ***4:30 P.M.*** - ***5:30 P.M.*** ***Track:*** ***Security and Technology***

Flipping the Odds by Innovating Your Approach to Third Party Risk

Being aware of vulnerabilities from third party vendors is only the start of an effective third party risk management program. Businesses need to consider a comprehensive approach that implements both detection and threat response across all of their connected partners – all of their cyber attack surface. A well-orchestrated threat response poses far-reaching benefits, as well as technical challenges on a business' security infrastructure, including how to use threat intelligence and deception technologies across their organization. This presentation explores the challenges faced when adversaries attack businesses in a coordinated campaign and proposes how those businesses can implement effective, coordinated threat responses.

Speaker Info

First Name	**Last Name**	**Company**
Allan	Thomson	LookingGlass Cyber Solutions

Date: ***11/12/2018*** ***Time:*** ***4:30 P.M.*** - ***5:30 P.M.*** ***Track:*** ***Threat Intelligence***

PreReconnaissance: Getting Earlier into the Kill Chain

In this session learn how to use large-scale internet datasets to identify threats before they hit your environment. Explore methodologies and use cases for threat hunting and research.

Speaker Info

First Name	**Last Name**	**Company**
Aaron	Mog	RiskIQ

Date: ***11/12/2018*** ***Time:*** ***4:30 P.M.*** - ***5:30 P.M.*** ***Track:*** ***Threat Intelligence***

Demonstration of the first Cybersecurity Situation room : ThreatQ Investigations

The industry is fighting to drive down MTTD (mean time to detection) and MTTR (mean time to response). Many do this by automating playbooks and integrating threat feed data with their layers of defense. But this can backfire as not all threat data or actions taken are equal. In this session learn how the ThreatQ™ Investigations platform is designed for collaborative threat analysis, shared understanding and coordinated response.

Speaker Info

First Name	Last Name	Company
Christian	Galladora	ThreatQuotient

Date: ***11/13/2018*** ***Time:*** ***8:15 A.M.*** - ***8:45 A.M.*** ***Track:*** ***Fraud***

Turning the Corner on Fraud: The Convergence of Fraud and Cyber Intelligence

As organizations contemplate, develop and mature cyberfusion centers leadership is also seeing the synergies with fraud operations. Fusing fraud operations and cyberdefense capabilities in large financial institutions is a necessary step being taken to improve detection and response times to account take-overs, business email compromise and other fraudulent activities. This presentation will show how fusing traditional cyberthreat intelligence and advanced analytics with fraud operations delivers real results in mitigating cybercrime and online fraud.

Speaker Info

First Name	Last Name	Company
Amy	Boawn	Booz Allen Hamilton
Anil	Markose	Booz Allen Hamilton

Date: ***11/13/2018*** ***Time:*** ***8:45 A.M.*** - ***9:15 A.M.*** ***Track:*** ***Threat Intelligence***

Moving Beyond Low-Level Indicators: Why Detecting Techniques is Where It's At

It's getting tougher to pin down the bad guys using low-level indicators like file hashes, domains and IPs thanks to adaptations in malware such as fileless malware, self-compiling malware, malware that uses legitimate services for command and control, compromised websites for communications and malware that that lives off the land (using PowerShell and other local tools). This session will take a look at how to leverage the ATTACK Framework from MITRE to focus in on using techniques for high fidelity detections.

Speaker Info

First Name	Last Name	Company
Travis	Farral	Anomali

Date: ***11/13/2018*** ***Time:*** ***9:45 A.M.*** **-** ***10:30 A.M.*** ***Track:*** ***Cloud***

The Multi-cloud Strategy: What You Get When You Don't Buy in Bulk

A multi-cloud strategy is important to the risk of unauthorized access or metadata monitoring. The 'secret sauce' is now coming from how microservices and applications are structured. As a result, there would be no real way to prevent a host from seeing that sort of configuration in their space. Basically, a company as large as the ones who are cloud providers today could probably break the law, pay the fine and leave a bank decimated. This conversation is interesting and this session will help draw the issue out of the shadows it currently seems to reside in.

Speaker Info

First Name	Last Name	Company
Cheney	Hester	Fifth Third Bank

Date: ***11/13/2018*** ***Time:*** ***9:45 A.M.*** **-** ***10:30 A.M.*** ***Track:*** ***Threat Intelligence***

Rebooting Threat Intelligence Through File Analysis Transparency

Threat intelligence is not about having information. It's about being able to answer critical questions with the information you have. In this presentation, learn a new approach the threat intelligence that focuses on the smart harvesting of existing data to surface and share critical threat indicators more effectively.

Speaker Info

First Name	Last Name	Company
William	Opet	JP Morgan Chase
Mario	Vuksan	ReversingLabs

Date: ***11/13/2018*** ***Time:*** ***9:45 A.M.*** **-** ***10:30 A.M.*** ***Track:*** ***Security and Technology***

The Devil Inside: Proactive Strategies for Late Stage Attack Investigations

After compromising an endpoint, does the attacker vanish? Many financial organizations lack visibility into traffic within the East-West corridor, which is where attackers will do their greatest damage. During this session, learn about a network traffic analysis capability, how it helped them move from reactive to proactive and make faster, data-driven implementation and change decisions. The session will review the East-West attack surface, late stage attack behaviors, attacks that have used these behaviors and the indicators that can be found within network traffic to reveal these activities.

Speaker Info

First Name	Last Name	Company
Mitch	Roberson	Curo Financial
Barbara	Kay	ExtraHop Networks Inc.

Date: ***11/13/2018*** **Time:** ***9:45 A.M. - 10:30 A.M.*** **Track:** ***Fraud***

Take Control of Your Security Posture

No matter how much you invest or how mature your security posture is, you experience collateral damage from every major breach. According to Verizon Data Breach Report, over 80% of breaches are the result of weak or stolen passwords. What's truly alarming is how many of those stolen passwords are reused across various websites - contributing to a 2% success rate in credential reuse, unauthorized access and escalating fraud rates.

Mass breaches and credential reuse happen because of centralized passwords. Faced with billions of credential stuffing attacks each month, enterprises are fighting back.

Learn how financial services leaders have moved towards true password-less security by leveraging decentralized authentication and FIDO standards. Understand what steps are being taken to eliminate fraud and credential reuse, and enhance user experience across mobile and web applications.

Speaker Info

First Name	Last Name	Company
George	Avetisov	HYPR Corp
Bojan	Simic	HYPR Corp

Date: ***11/13/2018*** **Time:** ***9:45 A.M. - 10:30 A.M.*** **Track:** ***Testing and Security Assurance***

Fannie Mae's DevSecOps Journey

Fannie Mae partners with lenders to create housing opportunities for families across the country, and helps make the 30-year fixed-rate mortgage and affordable rental housing possible for millions of Americans. To support this mission, Fannie Mae must support robust security practices, and aims toward conducting cybersecurity assessments earlier in the development lifecycle, and engaging business partners in the review and mitigation of cybersecurity risks. Through DevSecOps, Fannie Mae has reached that goal and stakeholders from development, operations, and cybersecurity now monitor, analyze, test, proactively determine and fix vulnerabilities earlier in the development lifecycle. This session explains how DevSecOps has helped increase code quality standards and reduce the vulnerabilities at Fannie Mae.

Speaker Info

First Name	Last Name	Company
Chitra	Elango	Fannie Mae
Stephanie	Derdouri	Fannie Mae

Date: ***11/13/2018*** **Time:** ***9:45 A.M. - 10:30 A.M.*** **Track:** ***Governance, Risk, and Compliance***

Conducting a Threat-based Annual Risk Assessment using FAIR

A multitude of statutory and regulatory requirements and guidance, including HIPAA, NYDFS and PCI, require an annual assessment of information risk as part of their security requirements. The assessments all include identifying assets, threats and vulnerabilities in an effort to determine risk. This presentation will explain how to execute a quantitative annual risk assessment using the FAIR model and a threat-oriented analysis approach.

