Date: ***30/10/2017*** ***Time:*** ***1100*** ***- 1130***

Ten Changes in Cyber Regulation: Number Six Will Shock You

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

Speaker Info

First Name	Last Name	Company
Stephen	Bonner	Deloitte

Date: ***30/10/2017*** ***Time:*** ***1145*** ***- 1230***

Lightning Talks

Speaker Info

First Name	Last Name	Company
Nick	Tuppen	FS-ISAC

Date: ***30/10/2017*** ***Time:*** ***1145*** ***- 1230***

Red Teaming the C-Suite: The Ultimate InfoSec Awareness Program

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

Speaker Info

First Name	Last Name	Company
Thomas	Stephenson	S&P Global

Date: ***30/10/2017*** ***Time:*** ***1145*** ***- 1230***

Know Thy Enemy: Views from the Deep and Dark Web Underground

The deep and dark web (DDW) is a rich source of data full of black market products and services, weapons and training manuals, malicious TTPs and dialogue between threat actors. Threatening activity from the most difficult to access and high-risk areas in the DDW can harm an organization's business, stakeholders, employees and customers.
This session will outline some of the challenges involved in effectively tracking and monitoring threats on the DDW including dispelling common myths surrounding attackers operating within these communities and providing insight into their mindsets and motivations through examples from past and current events.

Speaker Info

First Name	Last Name	Company
Maurits	Lucas	Flashpoint

***Date:* 30/10/2017 *Time:* 1230 - 1330**

FS-ISAC 101

This session is an interactive workshop on FS-ISAC services. It provides and 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
Greg	Temm	FS-ISAC

***Date:* 30/10/2017 *Time:* 1330 - 1415**

Offline and Local: The Hidden Face of Cybercrime

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

Speaker Info

First Name	Last Name	Company
Jonathan	Lusthaus	University of Oxford

***Date:* 30/10/2017 *Time:* 1330 - 1415**

Lessons Learned from the Frontlines: Responding to WannaCry and Petya

In this session, we will discuss the lessons learned by Microsoft in responding to the WannaCrypt and Petya attacks. This session will evaluate the techniques utilized to carry out these attacks and examine the specific mechanisms used by the malware to spread once inside an organization. We will also evaluate and share the technical guidance for responding to such attacks and explain the best practices we derived from our post mortem, incident response activities for making organizations more resilient against these and similar attacks. Future innovations and areas for information sharing and global collaboration to address such threats will be discussed.

Speaker Info

First Name	Last Name	Company
Jonathan	Trull	Microsoft

***Date:* 30/10/2017 *Time:* 1330 - 1415**

Detecting Breaches Using Deep Visibility into Malware Behaviors

Cybercriminals are extremely creative at slipping past defenses to get a foothold inside a network. A recent survey conducted at Black Hat found that 55% of respondents had suffered a breach. So, the challenge becomes how to detect a network breach before sensitive data is compromised. This presentation describes how breach detection starts with a detailed analysis of specific behaviors that malware is designed to execute that then can be correlated with detected network activity to separate benign activity from seemingly low-risk activity that can be deterministically associated with known malware behavior. The result is high success with detecting network breaches with low false positives.

Speaker Info

First Name	Last Name	Company
Marco	Cova	LastLine

***Date:* 30/10/2017 *Time:* 1445 - 1530**

Quantifying Cyber-Risk Using Threat Objectives Lifecycle Approach

This presentation will describe a Threat Objectives approach in quantifying cyber risk and effectively engaging business, management and governance structures in assessing the cyber threat landscape.

Speaker Info

First Name	Last Name	Company
Burim	Bivolaku	Intercontinental Exchange

***Date:* 30/10/2017 *Time:* 1445 - 1530**

Adversary-Centric Threat Hunting and Mitigation

There are a variety of ways to go threat hunting in an environment. This session will focus on a method of threat hunting that involves simulating attacker activity, scouring logs for evidence and then searching iteratively across the environment for signs. Learn how to develop countermeasures and mitigations against tools and attacks that can carry this approach into a quasi-red team activity.

Speaker Info

First Name	Last Name	Company
Colby	DeRodeff	Anomali
Travis	Farral	Anomali

***Date:* 30/10/2017 *Time:* 1445 - 1530**

What's in your Digital Footprint? A Retrospective on Recent Bank Attacks and High-Profile Vulnerabilities

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

Speaker Info

First Name	Last Name	Company
Fabian	Libeau	RiskIQ

***Date:* 30/10/2017 *Time:* 1600 - 1700**

Evolution of the Threat Landscape: Behind the Scene

Financial malware, remote access Trojans, targeted attacks and ransomware are among the most common manifestations of cybercrime and part of cybercrime's natural evolution. This presentation will provide an overview on the whys and wherefores of the ongoing cat-and-mouse game between criminals and security experts.

