MISSION: Share Timely, Relevant, Actionable Cyber and Physical Security Information & Analysis

- A nonprofit private sector initiative formed in 1999
- Designed/developed/owned by financial services industry
- Mitigate cybercrime, hactivist, nation state activity
- Process thousands of threat indicators per month
- Sharing information globally
- Members: 7,000 + financial institutions (up from 64 in 2004)
- Growth continues
  - Members in 72 countries using Member Portal
  - Variety of membership models
What the FS-ISAC Does

- Information Sharing
- Analysis
- Threat Monitoring & Crisis Escalation
- Exercises
- Support for regional coalitions
- Automation/“Soltra”
- Conferences/Education/Training
- Best Practices/Advisories
  - Collaboration with SWIFT in response to account takeover attacks
- Global Growth
- Support for other Sectors
- Platform for collaboration w/ other sectors and gov agencies
- Communications, including monthly executive brief
Global Momentum, Regional Sharing

- Members in 72 countries actively using Member Portal
- 10 regionally focused staff in 7 countries
- IBM after-hours operation to provide 24x7 support for posting alerts from member submissions
- Country-wide and regional initiatives:
  - Dedicated European intelligence officer and analyst base in region.
  - European Threat & Strategy Committee
  - APAC Threat & Strategy Committee
  - Regular Regional Threat Calls and Summits
  - Regional Joint Working Group Initiatives
  - Agreement for country-level sharing in Japan
  - Agreements for country-level sharing in Netherlands
  - Regional Joint Working Group Initiatives
## Example: FS-ISAC European Activity

### Membership
- 14 countries in Europe
- Relationships with external law enforcement and industry security organizations
- Representation EMEA Cyber-Security Strategy NIS working group, ENISA EG-FI, JWGI

### Services
- Bi-weekly Euro threat briefing call
- Region-specific mailing lists
- Regional working groups: insider threat, legal & regulatory, security testing.
- European Threat & Strategy Committee
- EMEA CAPS Exercise

### Events & Meetings
- FS-ISAC Summit Barcelona 7-9 Nov 2016 (prior European Summits in London)
- Multiple regional workshops (banking fraud & best practices, cloud, sharing best practice)
- Multiple regional member meetings UK, FR, NL, ES, DE.
Example: FS-ISAC/Netherlands Agreement

- Final agreement executed February 1, 2016 with Dutch Payments Association
- Nine Dutch financial services companies joined FS-ISAC
- Remaining small Dutch financial services companies allowed to join at no additional cost.
- Access to FS-ISAC worldwide information sharing of threat intelligence, vulnerability and incident information.
- Win-win for both organizations and for Dutch financial services companies.

- Other news: Vincent Thiele, ING CISO, elected to FS-ISAC Board of Directors.
Threat Landscape: Adversaries

**Cyber Crime**
- Bad actors are typically concentrated in a few geographic areas but utilize a global hacking infrastructure
- A complete service based economy supporting activities
- Attacks, often blended threats, a mix of social engineering and technical attack

**Hacktivists**
- “Anonymous” response to WikiLeaks donation stoppage
- DDoS attacks
- Website defacement

**Nation State**
- Motivations: espionage, disruption, or destruction
- Targeting Government + private sector
- Attempt to gain economic advantage
Top Tactics of Malicious Cyber Adversaries

- Destructive malware
- Business email compromise leading to fraudulent wire transfers
- Targeted spear-phishing campaigns
- Ransomware attacks
- Distributed denial of services (e.g., “DDoS for Bitcoin”)
- Supply chain threats (including hardware and software integrity)
- Blended physical and cyber attacks
- Mobile platforms
- Social Media
- Insider threats
Example: Business Email Compromise (BEC) 2016 Major Losses

- Mid-sized Belgian bank targeted in January 2016, lost over €70 million
- Belgian newspapers report the bank was a victim of CEO fraud (or BEC scam – Business Email Compromise).
- FACC, Austrian aerospace parts manufacturer, terminates its CFO for a €50 million BEC loss that occurred in January.
- Two possible tactics:
  1) Email system compromise including CEO emails and calendar; or
  2) spoof of CEO’s email address, e.g., Xxxx@Belgianbank.co instead of Xxxx@Belgianbank.com.
- FS-ISAC and law enforcement have been warning of these new BEC tactics for over a year.

Sources: Help Net Security, posted 1/26/2016; Reuters, 2/3/2016
Circles of Trust

- Clearing House and Exchange Forum (CHEF)
- Payments Risk Council (PRC)
- Payments Processor Information Sharing Council (PPISC)
- Business Resilience Committee (BRC)
- Threat Intelligence Committee (TIC)
- Community Institution Council (CIC)
- Insurance Risk Council (IRC)
- Compliance and Audit Council (CAC)
- European Threat & Strategy Committee (ETSC)
- Singapore Threat Intelligence Group (STIG)
- Cyber Intelligence Listserver
- Broker Dealer Council
- Securities Industry Risk Group (SIRG)
  - Asset Managers, Alternative Investors, Broker Dealers
- APAC Threat & Strategy Committee (ATSC)
FS-ISAC Information Flow

Information Sources
- CERTs
- FS Regulators
- Law Enforcement
- Other Intel Agencies

Government Sources
- Threat Intelligence Providers
- Vulnerability Alerting
- Malware Forensics
- PS Incidents & Analysis
- After hours IAT support

Private Sources
- Cross Sector (other ISACS)
- Open Sources (Hundreds)

CROSS SECTOR SOURCES

FS-ISAC 24x7 Security Operations Center

Member Communications
- Information Security
- Physical Security
- Business Continuity/Disaster Response
- Fraud Investigations
- Payments/Risk

Alerts
Member Submissions

TLP Green

GOVERNMENT SOURCES
Example: FS-ISAC Response to SWIFT Related Bank Heist

April: FS-ISAC’s ISAC Analysis Team tracked incident updates and sent regular updates to members. FS-ISAC members continuously shared voluntary information on threats and analysis.