Speaker Info

First Name	Last Name	Company
Angela	Dunkle	Globe Life and Accident Insurance Company
Michael	Priest	Globe Life and Accident Insurance Company
Miguel	Villarreal	Globe Life and Accident Insurance Company

Date: ***11/13/2018*** ***Time:*** ***10:45 A.M.*** - ***11:30 A.M.*** ***Track:*** ***Cloud***

One Community Bank's Approach to Leveraging Cloud Technologies

This session is an overview of how a community bank is leveraging cloud technologies. Hear an overview of goals to achieve process for evaluation through deployment; involvement of IT Steering Committee; VMO analysis and involvement; involvement of internal audit and/or regulators; project planning; leveraging 3rd party consultants; benefits to achieve improvements to BCP/DR, monthly cost as opposed to large capital outlay, flexibility; security considerations; final deployment-IAAS environment with Office365 (Azure); and unexpected outcomes, both negative and positive.

Speaker Info

First Name	Last Name	Company
Jeff	Jackson	NASB

Date: ***11/13/2018*** ***Time:*** ***10:45 A.M.*** - ***11:30 A.M.*** ***Track:*** ***Security and Technology***

Endpoint Protection – Much More than Just Detection

Spending on cybersecurity by enterprises will top $96 billion USD in 2018 [Gartner], with a significant portion dedicated to fighting malware. But are these hard-won cybersecurity budgets well spent? This presentation will address what is sometimes called the “protection deception”. In particular, that means examining the “arms race” between black hats and the technologies designed to thwart them. Approaches for actual protection, including automatic containment and cloud-based verdicting, as well as how to keep users productive, even as unknown files undergo verdicting, will be reviewed.

Speaker Info

First Name	Last Name	Company
Carlos	Solari	Comodo Cybersecurity

Date: ***11/13/2018*** ***Time:*** ***10:45 A.M.*** - ***11:30 A.M.*** ***Track:*** ***Security and Technology***

Simple, Agile, Secure Key Management: Fact or Fiction?

Data encryption, advanced authentication, digital signing and other cryptography-based security functions have come to play a vital role in financial organizations’ cybersecurity and regulatory compliance initiatives. To secure their digital assets effectively, organizations must protect their cryptographic keys, much like guarding the key to a safe in today’s increasingl complex, open and interconnected IT environment. In this session learn about the impact of digital transformation on key management and how financial institutions are leveraging software-defined cryptography to securely adopt the public cloud, protecting their cryptographic keys, supporting a need for agility, automation and elasticity for a variety of use cases including data protection, PKI, authentication, digital signing and secure custody of cryptocurrencies and digital assets.

Speaker Info

First Name	Last Name	Company
Bob	Blakely	Citigroup
Oz	Mishli	Unbound Tech

Date: ***11/13/2018*** ***Time:*** ***10:45 A.M. - 11:30 A.M.*** ***Track:*** ***Security and Technology***

Ethereum Smart Contract Security Essentials

On the blockchain, there are no secrets. Every transaction is logged and everyone has a copy of all of the code. Over the past year enterprising hackers have used flaws in smart contracts to whisk away millions. Made possible thanks to Ethereum, the technology that powers CryptoKitties and Solidity, a high-level language used to write Ethereum's Turing complete smart contracts. This session will introduce smart contract security, present common vulnerability classes and walk through the methods used by hackers to exploit them for financial gain. Also learn about tools and techniques to securely develop smart contracts that are resistant to these attacks.

Speaker Info

First Name	Last Name	Company
Daniel	Guido	Trail of Bits

Date: ***11/13/2018*** ***Time:*** ***10:45 A.M. - 11:30 A.M.*** ***Track:*** ***Governance, Risk, and Compliance***

Financial Services Sector Cybersecurity Profile

With the increasing volume and sophistication of cyber attacks and a projected global shortfall of two million cybersecurity professionals by 2021, the sector and supervisory community must find an approach to cybersecurity that effectively counters the dynamic, evolving threat. This session provides an overview of the Financial Services Sector Cybersecurity Profile, based on the NIST Cybersecurity Framework and explores how to use the approach at your firm. The Profile is a harmonized approach to cybersecurity that recognizes the multiple, often overlapping, regulations and supervisory agencies while fostering an efficient, result-oriented approach to cybersecurity for institutions of all sizes and complexity.

Speaker Info

First Name	Last Name	Company
Denyette	DePierro	American Bankers Association
Josh	Magri	Financial Services Roundtable/BITS

Date: ***11/13/2018*** ***Time:*** ***10:45 A.M. - 11:30 A.M.*** ***Track:*** ***Resiliency and Recovery***

Moving Beyond Discussion-based Tabletop Exercises

Most firms realize the value of conducting exercises as a preparedness activity to improve resiliency and examine cyber-incident response. This expert panel covers key topic areas including fundamentals of drills, cyber-ranges and functional exercises; lessons learned from planning and conducting operations-based exercises; keys to effective program-level planning such as choosing the right exercises for the right reasons; and how to effectively engage across the enterprise and with response teams.

Speaker Info

First Name	Last Name	Company
Jeff	Wright	Bank of America
Adam	Bulava	JP Morgan Chase
Matt	Goard	Morgan Stanley

Date: ***11/13/2018*** ***Time:*** ***11:45 A.M. - 12:15 P.M.*** ***Track:*** ***Threat Intelligence***

How FIs Can Implement Anti-Impersonation Protections for Email

Email is the primary vector of attack for hackers who exploit email's weaknesses and use it to gain fraudulent entry into organizations' networks by impersonating trusted senders. Companies have invested significantly in malware and content filtering technologies to protect against these attacks. Most email attacks target weaknesses in companies' trust infrastructures by impersonating trusted senders through email messages that lack malware or other scannable content. In this session, learn about how hackers attack with impersonation, hear case studies, and explore a vision for financial services to build a trusted framework around email without touching PII.
Learn how anti-impersonation technology complements secure e-mail gateways, anti-phishing training, and encrypted e-mail; we'll also address how these technologies can work together with a reputation framework to create a complete, automated system for e-mail trust and security.

Speaker Info

First Name	**Last Name**	**Company**
Alexander	Garcia-Tobar	Valimail
Karl	Mattson	City National Bank

Date: ***11/13/2018*** ***Time:*** ***7:00 A.M. - 8:00 A.M.*** ***Track:***

Breakfast

Speaker Info

First Name	**Last Name**	**Company**

Date: ***11/13/2018*** ***Time:*** ***12:30 P.M. - 1:45 P.M.*** ***Track:***

Direct from the Incubator Lunch

Speaker Info

First Name	**Last Name**	**Company**

Date: ***11/13/2018*** ***Time:*** ***12:15 P.M.*** ***-*** ***Track:*** ***Security and Technology***

Case Study: Using Decision Automation to Improve Alert Triage by 10x

We often hear that machines are good at speed, but humans are better at decisions. New breakthroughs in decision automation technology have turned this paradigm upside down. Learn how a top bank fully automated its alert triage processes and realized a five-time improvement in accuracy over what analysts used to do manually. Discuss the underlying technology and processes that made this improvement possible, the key lessons learned and how to strategically plan for intelligent automation.

Speaker Info

First Name	Last Name	Company
Kumar	Saurabh	LogicHub

Date: ***11/13/2018*** ***Time:*** ***12:15 P.M.*** ***-*** ***Track:*** ***Threat Intelligence***

Detect, Identify and Localize Unauthorized Mobile Devices for Security, Regulatory Compliance

Unauthorized mobile devices represent a massive unmonitored threat vector and compliance blind spot. In addition to texts and voice calls, mobile phones connect to corporate networks, laptops, create hotspots and introduce new threats into the enterprise. It's been challenging for companies to limit and detect unauthorized mobile devices. Most have historically relied solely on an honors system, with occasional physical security checks. But today organizations can rely on alerting systems and analytics platforms to help them more readily find unauthorized devices connected to their networks. This session reviews new doors of security technology that allow companies to detect, identify and localize mobile phones on a floor-plan map just using the cell signal.