Speaker Info

First Name	Last Name	Company
Gaetan	van Diemen	Fox-IT

***Date:* 30/10/2017 *Time:* 1600 - 1700**

Eliminating Payment System Attacks

Cyber-attacks on financial payment systems have become a fact of life. Watering-hole attacks disseminating web-based malware and targeted spear phishing emails are increasingly utilized by attackers. No matter the size of the security team, institutions of all sizes assume the same amount of risk by allowing employees free access to the web and to click on web and document links in email. Traditional detection-based security products prove ineffective. Security professionals are locked in a cat-and-mouse struggle with smart, motivated, well-financed attackers, where detection-based prevention technology sparks a new generation of attacks to evade defenses. In this session learn methods to prevent payment systems attacks.

Speaker Info

First Name	Last Name	Company
Jason	Steer	Menlo Security

***Date:* 30/10/2017 *Time:* 1600 - 1700**

Uncovering Fraud Faster and More Effectively

With customers expecting faster and more convenient services, the challenge isn't just intercepting suspicious transactions it's also enabling legitimate transactions to proceed without interruption. To more effectively assess the fraud risk, it requires the ability to view account activity in context across channels. This session will review an approach that helps spot new patterns more quickly, connect the dots to deliver more accurate risk assessments and adaptive intelligence so organizations can adapt faster and apply countermeasures more quickly.

Speaker Info

First Name	Last Name	Company
Ayelet	Avni	IBM Security

***Date:* 30/10/2017 *Time:* 1600 - 1700**

Attacker Resistance: Redefining Risk from a Hacker Perspective

When it comes to understanding your security risk, hope is not a course of action. Today, breaches are leading to stolen financial assets, reputation loss and damage to the business. Unfortunately, traditional models fall short when trying to assess risk. Organizations need to bring hackers in the loop to truly understand the human ingenuity behind an attack and the system's hardness against it. In this session, learn how you can assess your risk from the adversary's perspective, using a crowd of the world's most skilled and vetted ethical hackers paired with groundbreaking vulnerability intelligence technologies.

Speaker Info

First Name	Last Name	Company
Jay	Kaplan	Synack

***Date:* 30/10/2017 *Time:* 1600 - 1700**

Pinpointing a Cyber Attacker Quickly using Behavioural Analytics

Detecting insider threats quickly whether from ransomware, an external attacker with stolen credentials, or from an employee, remains a challenge for many financial institutions. However new advances in the area of behaviour analytics and intelligent automation are now rapidly accelerating the detection, investigation and response to threats – far outpacing legacy systems – and turning the tide in favour of the security analysts. This session takes a look at these developments and how they pinpoint an attacker.

Speaker Info

First Name	Last Name	Company
TBD		Exabeam

***Date:* 31/10/2017 *Time:* 0945 - 1015**

Real-Time Risk Management

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

Speaker Info

First Name	Last Name	Company
David	Damato	Tanium
Ryan	Kazanciyan	Tanium

***Date:* 31/10/2017 *Time:* 1115 - 1200**

The Year in Cyber: Annual Review & Predictions

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

Speaker Info

First Name	Last Name	Company
Teresa	Walsh	FS-ISAC

Date:* *31/10/2017 ***Time:* *1115* - *1200***

Trends, Predictions & Real-world Tradecraft. The Lessons Learnt in Responding to the Most Advanced Attacks

2017 will be remembered as a year where nation state hacking dominated the media. These attacks are the most challenging that any organization can face because a nation state actor can invest a significant amount of R&D to target an organisation and isn't driven by a profit motive. Yet techniques adopted by these actors invariably find their way into the mainstream criminal world and are a leading indicator of what to prepare for. In this briefing, our speakers look to the year ahead and make predictions of what you should expect to see and how you should focus your resources. Using real-world examples to illustrate the extraordinary tradecraft that is routinely employed to steal state secrets, gain access to critical infrastructure or poach valuable intellectual property, we will expose how the European threat landscape has changed in recent months.

Speaker Info

First Name	Last Name	Company
Zeki	Turedi	CrowdStrike

Date:* *31/10/2017 ***Time:* *1200* - *1300***

Applying Fraud Data to Improve Risk-Based Decisions

Analysis of large volumes of data to identify the behavioral patterns associated with genuine and fraudulent activity is critical to improve the accuracy of fraud risk assessments and detection capabilities. From mobile to mules, this session will highlight various characteristics and trend patterns across a number of fraud use cases as seen within RSA's Risk Engine including the relationship between fraud, new accounts, and device and channel type.