Speaker Info

First Name	Last Name	Company
Chris	Riley	Bastille

Date: ***11/13/2018*** ***Time:*** ***12:15 P.M. -*** ***Track:*** ***Threat Intelligence***

Escaping the 'Echo Chamber' through Cross-Sector Cyber-Intelligence Exchange

Security Operations Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs) have rapidly matured over the past 2 years. Security teams once wished for more intelligence data, and now we have so much of it we don't have enough tools or teams to sort through it all and make it actionable.

Threat intelligence is now fundamentally a question of knowledge management and collaboration. Understanding how an intelligence platform correlates and manages big data is essential to determining how you can evaluate, respond to, and share incidents in real-time. Intelligence exchange can help organizations prevent security breaches while getting smarter about broader the attack surface in the process.

The concept of sharing threat intelligence expands beyond the context of individual security teams. Fraud, cyber threat intelligence, and physical security data can be correlated across internal teams to identify patterns and recognize threats faster. Siloing important threat data within the four walls of a company only creates an echo chamber, limiting the fidelity of threat intelligence sources.

In this presentation, TruSTAR Co-Founder and CEO Paul Kurtz will outline best practices for threat intelligence exchange while showcasing two case studies. Case Study #1: How Fortune 500 Financial Services companies operationalize FS-ISAC threat intelligence by enriching it with open and closed intelligence sources. Case Study #2: How Fortune 500 Cloud Service Providers created a fraud/threat intelligence exchange to mitigate threats faster.

Speaker Info

First Name	**Last Name**	**Company**
Paul	Kurtz	TruSTAR

Date: ***11/13/2018*** ***Time:*** ***12:15 P.M. -*** ***Track:*** ***Governance, Risk, and Compliance***

Learn more about how financial services can provide continuous compliance utilizing IBM Security HC3 Continuous Compliance

As financial services companies migrate workloads to the cloud, there will be a number of regulatory obligations that will need to be met in order for the regulators and internal risk assessors to approve the use of hybrid cloud. In addition, the regulators will require that controls are put into place to ensure that workloads are secure and meet the stringent requirements for data protection and data privacy. In this session, you will learn about the IBM managed service, HC3, that simplifies the path to continuous compliance with a standard security framework monitored by Watson for FSS Reg Tech.

Speaker Info

First Name	**Last Name**	**Company**
Tiffany	Luo	IBM Security
Gary	Meshell	IBM Security

Date: ***11/13/2018*** ***Time:*** ***12:15 P.M. -*** ***Track:*** ***Governance, Risk, and Compliance***

Open Source - Don’t be Afraid, Embrace it, Enable Your Teams for the Future of Software Securely and Compliantly

Modern Software development has many of its roots in the Open Source successes of the past two decades. Open Source doesn't have to be synonymous with insecure or cause anxiety and friction. In this session we will discuss data, workflows and integrations that are available to help risk averse companies embrace open source consumption and contribution with confidence.

The way people build software is evolving fast—from mobile applications to the infrastructure of our largest financial institutions. The early days of Facebook and flip phones have come to an end, meaning security is no longer an acceptable afterthought..

With fast-paced development comes a greater risk of security breaches. It’s not uncommon for major organizations to accidentally leave passwords in public source code, leak sensitive personal customer data, and deploy critical applications into production with clearly exposed vulnerabilities.

As organizations strive to ship new software faster, they are struggling to ensure that software stays secure. The tension between working fast and building securely is clear for financial institutions. New development methodologies bring code to market faster, but inadequate tooling and processes can lead to gaps in security.

Fortunately, there are a few best practices teams can follow to keep code safe from errors, breaches, and other exploitable vulnerabilities. This talk will discussion strategies and best practices you can use today to meet many of your policy, security, and workflow needs.

Speaker Info

First Name	**Last Name**	**Company**
Michael	Filosa	GitHub

Date: ***11/13/2018*** ***Time:*** ***12:15 P.M. -*** ***Track:*** ***Security and Technology***

Streamlining Threat Intelligence

Using threat intelligence in a meaningful way for your organization can be hard. Contributing back to the body of knowledge is even more difficult. This session tells a story that helps tackle both of those issues in a streamlined fashion.

Speaker Info

First Name	**Last Name**	**Company**
Wes	Spencer	Perch Security

Date: ***11/13/2018*** ***Time:*** ***12:15 P.M.*** ***-*** ***Track:*** ***Threat Intelligence***

What We Can Learn from the Spooks: The Convergence of Intelligence and Commercial Defense Tactics

It has become commonplace to claim that "if a major intelligence agency wants to get into your networks, they will succeed." But this isn’t true and certainly cannot be accepted when intelligence agencies share the same skills and resources that high-end cybercrime rings possess. Historically, the way governments defended themselves against these sophisticated attackers involved major operational impacts. But new security technologies mean that even mainstream commercial organizations can protect against sophisticated attackers, without having a major impact on operational efficiencies. This session outlines some of these key technologies and how they are being used.

Speaker Info

First Name	**Last Name**	**Company**
Henry	Harrison	Garrison

Date: ***11/13/2018*** ***Time:*** ***1:45 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Threat Intelligence***

The Uses, Misuses & Abuses of Cyber Intelligence Models

Cyber-intelligence models are misused and abused on a daily basis. This presentation shows pitfalls and provides examples on how to apply the model for maximum effectiveness.

Speaker Info

First Name	**Last Name**	**Company**
Kyle	Davis	Target Corporation

Date: ***11/13/2018*** ***Time:*** ***1:45 P.M.*** ***-*** ***2:30 P.M.*** ***Track:*** ***Governance, Risk, and Compliance***

Security Maturity: How Can FIs Improve?

Cybersecurity and IT leaders, especially those in heavily regulated industries such as the financial sector, are often asked to measure the maturity of their security capabilities (people, processes and technology) against industry peers and frameworks. Frameworks like ISO 27000, CIS, Cobit 5 and NIST, while helpful, require significant time and resources to complete. Join this session to learn how one model combines the best of these frameworks and includes measures of the inherent risk a company faces across five domains. Learn more about the model, experience a live demonstration and explore how the model would be useful.

Speaker Info

First Name	**Last Name**	**Company**
Hadi	Hosn	Secureworks
Ken	Athaide	Secureworks

Date: ***11/13/2018*** ***Time:*** ***1:45 P.M. - 2:30 P.M.*** ***Track:*** ***Security and Technology***

Past, Present, and Future of Security Analytics

As security analytics evolve, so do threat-actor's methods and practices. This session is a kaleidoscope of 10 years ago, current day and 10 years future to examine how defenders require new security analytics to protect their digital business in the face of an active adversary. This session focuses on answering the question of what it mean to deliver superior security analytics. Explore security analytics in its entirety, reviewing new forms of telemetry; analytical techniques; and lastly the mistakes and shortcomings of the past so the do not happen in the future.

Speaker Info

First Name	Last Name	Company
TK	Keanini	Cisco

Date: ***11/13/2018*** ***Time:*** ***1:45 PM - 2:30 PM*** ***Track:*** ***Governance, Risk, and Compliance***

Adopting Cyber-Risk Management in the Digital Era

Cyber Risk Management has traditionally been a vastly qualitative field, with instances of quantitative measurements within very focused efforts. With the increased significance in recent times for prioritized investments and senior management focus on "return on security investments," a large number of organizations are transitioning towards larger adoption of quantitative methods to measure Technology/Cyber Risk Exposure.

In this session you will learn about the need of leveraging this data along with quantification models to make better informed risk management decisions, factors to consider when selecting the right approach for your organization, where to start the process, common roadblocks you may experience, and how to gain stakeholder alignment to your vision and strategy.

This session will also provide a unique opportunity to hear leading industry digital security and risk experts discuss various aspects of adoption of a data and quantitative model driven digital risk management strategy:

External and internal driving factors pushing towards continuous improvement in risk management maturity and what it means for your organization
Journey of evolution of risk management decision making through the stages of trial and error driven to collective wisdom driven to data and quantification model driven
Factors to consider while selecting the right execution approach for your organization and trade-offs to examine. How to adopt a crawl, walk, run approach towards building your next gen risk management strategy
Common pitfalls that we have seen being encountered in the journey with proposed avoidance measures and course of actions

Speaker Info

First Name	Last Name	Company
Husam	Brohi	PwC

Date: ***11/13/2018*** ***Time:*** ***1:45 P.M. - 2:30 P.M.*** ***Track:*** ***Security and Technology***

Automating Security Controls Using Models and Security Orchestratio

Many organizations have adopted machine learning and data analytics to help identify security anomalies. However, mere identification isn't good enough in a world where Petya and other modern attacks can take down 15,000 servers in under two minutes. To combat new types of malware, organizations should be looking at a model driven security orchestration automating and driving security responses at machine speed. In this presentation, learn about a one security orchestration program, including what worked, what didn't work and lessons learned.

Speaker Info

First Name	Last Name	Company
Kurt	Lieber	Aetna

Date: ***11/13/2018*** ***Time:*** ***1:45 P.M. - 2:30 P.M.*** ***Track:*** ***Governance, Risk, and Compliance***

Avoiding Legal Pitfalls in IT Vendor and Service Contracts

The contract with a third-party is the key to the vendor relationship. It specifies deliverables, terms, conditions, requirements, procedures, and limitations. Yet, obscure legal jargon can severely limit any recourse if the vendor fails to deliver. In this session, explore some of the common pitfalls of IT contracts, including confidentiality, indemnification, limitations of liability and others that by default are typically sided in favor of the vendor. Hear about the essential elements of fair contracts, enabling you to improve your negotiation for the right terms and conditions for your third-party service contracts.

Speaker Info

First Name	Last Name	Company
Darrell	Bateman	City Bank

Date: ***11/13/2018*** ***Time:*** ***2:45 P.M. - 3:30 P.M.*** ***Track:*** ***Cloud***

Addressing the Hard Questions About Cloud Security

The transition to the cloud is underway and is poised to be a top area of focus for most financial institutions. As organizations begin to shift mindsets and workloads, they also are grappling with questions about the paradigm shift in security. This session addresses the questions you should be asking cloud providers such as their access controls, information protection, threat detection and response and compliance with standards. This presentation will tackle the tough questions you should be asking and will show why cloud computing can offer stronger controls and better threat management than most traditional tools and environments.

Speaker Info

First Name	Last Name	Company
Lisa	Lee	Microsoft

Date: ***11/13/2018*** ***Time:*** ***2:45 P.M.*** **-** ***3:30 P.M.*** ***Track:*** ***Threat Intelligence***

You Can Steal an Identity, But You Can't Steal Behavior

Behavior-based security analytics and big data analytics can determine if anomalous behavior is risky. Telling you what's happening is not helpful. But telling you when something bad is happening is critical. This session reviews how to use a context build on machine learning and big data to determine whether behavior is risky. Gain a better understanding of how behavior analytics built on big data are changing the game when it comes to predicting, identifying and stopping cyberthreats.

Speaker Info

First Name	**Last Name**	**Company**
Jerry	Archer	Sallie Mae

Date: ***11/13/2018*** ***Time:*** ***2:45 P.M.*** **-** ***3:30 P.M.*** ***Track:*** ***Security and Technology***

Board and Senior Management Level Cyber-Resilience Risk Metrics to Enable Business Decisioning

Despite the number of companies that "measure" cyber-risk, financial institutions boards need more than single point solutions. Metrics for boards need to be tailored to specific organizations so that directors can make informed decisions about the ability to manage operations and invest in the future of their business. These metrics need to incorporate both internal and external data into consumable formats for management and the board with an eye toward future investments against a changing risk landscape. This panel will include a seasoned strategy and risk consulting professional and a member institution to share how they shaped risk metrics for senior management to enable business decisioning and future investment.

Speaker Info

First Name	**Last Name**	**Company**
David	Cooper	Accenture

Date: ***11/13/2018*** ***Time:*** ***2:45 P.M.*** **-** ***3:30 P.M.*** ***Track:*** ***Governance, Risk, and Compliance***

It's Time for a Better Solution to Access Rectification

Most companies are required to undergo some sort of access recertification process, yet few of these programs do much in the way of reducing risk. These processes are typically treated as a "check the box" compliance exercise that is seen as a mandatory annoyance. In this session, learn new ways to recertify access that reduces security risk, reduces time from business partners and address compliance issues.

Speaker Info

First Name	**Last Name**	**Company**
Kurt	Lieber	Aetna

***Date:* 11/13/2018** ***Time:* 2:45 P.M. - 3:30 P.M.** ***Track:* Security and Technology**

Incident Response for Overwhelmed, Understaffed and Unprepared

Incident response consultants typically say the same thing "Have a plan, follow the plan". Everyone knows how to fix a problem when everything is wrapped up in a tight bow, the tools are deployed, the data is accessible and everyone is in agreement on exactly what to do and how. This session is about the incidents that are not always easy to fix. Hear guidance and ideas to get started on what you can do now to prepare and what you can do when your preparation timeline is out of sync with the attackers.

Speaker Info

First Name	Last Name	Company
Tony	Drake	Intercontinental Exchange

***Date:* 11/13/2018** ***Time:* 2:45 P.M. - 3:30 P.M.** ***Track:* Fraud**

Protecting Payment Eco-Systems from Cyber Attacks

Payment networks and their eco-systems are targeted by sophisticated actors including nation-states, resulting in multimillion dollar in losses. Attacks include a variety of sophisticated methods and tools including targeted social engineering, custom designed malware, insider threats and zero-day vulnerabilities. In this session learn how to get executive commitment to diffuse this ticking time bomb; what steps to take - from ideation through analysis; staggered implementation; and the type of controls required. The objective of this session is to arm you with a concrete “how to” guide to strengthen your payment eco-system, in turn strengthening our overall shared payments network.

Speaker Info

First Name	Last Name	Company
Elon	Ginzburg	Wells Fargo
Robert	Thomson	Wells Fargo
Yonesy	Nunez	Wells Fargo

Date:* 11/13/2018** ***Time:* 3:30 P.M. - 4:00 P.M.** ***Track:

Networking Break

Speaker Info

First Name	Last Name	Company

Date: *11/13/2018* **Time:** *4:00 P.M. - 4:45 P.M.* **Track:** *Threat Intelligence*

Inside the Cyber Underworld: Black Market for Financial Data

From credit card data to counterfeit passports, just about anything is available for the right price on the dark web. In this session, walk through the prices for stolen credit cards and bank information; how cybercrime-as-a-service has shaped the threat landscape; the sale of malware, exploits, code-signing certificates and more; why your social media accounts and airline rewards points are valuable to hackers; and how hackers profit from identity theft and the sale of false documents.

Speaker Info

First Name	Last Name	Company
Ryan	Smith	Armor

Date: *11/13/2018* **Time:** *4:00 P.M. - 4:45 P.M.* **Track:** *Security and Technology*

How Financial Services Institutions Can Counter Breaches by Moving to Active Defense

Nine out of ten companies have been breached, 40% report five or more significant incidents this year and five million records are stolen every day. This lively discussion faciliated by a financial services security expert discuss why breaches happen, why 100% security doesn't exist and the investment trends to detection and incident response. The panel will share insights into active defense technology, its value and how it changes the game on attackers.