Speaker Info

First Name	Last Name	Company
Ian	Newns	RSA

Date:* *31/10/2017 ***Time:* *1115* - *1200***

CISO Case Study: Teaching Old Data New Tricks

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

Speaker Info

First Name	Last Name	Company
Nik	Whitfield	Panaseer
Rob	Hyde	Schroders Plc

***Date:* 31/10/2017 *Time:* 1200 -**

Security Orchestration: The Future of Incident Response

In this session, hear how financial services customers worldwide are improving their security posture through security orchestration and automation. As the volume of sophisticated attacks continues to grow, security teams need to leverage the security tools in their arsenal to reduce their time to detect and contain attacks, this session will showcase examples of how organisations are combining people, process and technology to better coordinate their response strategy.

Speaker Info

First Name	Last Name	Company
Allen	Rogers	IBM Security

***Date:* 31/10/2017 *Time:* 1330 - 1415**

Cyber-Attack against Payment Systems (CAPS), EMEA 2017 After-Action Report

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

Speaker Info

First Name	Last Name	Company
Charles	Bretz	FS-ISAC

***Date:* 31/10/2017 *Time:* 1330 - 1415**

A Journey into Hancitor

The presentation will provide an introduction into Hancitor malware and related phishing campaigns, associated TTPs and the conclusion from research into the delivery and C2 infrastructure used by Hancitor and links to other malicious activity.

Speaker Info

First Name	Last Name	Company
Edward	Millington	Winton Group

***Date:* 31/10/2017 *Time:* 1330 - 1415**

Collective Security – Prairie Dogs versus Humans

As the security industry has continued to under invest in the human element of security, phishing has become the top attack vector for cybercriminals. Breaches continue to occur in record numbers, identification takes an exorbitantly long time and the most preferred target is an organization's human assets. Empowering human assets to provide vetted intelligence into your incident response teams is often overlooked. Every organization has these human sensors and there's a natural desire for these employees to want to help. In this presentation learn why the cybersecurity industry is broken; how to reduce susceptibility to human-targeted attacks; and how to empower users to become human sensors to recognize and report suspected attacks.

Speaker Info

First Name	Last Name	Company
Jim	Hansen	PhishMe

***Date:* 31/10/2017 *Time:* 1445 - 1530**

Positive Regulatory Engagement over Regulation: The Changing Nature of the Relationship

Cyber-resilience is a sector top priority and regulators want to be part of the solution not the problem. Rather than dictating compliance regulators are looking to collaborating on security. This session explores how coordination of cybergroups are proving to be a vehicle for open and productive collaboration. Learn about how CBEST helped modify the intrusive nature of the testing and has changed the relationship that firms' cybersecurity teams have with their regulators, reinforcing the desire for a collaborative over a compliance based approach to securing the sector.

Speaker Info

First Name	Last Name	Company
Simon	Onyons	Financial Conduct Authority
Robin	Jones	Financial Conduct Authority

***Date:* 31/10/2017 *Time:* 1445 - 1530**

Keeping Up with FinTech: Security Testing in a Fast-Paced World

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

Speaker Info

First Name	Last Name	Company
Ralf	Huuck	Synopsys

***Date:* 31/10/2017 *Time:* 1445 - 1530**

Betrayal-as-a-Service: Proliferation of Insider Spies and the Future of Theft

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

Speaker Info

First Name	Last Name	Company
John	Wetzel	Recorded Future

Date: ***1/11/2017*** ***Time:*** ***0900*** ***- 0945***

Ransomware and WannaCry: Sharing Experiences of the Critical Success Factors. Now What's Next?

This session features a panel discussion with key specialists from financial services, including a brief presentation on the history of ransomware, key insights into the threat, the impact of ransomware and how best to defend against it. Learn about trends and developments, the main challenges of ransomware, the human factor, destructive wiper attacks, what could be on the horizon and more.

Speaker Info

First Name	Last Name	Company
David	Aubrey-Jones	RBS

Date: ***1/11/2017*** ***Time:*** ***0945*** ***- 1030***

Innovation Challenge

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

Speaker Info

First Name	Last Name	Company
TBD		FS-ISAC

Date: ***1/11/2017*** ***Time:*** ***1045*** ***- 1130***

Developing an Intel Sharing Maturity Model

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

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

Speaker Info

First Name	Last Name	Company
TBD		FS-ISAC

Date: ***1/11/2017*** ***Time:*** ***1045*** ***- 1130***

Money Muling

Case study of how easy phished financial data can be monetized with the use mules.