Speaker Info

First Name	Last Name	Company
Tony	Cole	Attivo Networks
Jim	Trainor	Fmr. FBI
Lance	Spitzner	SANS Security Awareness

Date: *11/13/2018* **Time:** *4:00 P.M. - 4:45 P.M.* **Track:** *Governance, Risk, and Compliance*

Strategies for Co-existing with TLS 1.3

The Internet Engineering Task Force (IETF) is currently rolling out version 1.3 of the Transport Layer Security (TLS) protocol designed to ensure forward secrecy for sessions to prevent pervasive monitoring and establish secure internet connections faster by streamlining the handshake process to maximize performance. This session will describe a proposed public-private collaboration to develop pragmatic solutions for security, compliance and fraud monitoring that do not rely on visibility into TLS connections.

Speaker Info

First Name	Last Name	Company
Donna	Dodson	NIST

Date: ***11/13/2018*** ***Time:*** ***4:00 P.M.*** - ***4:45 P.M.*** ***Track:*** ***Threat Intelligence***

TIP Gardening 101

With the increasing complexity of the threat landscape, more organizations are building a threat intelligence program and ingesting intelligence information from multiple sources. This information can come in a variety of forms and in large quantities making it easy for intelligence analysts to be inundated. A TIP is an important step in the maturity of a secure environment and helps organizations aggregate, correlate and analyze threat data. Learn how one organization cultivated its TIP to grow endless crops of beneficial use-cases such as integration into its data warehouse for monitoring risky users; integration in its internal control systems to look for possible threats; profiling of threat actor campaigns; integration with its workflow and orchestration platform; and integration with its vulnerability scanning tool.

Speaker Info

First Name	Last Name	Company
Brent	Simon	American Express

Date: ***11/13/2018*** ***Time:*** ***4:00 P.M.*** - ***4:45 P.M.*** ***Track:*** ***Security and Technology***

Open Apertures and Unauthenticated Input in Non-Traditional Technologies-- Information Security Risks and Protection Strategies

In this presentation, explore a set of commonly used technologies that may not be closely examined as part of traditional information security programs. However, they likely introduce critical risks via open apertures allowing for unauthenticated inputs by anonymous users. Discover vulnerabilities in a new light in this in this increasingly connected world and hear new strategies through exciting examples that will shape how you interpret "the matrix" around you and assist in your design of security controls to uplift your defenses.

Speaker Info

First Name	Last Name	Company
Ian	Schneller	Bank of America

Date: ***11/13/2018*** ***Time:*** ***4:00 P.M.*** - ***4:45 P.M.*** ***Track:*** ***Security and Technology***

Expanded Tiering System for Cybersecurity Incident Response

This session focuses on an expanded system for rating cybersecurity incidents and how to align the rating system with business and technical impact ratings thereby achieving a greater understanding and faster response by all parties involved in incident response. Explore the expanded tier rating system; the scope of each rating; the related business and technical impacts for each rating; the required participation for each tier rating; and the level of decision-making required.

Speaker Info

First Name	Last Name	Company
Jeffrey	Wiley	MT Bank
Matthew	Braun	MT Bank

Date: ***11/13/2018*** ***Time:*** ***5:00 P.M.*** - ***6:00 P.M.*** ***Track:*** ***Testing and Security Assurance***

Simulating the Adversary To Validate Security

Attackers are relentless, persistent and always looking for the next seam in defenses. Security teams need to adopt the adversary mindset and challenge our security with the same techniques attackers are using. In this session, dive into an emerging technology called Breach and Attack Simulation. Unlike penetration testing or red team engagements simulatior validates security controls continuously using hacker breach methods without risking or interfering with user, data or system activity. Security teams can identify security gaps across their network, in the cloud or on their endpoints, prove where people, process and technologies are working (or not) and remediate ahead of the breach.Hera best practices on implementing breach and attack simulation to effect meaningful changes in multiple security initiatives.

Speaker Info

First Name	**Last Name**	**Company**
Jeff	Williams	SafeBreach
Jeff	Williams	Bain Capital Ventures

Date: ***11/13/2018*** ***Time:*** ***5:00 P.M.*** - ***6:00 P.M.*** ***Track:*** ***Threat Intelligence***

Managing the Insider Threat: Why Visibility Is Critical

It’s no secret that limited visibility into user actions keeps cybersecurity professionals up at night. The right level of cybervisibility for financial services institutions can produce positive insights that enable business results. Additionally, indicators of out of policy activities can stop an insider threat before it becomes a full-blown incident. This session focuses on the key components to gaining full cybervisibility such as user activity, data activity and analytics; how to incorporate insider threat management best practices; and key questions you should be asking to stem the risk of insider threat in your organization.

Speaker Info

First Name	**Last Name**	**Company**
Saikrishna	Chavali	ObserveIT

Date: ***11/13/2018*** ***Time:*** ***5:00 P.M.*** - ***6:00 P.M.*** ***Track:*** ***Cloud***

Corporate Cloud Apps: Why the Dangers Are Not What You Think.

Every financial services firm is talking about how cloud plays into their strategy, especially as they move to Office 365. Cloud security requires a new approach since the protection targets are different. For example, an increase in compromised Office 365 accounts that are used to launch attacks from BEC to internal phishing. One needs to think beyond shadow IT and internal mail scanning and seek visibility into data access, potential threats and user behavior in cloud apps. What are best practices to defend your data in the cloud? Who are the people and what are the third-party apps that access these services? This session explores real-world discoveries that challenge common assumptions.

Speaker Info

First Name	**Last Name**	**Company**
Yair	Grindlinger	Proofpoint

Date: ***11/13/2018*** ***Time:*** ***5:00 P.M.*** - ***6:00 P.M.*** ***Track:*** ***Threat Intelligence***

Turning the Tide - Using Criminal's Stolen Data against Them

Cyber criminals are constantly upgrading their technology to perform more sophisticated, widespread attacks. Preventing breaches and account takeover begins with understanding how criminals operate. This presentation will guide guests through the criminal's timeline and methods, as well as explain why existing prevention products aren't providing the protection organizations think. More interestingly, we will demonstrate how this same data can be used to find criminals true identities! Learn how law enforcement hunts threat actors and how their tactics can be applied to corporate protection.

Speaker Info

First Name	Last Name	Company
Ted	Ross	SpyCloud

Date: ***11/13/2018*** ***Time:*** ***5:00 PM*** - ***6:00 PM*** ***Track:*** ***Security and Technology***

A Phishful of Dollars - How to Automate and Standardize Response

Phishing emails are one of the most frequent, easily executable and harmful security attacks that organizations - especially financial firms - face today. In this session, learn how a Security Orchestration, Automation and Response (SOAR) platform plugs critical gaps within the phishing response lifecycle. An in-depth demo will highlight how SOAR tools unify and automate actions across security products, structure processes through task-based workflows, and free up analysts' time for important decision-making and deeper investigations. The session walks through a phishing use case and underscores how SOAR platforms help.

Speaker Info

First Name	Last Name	Company
Bob	Kruse	Demisto

Date: ***11/14/2018*** ***Time:*** ***3:15 P.M.*** - ***4:00 P.M.*** ***Track:***

Tempt the Titans

After making its debut at the FS-ISAC Annual Summit in the spring, the Tempt the Titans session is back by popular demand. In this session, a select group of tech start-ups, which we call Early Stage Innovators, get a chance to appear on stage and present their technologies before our panel Titans, a group of esteemed CISOs from the FS-ISAC membership. During the Summit, attendees will vote on these Early Stage Innovators to determine which ones get to appear on stage, and tempt FS-ISAC's Titans about how they might best position their solutions in the market.

Speaker Info

First Name	Last Name	Company
Greg	Temm	FS-ISAC
Andy	Matthiesen	Gen Re
Ron	Green	Mastercard
Aman	Raheja	BMO
Kristin	Royster	Bank of America

Date: ***11/14/2018*** **Time:** ***8:15 A.M. - 8:45 A.M.*** **Track:** ***Threat Intelligence***

Understanding the Criminal Mind: How European BEC Syndicates Leverage Business Intelligence

At the FS-ISAC Annual Summit in May, Agari presented a new "Active Defense" model to disrupt business-email-compromise cybercriminals and demonstrated those capabilities by profiling a South African-based BEC "trifecta" gang and one of their victims, Julia. This time, we will move up the criminal pyramid to unveil the inner workings of a large, more sophisticated UK-based criminal organization. We will focus on the collection and dissemination of business intelligence that makes their large-scale BEC attacks possible, revealing the targeting of FS-ISAC member finance teams. We will also share how an FS-ISAC member has used so-called active defense techniques to reveal criminals moving from bank accounts to prepaid cards for theft. Additionally, a leading FS-ISAC financial organization will provide updates about its mule intelligence system and provide recommendations for FS-ISAC members. Members can expect to better understand the criminals and how to leverage threat intelligence and practical tips to disrupt the criminals and their fraud rings.

Speaker Info

First Name	Last Name	Company
Patrick	Peterson	Agari

Date: ***11/14/2018*** **Time:** ***8:45 A.M. - 9:15 A.M.*** **Track:** ***Threat Intelligence***

FBI's Approach to Combatting National Security and Criminal Cyber Threats

This isn't your typical law enforcement briefing. Agent Patel puts the business threat in plain engaging language that will enlighten no matter your level of technical proficiency. This FBI briefing will provide key insights based on case studies and analysis of current and emerging cyber threats to U.S. companies from motivated nation state and criminal adversaries.

Speaker Info

First Name	Last Name	Company
Jay	Patel	FBI

Date: ***11/14/2018*** **Time:** ***9:15 A.M. - 9:45 A.M.*** **Track:** ***Threat Intelligence***

Intelligent Threat Intelligence

The prior approach to assessing threat intelligence measures how good data sources are and the operational utility of this data. This is useful and should be a part of any mature security practice. Learn about a model that attempts to describe the effectiveness of the threat itself and the amount of risk that a remediation mitigates. Explore how remediating 299 CVEs and never worry about those strands again is a more intelligent approach than dealing with attacks and mutations. Context and appropriate statistical blending of the data makes threat intelligence intelligent.

Speaker Info

First Name	Last Name	Company
Michael	Roytman	Kenna Security

Date: ***11/14/2018*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Cloud***

Protecting your Riskiest Asset in the Cloud: Best Practices for Office 365

Between phishing/pretexting and business email compromise, many don't understand the risks and/or view cloud-based email as too risky. As organizations move email from on-prem to cloud-based SaaS such as Office 365 the need emerges to evaluate security controls that could be lost, gained or maintained. In this session hear from an organization that has gone through this analysis, the challenges encountered and solutions found. Understand the choices available for security such as networking, conditional access, classification, email protection, authentication and encryption within Office 365.

Speaker Info

First Name	Last Name	Company
Kenneth	Crist	GEICO

Date: ***11/14/2018*** ***Time:*** ***10:00 AM - 10:45 AM*** ***Track:*** ***Fraud***

Applying a Customer Journey View to Financial Crime

Large banks face hundreds of millions of dollars in online fraud losses annually, often growing at a double-digit rate. This session explores establishing cross-functional capabilities to identify current and emerging threats; developing priority abuse cases to help mitigate some addressable risks; leveraging journey-based principles to engage across lines of business and function; and using a customer-experience lens to redesign authentication and fraud risk-management.

Speaker Info

First Name	Last Name	Company
Salim	Hasham	McKinsey & Company

Date: ***11/14/2018*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Security and Technology***

Global Volatility Risk On Organization Networks

This session is an in-depth look at the frequency, magnitude and manner in which modern enterprise networks change and the risks these changes pose. This session highlights different technological and organizational processes and outlines how these result in unexpected, large and rapid changes in modern enterprise networks as well as how these types of unexpected changes create exposures that have led to large, well publicized breaches.

Speaker Info

First Name	Last Name	Company
Tim	Junio	Expanse

Date: ***11/14/2018*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Governance, Risk, and Compliance***

Focus Security Where It Matters Most

Enterprises are navigating the perfect storm to enable digital convergence across every area of their business while also maintaining a secure environment. With innovation and disruption, the attack surfaces are expanding. This has caused increasing internal and external pressure, as well as security program complexity, while making it nearly impossible to prove return-on-investment or quantify actual mitigation of risk. Please join Dave Ostertag, founder and author of the Verizon Data Breach Investigations Report, as he discusses critical landscape threat trends, threat-data utilization and quantifying ROI to your organization.

Speaker Info

First Name	Last Name	Company
David	Ostertag	Verizon

Date: ***11/14/2018*** ***Time:*** ***10:00 A.M. - 10:45 A.M.*** ***Track:*** ***Resiliency and Recovery***

Diplomacy and Technology: Enhancing Finance Sector Cyber-Resilience is a Global Business

As threat faces develop and diversify with an ever growing pace, so should alliances. Deeper and wider engagement is required and FI partners, governments, law enforcement, military and regulators are part of the solution. The global outlook includes regional (country) engagement and alignment (identify, engage, learn, understand, collaborate). In this session learn how to build the electronic network and how to get people to know, understand and trust each other before they will commit to use it.

Speaker Info

First Name	Last Name	Company
Nicholas	Tuppen	Bank of America

Date: ***11/14/2018*** ***Time:*** ***10:00A.M. - 10:45 A.M.*** ***Track:*** ***Threat Intelligence***

The Business of Strategic Intelligence

This presentation demonstrates how two intelligence veterans used business strategy and proven military methodology tc expand an intelligence shop to a security intelligence arm. Key points include leveraging strategic intelligence to gain executive and board buy-in for tools that action tactical and operational intelligence; understand customers and markets; develop teams and products to meet the needs of target customers; and govern with adaptable, extensible and sustainable doctrine and methods.

Speaker Info

First Name	Last Name	Company
Jonathan	Shiflet	PNC

Date: ***11/14/2018*** **Time:** ***10:00 A.M. - 10:45 A.M.*** **Track:** ***Human Element***

Creating a Women in Tech Employee Resource Group

This presentation will walk through the first year of a Women in Tech (WIT) employee resource group! Discuss how to celebrate the successes; examine the challenges; and cover a step-by-step approach to getting the group started.

Speaker Info

First Name	Last Name	Company
Emy	Dunfee	FirstBank

Date: ***11/14/2018*** **Time:** ***10:45 A.M. - 11:15 A.M.*** **Track:**

Networking Break

Speaker Info

First Name	Last Name	Company

Date: ***11/14/2018*** **Time:** ***11:15 AM - 12:00 PM*** **Track:** ***Security and Technology***

Aligning Procurement & Security to Better Manage Third Party Risk

Procurement and Security groups have typically butted heads when it comes to reviewing the security risk posture of current and prospective third parties. In particular, Security teams are pressed to turn around assessments of third parties with greater speed - all without compromising on the breadth and scope of due diligence. At the same time, Procurement teams are expected to have a more intimate understanding of security concepts than ever before.

Some leading organizations have now implemented new processes and technologies to better manage third party cyber risk without impeding the speed of business decisions. This has created better alignment between Procurement and Security teams, resulting in a better relationship that leads to more effective business decisions.