Speaker Info

First Name	Last Name	Company
Derek	Pillar	Mastercard

Date: 1/11/2017 Time: 1045 - 1130

Threat Intelligence-Led Red Teaming Frameworks in Europe

Threat intelligence-led red teaming frameworks are gaining popularity. Testing the cyber-resilience of the financial sector by simulating advanced attackers on live systems is being introduced by multiple authorities in Europe and beyond. This presentation reviews development of the different frameworks by regulators and central banks, where they differ and what the expected developments of the future are.

Speaker Info

First Name	Last Name	Company
Maarten	Bras	Dutch Central Bank

Date: 1/11/2017 Time: 1145 - 1215

DDoS Threat

Update on the DDoS threat and the work of the DDoS JWGI. Full details not yet worked out but mooted suggestion with Teresa and Ray at FS-ISAC Spring Summit in Orlando.

Speaker Info

First Name	Last Name	Company
Tracy	Watts	Lloyds Banking Group
Paul	Branley	Lloyds Banking Group

Date: 1/11/2017 Time: 1145 - 1215

Threat Intelligence-Led Red Teaming Exercises- Participant Panel

A panel session featuring representatives of some of the firms that have already undertaken regulatory-led and central bank led red-team exercises. This panel will discuss the pros and cons of the exercises and how they differ from internally driven schemes; how they see the role of the regulator or central bank running the scheme and how this has changed over time; and offer their insights into how the frameworks may evolve in the future. Attendees will also discover lessons learned from early participants and why it is not necessary to carry out pre-testing ahead of these regulatory and central bank led red teaming exercises.

Speaker Info

First Name	Last Name	Company
Dave	Evans	UBS

Date: 1/11/2017 Time: 1330 - 1415

From Secure Cloud to Competitive Advantage

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

Speaker Info

First Name	Last Name	Company
Mario	Maawad	Caixabank
Romana	Sachova	Caixabank

Date: 1/11/2017 Time: 1330 - 1415

Cybersecurity and the 323 Year Old Bank: Using Threat Intelligence to Tell Your Story and Inspire Your People

Cybersecurity is a people challenge every bit as much as is it a technical challenge. Unlike technology, people need motivating, educating and inspiring and when you get this right, your people become your first line of defence. This presentation will show how threat intelligence was used to tell the story of why cybersecurity matters in a 323-year-old organisation and how threat intelligence drives risk, policy, education and investment as well as threat detection.

Speaker Info

First Name	Last Name	Company
Andrew	Huddart	Bank of England

Date: 1/11/2017 Time: 1430 - 1515

From Compliance to Culture, from Awareness to Action

Most organisations now agree that as part of a rounded cyber defence programme, staff awareness, training and education have a large part to play. So why isn't it working? In this session John Scott will discuss why focussing on awareness isn't enough, and why successful organisations need to look at behavioural and ultimately cultural change to turn their people from the weakest link to the strongest. He will share the approach the Bank of England has taken on this and look at what simple steps any organisation can take to make their staff the first line of defence.

Speaker Info

First Name	Last Name	Company
John	Scott	Bank of England

Date: 1/11/2017 Time: 1430 - 1515

Innovation Bridges

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

Speaker Info

First Name	Last Name	Company
Dr. Tal	Steinhartz	Israeli National Cyber Directorate

***Date:* 1/11/2017 *Time:* 1430 - 1515**

SWIFT's Customer Security Programme – Creating a Security Baseline for Financial Services

In recent and well publicised cases, SWIFT customers have suffered targeted, sophisticated and patient APT cyber-attacks on their local infrastructure that steal valid operator credentials and submit fraudulent payment messages.

While customers are responsible for protecting their own environments, SWIFT's Customer Security Programme (CSP) was established as a direct response this this ever-evolving threat to support customers fight against cyber-attacks, help recover lost funds and create a security baseline for cyber-hygiene across global financial services.

This session provides an update on the CSP Programme (securing and protecting your environment, preventing and detecting fraudulent activities with your counterparts and sharing information with the community) and includes an overview and timetable of the mandatory and advisory security controls, against which all 11,000 SWIFT customers will need to attest their compliance.

Combating cyber fraud is a challenge for the whole industry - there are no quick fixes - both SWIFT and its customers have to remain vigilant and work together to mitigate the risks.

Speaker Info

First Name	Last Name	Company
Tony	Wicks	SWIFT

***Date:* 1/11/2017 *Time:* 1530 - 1615**

Public-Private Partnerships: UK NCSC and US NCCIC Update

Speaker Info

First Name	Last Name	Company
Mandy	Misko	FS-ISAC
Lucie	Usher	FS-ISAC