In this session Hmong Vang, VP of Infosecurity for E*Trade and Jake Olcott, VP of Strategic Partnerships for BitSight discuss:

Why creating alignment between Procurement and Security teams is essential to manage third party cyber risk and create business value
Best practices for gaining trust and fostering more effective relationships between departments
How procurement and security teams should report initiatives and progress to senior leadership and the Board

Speaker Info

First Name	Last Name	Company
Jake	Olcott	Bitsight
Jeff	Ciavone	E*Trade

Date: ***11/14/2018*** **Time:** ***11:15 A.M. - 12:00 P.M.*** **Track:** ***Security and Technology***

Remove Business Friction with Risk Adaptive Protection and UEBA

In our cloud-first world, trust is not absolute. The binary choice of blocking all perceived threats or trusting everyone doesn't work in an anonymous digital world. In order to continue innovation, many organizations have adopted a cloud-first approach, but most do not want to implement wholesale policies that forbid the use of personal devices and cloud apps. However, the same Cloud apps and services that provide tangible business and productivity benefits are the very ones that can invite risk into the business. What if there was a solution that could adapt protection dynamically and apply monitoring and enforcement controls, offering protection based on the risk level of users and the value of data accessed? This could enable security organizations to quickly understand risky behavior and automate the enforcement of policies, dramatically reducing the quantity of alerts requiring investigation and providing more efficient cybersecurity. Join in the discussion around the next generation of data protection. This session explores integrating UEBA with other security technologies, for example: UEBA/DLP solutions for Adaptive Data Insights and UEBA/Endpoint Collection for Adaptive User Insights.

Speaker Info

First Name	Last Name	Company
Homayun	Yaqub	Forcepoint

Date: ***11/14/2018*** **Time:** ***11:15 A.M. - 12:00 P.M.*** **Track:** ***Human Element***

Brain Hacks for Successful CEO Fraud

Understanding psychology and cognitive processes work helps clarify how to secure environments and prevent financial fraud. This session will explore the cognitive processes being exploited by criminals to compromise private and corporate systems through email fraud and social engineering tactics. Learn which cognitive biases are used to allow for an attack to be successful, including simple effective checks and processes to prevent an fraudulent activity to you or your organization.

Speaker Info

First Name	Last Name	Company
Lance	Wantenaar	Worldpay

Date: ***11/14/2018*** **Time:** ***11:15 AM - 12:00 PM*** **Track:** ***Security and Technology***

Security, Privacy, Agility: How Leading Financial Institutions Achieve All Three

With a surge in demand for real-time access, information-sharing, and transaction speeds, financial institutions are facing mounting pressure to re-evaluate their security approaches and postures. And it has brought a massive and complex challenge into focus: embracing technological innovation, adhering to new requirements, and meeting the evolving needs of digital businesses while protecting the world's most valuable and sensitive data sources from a wide range of external and internal threats.

At the same time, the legacy solutions still heavily relied on today are known for being noisy, resource-intensive, and invasive – and they also provide little understanding of what is happening on and off networks. This session will explore how modern financial institutions and global enterprises are leveraging new forms of intelligence to illuminate network and human activities; detect anomalies and banking fraud; and achieve scalable, enterprise-wide visibility while protecting user privacy and empowering trusted insiders. It will also feature real-world use cases and applications, adapted from financial institutions, that underscore the benefits of an agile, intelligence-based security approach.

Speaker Info

First Name	Last Name	Company
Christy	Wyatt	Dtex Systems

Date: ***11/14/2018*** ***Time:*** ***11:15 A.M. - 12:00 P.M.*** ***Track:*** ***Threat Intelligence***

Empowering Your Business With Cyberthreat Intelligence

This session focuses on concepts of using cyber-intelligence to empower the business and key decision makers to drive strategy, policy and a better security posture. Learn about the parts of the intelligence lifecycle as well as methods and techniques that build relationships and trust with your internal business stakeholders and develop meaningful intelligence processes that meet their requirements. This discussion includes best practices for receiving and incorporating feedback, as well as measuring impact and continuous improvement to the intelligence process. Explore some of the challenges of tailoring intelligence for internal consumers and enabling those internal customers to be savvy intelligence users and collaborative partners who embrace external sharing and a partnership approach.

Speaker Info

First Name	Last Name	Company
James	Katavolos	Citigroup
Michael	Swift	Citigroup

Date: ***11/14/2018*** ***Time:*** ***12:00 P.M. - 1:00 P.M.*** ***Track:***

Lunch

Speaker Info

First Name	Last Name	Company

Date: ***11/14/2018*** ***Time:*** ***1:00 P.M. - 1:45 P.M.*** ***Track:*** ***Security and Technology***

The Front Line of the Fight Against Fraud: Behavioral Biometrics

The ability to fight fraud has traditionally come at the expense of user experience. But even with account takeover fraud among the top concerns of financial service organizations, today's hyper-competitive market demands that firms ensure the ability to prevent fraud and cyber attacks without slowing down usability and functionality. This session draws on several use cases where financial service and technology companies have made measurable improvements in fraud prevention by using behavioral biometrics to prevent account takeover, stop fraud and create a frictionless digital user experience.

Speaker Info

First Name	Last Name	Company
Olov	Renberg	BehavioSec
Alan	Goode	Goode Intelligence

Date: ***11/14/2018*** ***Time:*** ***1:00 P.M. - 1:45 P.M.*** ***Track:*** ***Threat Intelligence***

The TIC's Role in FS-ISAC's Threat Intel Sharing

Join members of the Threat Intelligence Committee (TIC) in a panel discussion on the purpose and role of the TIC. As the financial-sector member interface with FS-ISAC, the TIC is designed to ensure members are receiving the support needed to provide intelligence to their organizations. In this session, TIC members will provide an overview of the TIC charter and what it means to FS-ISAC members. This panel will also discuss the information-sharing mission, monitoring the threat environment to ensure member awareness and utilizing subject-matter expertise to provide guidance to FS-ISAC members as well as a Q&A.

Speaker Info

First Name	Last Name	Company
Tom	Scarborough	Fifth Third Bank
Max	Morris	Ally
David	Goodpaster	TD Bank
Greg	Temm	FS-ISAC
John	Suver	Bank of America

Date: ***11/14/2018*** ***Time:*** ***1:00 P.M. - 1:45 P.M.*** ***Track:*** ***Security and Technology***

Overcoming the Cyber-Risk Dilemma: How Do You Know Where You Stand?

This session outlines how security professionals can use continuous security validation to gain visibility into the effectiveness of their security controls, get insights into the things that matter most, and evolve and rationalize security within the context of their cyberprograms.

Speaker Info

First Name	Last Name	Company
Mike	Spanbauer	NSS Labs

Date: ***11/14/2018*** ***Time:*** ***1:00 P.M. - 1:45 P.M.*** ***Track:*** ***Security and Technology***

Operationalizing Automation and Workflow

An interactive discussion cyberfusion center implementation of an orchestration platform to help proactively gather evidence to quickly remediate attacks from threat actors using automated software-defined security methods. Learn how tp be able to automatically unify, analyze and resolve alerts from existing security tools by leveraging a single stream and integrated management process. Also hear 'lessons learned' on leveraging the security orchestration engine to improve efficiencies, standardize processes and automate tasks.

Speaker Info

First Name	Last Name	Company
Gregory	Razka	American Express
Deborah	Janeczek	American Express

Date: ***11/14/2018*** ***Time:*** ***1:00 P.M.*** - ***1:45 P.M.*** ***Track:*** ***Security and Technology***

Measuring Metrics that Matter – Help Management with Decision Making and Improve the

Information security metrics presents a holistic view of the information security posture of the organization and is the key to analyze and aggregate metrics for different domains and provide an overall security risk score card to help them with decision making. Visualizing and leveraging cybersecurity data is of utmost importance in today's world and viewers will gain practical skills in how they can build out a similar function in their organization. The overall objectives of the project is to improve the security posture of the organization (people, processes, technology and operations); effectively communicate the information security posture; drive performance improvement; prioritize and mitigate high-risk areas; improve security operations by providing quantitative measurements supported by trending; and demonstrate the value of investment and help with decision making.

Speaker Info

First Name	Last Name	Company
Sanaz	Sadoughi	International Monetary Fund

Date: ***11/14/2018*** ***Time:*** ***1:00 P.M.*** - ***Track:*** ***Governance, Risk, and Compliance***

Cybersecurity Due-Diligence SWIFT KYC CSP

Utilizing the SWIFT KYC CSP counterparty control attestation portal we are able to engage with counterparty BIC owners. A scoring model was developed to score the responses from the granted access attestations. Using the sixteen required controls, we are able to monitor the implementation of the controls due 12/31/18. The scoring results serve as guidance to our GRC organization for the implemented controls. Unlike the Standard Information Gathering or other questionnaires the SWIFT KYC CSP attestations provide attestations to relating to each BIC.

Speaker Info

First Name	Last Name	Company
Ronald	Jones	CLS-Bank

Date: ***11/14/2018*** ***Time:*** ***1:00 P.M.*** - ***Track:*** ***Governance, Risk, and Compliance***

New York DFS Cybersecurity Requirements - Challenges and Solutions

While most compliance dates for the NY DFS Cybersecurity regulation have passed, a wave of cyber-regulation continues to sweep across many states. Many of the regulations in the coming year will be based on NY DFS or a version of the NAIC model law. Join this session to hear from several leaders in information security regarding how to address these new regulations and overcome organizational and technical challenges during implementation.

Speaker Info

First Name	Last Name	Company
John	Rogers	BNP Paribas
Andy	Matthiesen	Gen Re

Date: ***11/14/2018*** ***Time:*** ***1:00 P.M.*** ***-*** ***Track:*** ***Governance, Risk, and Compliance***

What's in a Framework?

Without a framework, an assessment is a non-repeatable, point-in-time exercise that can lead to poor, or worse, harmful outcomes. There are various frameworks, and crosswalks between frameworks. In this TED Talk you'll hear how to figure out what a framework can mean, even if you're a community institution.

Speaker Info

First Name	Last Name	Company
William	Bailey	Police & Fire FCU

Date: ***11/14/2018*** ***Time:*** ***7:00 A.M.*** ***-*** ***8:00 A.M.*** ***Track:***

Breakfast

Speaker Info

First Name	Last Name	Company

Date: ***11/14/2018*** ***Time:*** ***1:00 P.M.*** ***-*** ***1:45 P.M.*** ***Track:*** ***Governance, Risk, and Compliance***

How Infosec Oversight Requirements are Changing/Strengthening Due to Compliance Reqs

This panel will discuss how InfoSec oversight requirements are changing and strengthening due to compliance regulations. Hear about the challenges this presents and approaches to compliance.

Speaker Info

First Name	Last Name	Company
Peter	Falco	FS-ISAC
Meg	Anderson	Principal
Dennis	Lamm	Fidelity Investments
Josh	Magari	BITS

Date: ***11/14/2018*** **Time:** ***2:00 P.M. - 2:45 P.M.*** **Track:** ***Security and Technology***

STIX2/TAXII2 Workshop

This workshop will explore the new STIX and TAXII standards, looking at a brief background on what changed and why, and what we can expect in future STIX2 and TAXII2 releases. The workshop will include interactive coding examples using the python stix2 and taxii2 libraries to model a real-word threat report, integrate TAXII2 threat feeds into MISP, and generate STIX2 sightings.

Speaker Info

First Name	Last Name	Company
Chris	Ricard	FS-ISAC

Date: ***11/14/2018*** **Time:** ***2:00 P.M. - 2:45 P.M.*** **Track:** ***Security and Technology***

Crypto-Agility Task Force Update

In this session join the Crypto Agility Task Force to review emerging threats related to public-key infrastructure and certificate authorities. Learn best practices for mitigating the risks associated with those threats.

Speaker Info

First Name	Last Name	Company
Dave	Edelman	Citi Bank
Bob	Blakely	Citi Bank

Date: ***11/14/2018*** **Time:** ***2:00 P.M. - 2:45 P.M.*** **Track:** ***Resiliency and Recovery***

How to Solve Cybersecurity in the Next Five Years

Over the next few years attackers wil refine and mature their capability to drive outcomes that result in the inability to recover from an attack. This session explores the compelling need to consider new, business-aligned design patterns that enable systems that are fully resilient against destructive, irreversible attacks and why you should consider pivoting to this approach within the next five years to survive. The session will touch on the implications for our industry and reveal a new set of concrete measurements and metrics that enable us to focus on true solutions and not just an never-ending list of vulnerability and patching metrics.

Speaker Info

First Name	Last Name	Company
Sounil	Yu	Bank of America

Date: ***11/14/2018*** ***Time:*** ***2:00 P.M. - 2:45 P.M.*** ***Track:*** ***Governance, Risk, and Compliance***

Briefing your Board of Directors

Cybersecurity has taken over corporate governance as the number one topic of interest. How should you engage? This session features hands-on tips direct from a CISO on communication cadence, material, and metrics. Rounded out with discussion on what works, what falls flat and predictions on what's next.

Speaker Info

First Name	Last Name	Company
Jerry	Perullo	ICE/NYSE

Date: ***11/14/2018*** ***Time:*** ***2:00 P.M. - 2:45 P.M.*** ***Track:*** ***Fraud***

Threat intelligence Based Blocking of Investment Fraud and Love Scam

This presentation will explore how one organization focused on investment in fraud and love scams. To get a better picture of the types of criminals targeting customers we will walk through practical examples of how this information helped drive a counter fraud department and reduce customer losses. Learn how cross-sector cooperation is imperative to counter the growth in organized crime and financial institutions play a central part in such cooperation.

Speaker Info

First Name	Last Name	Company
Sebastian	Takle	DNB

Date: ***11/14/2018*** ***Time:*** ***2:00 P.M. -*** ***Track:*** ***Threat Intelligence***

Combatting Complex Attacks against Payment Systems

Financial institutions experience complex attacks against their ATM networks and wholesale cross-border payment systems on an ongoing and regular basis. Law enforcement has provided alerts about pending attacks and follow-up analysis attributes many of these attacks to nation-states. This members-only workshop, reviews these complex payments attacks and provides best practices for risk mitigation.

Speaker Info

First Name	Last Name	Company
Charles	Bretz	FS-ISAC
Mandy	Misko	FS-ISAC

Date: ***11/14/2018*** ***Time:*** ***2:00 P.M.*** ***-*** ***Track:*** ***Security and Technology***

Protecting Your Bank While Positioning for the Rewards of FinTech

AI, machine learning and interconnected devices are increasing the volume, sophistication and targets for cyber attacks throughout the world. Today, cybersecurity requires layers of protection and must be approached and supported holistically from the C-Suite throughout the bank, employees and customers. Join this panel of C-Suite banking executives to learn about the implementation of .BANK as a foundation for layers of cybersecurity, how they planned for and executed the migration, how they've benefited, how customers responded and where they see things evolving within their new, more secure, digital channels.

Speaker Info

First Name	Last Name	Company
David	Saleh	First National Bank of Louisiana
Craig	Schwartz	fTLD Registry Services
Travis	Collins	First National Bank in Louisiana

Date: ***11/14/2018*** ***Time:*** ***2:00 P.M.*** ***-*** ***2:45 P.M.*** ***Track:*** ***Threat Intelligence***

Automating Phishing Site Takedowns Using Splunk

Phishing sites who target customers of financial institutions that occur outside of enterprise networks are a significant problem, and taking action to mitigate the risks and reduce the customer impact is difficult. This presentation outlines a strategy that relies on threat intelligence research, web-facing application logs in Splunk and automation to discover and submit phishing site URLs to an external vendor for quick takedown, reducing the time from discovery to removal. Lessons learned from the implementation and adjustment to this process and ideas for future iterations will be highlighted.

Speaker Info

First Name	Last Name	Company
Jordan	Berry	BB&T

Date: ***11/14/2018*** ***Time:*** ***2:45 P.M.*** ***-*** ***3:15 P.M.*** ***Track:***

Networking Break with Raffle

Speaker Info

First Name	Last Name	Company