Late April: As news broke, FS-ISAC’s Media Response Team, made up of communications professionals from member firms, developed media speaking points.

May 9: FS-ISAC shared Indicators of Compromise (IOCs) and important SWIFT software updates with its members.

April-May: FS-ISAC’s CEO and other execs took multiple press calls and educated reporters and counterbalance “fear, uncertainty and doubt” or FUD.

- Key messages included the fact that SWIFT itself was not attacked nor compromised.
- FS-ISAC secured an approved statement from SWIFT that it added to the key messages.
- FS-ISAC worked with experts at other payment associations on an overview document on how SWIFT works.
Example: FS-ISAC Response to SWIFT Related Bank Heist

**June 1:** FS-ISAC convened a member conference call with over 2,700 attendees. FS-ISAC executives, member facilitators, SWIFT, and FBI provided briefings.

**June 7:** US financial regulatory agencies issued a statement on safeguarding the cybersecurity of interbank messaging and payment networks that includes reminders of prudent security controls and existing regulatory requirements.

**June:** Additional SWIFT Indicators of Compromise sent to members.

**June 21:** FS-ISAC CEO appears in SWIFT cybersecurity video posted to SWIFT website.

**June 22:** FS-ISAC Chief of Staff participates in cyber security panel with SWIFT at Fed-sponsored Secure Payments meeting.

**July 1:** Released *Security of Payment Network Access Points: Risk Mitigation Recommendations Related to Recent Payment Account Takeover Attacks Against Banks Leveraging the SWIFT Network*

- Developed in collaboration with member financial institutions experts and associations, including American Bankers Association, BITS division of the Financial Services Roundtable and NACHA.
- Provides an overview of best practices and recommendations for risk mitigation, building upon the 2012 FS-ISAC paper *Recommended Practices for Financial Institutions to Prevent, Detect and Respond to Corporate Account Take Over Fraud*.
Investment in Protecting the Sector

• Maintain Automated Indicator Sharing & Repository
  o Used by FS-ISAC Members, powered by Soltra Edge

• Coordinate exercises including Cyber Attack against Payment Systems (CAPS) simulations in Americas, EMEA, APAC

• Request for Information (RFI Program, US)
  o Fis can check anonymously with peers & others to get more info on anomalous behavior

• Additional training and exercise programs under development

• Initiated legal actions including multiple Botnet Takedowns (working with law enforcement)
• Microsoft detected around 500,000 infected machines, starting in 2014 and into 2015.
• FS-ISAC helped take legal action.
• Botnet servers seized in Germany, Italy, the Netherlands, the United Kingdom.
• Microsoft and Symantec released a remedy to clean and restore infected computers' defenses automatically.
• Other prior takedowns included: Shylock (2014), Citadel (2013)
New Paradigm in the Fight Against Cyber Crime

Criminal Action Only:
Continue to let criminals steal from customers while law enforcement builds cases against Eastern Europeans which are
1. difficult to prosecute,
2. obtain meaningful convictions, and
3. take months or years of investigation.

Civil and Criminal Action:
Disrupt criminals’ operations through civil action that
1. identifies the defendants quickly,
2. notifies the customers re: infected machines
3. provides remediation tools and,
4. still allows for prosecution of defendants through criminal action.
Automated Sharing: Soltra Edge®

- Soltra Edge® is a threat communications platform created by FS-ISAC and DTCC.
- The project was funded by CEOs at over a dozen FS-ISAC member firms.
- Edge is based on open standards including STIX (content standard) and TAXII (transport standard).
- Edge helps solve challenges including:
  - How to improve real-time information sharing within a community.
  - How to handle information overload.
  - How to do this at machine speed.

“Soltra Edge is truly created by users, for users, to enable real-time sharing.”

Richard K. Davis, CEO, U.S. Bancorp
Reducing Time from Awareness to Action

**Manual vs. Automated**

**Worst Case**

- **MANUAL**
  - 11 Hours
- **AUTOMATED**
  - 10 Minutes

**Best Case**

- **MANUAL**
  - 10 Minutes
- **AUTOMATED**
  - 1 Second

98% Time Reduction from Awareness to Course of Action

10,000x Triage capacity increase

TLP Green
Education & Tools

- Convene 4 Summits
  - Miami on May 1-4
  - Singapore on June 20-22
  - Nashville on October 24-26
  - Barcelona on Nov 7-9

- Over 20 Workshops & trainings

- In depth Cyber Threat Training courses

- Publish threat alerts (often w/ FBI/USSS)

- Provide mitigation strategies

- Create crisis management playbooks
Exercises Program

A Sector-wide, Sustainable All Hazards Exercise Program for the Financial Sector

- Support needs of large and small financial institutions covering cyber and physical threats
- Serve as nexus for financial sector, US Government, and cross sector coordination
- Coordinate exercises calendar to minimize conflicts and drive towards enhanced capabilities
- Advance exercising beyond “tabletop” model to enhance operational skills and capabilities
- Close out 2015 “Hamilton” series and other sector exercise action items
- Include Request for Technical Assistance (RTA) drills
- Build a library of vendors and their capabilities to assist in the development of the program
- Establish governance structure that incorporates key stakeholders (public and private)
- Expanding participants to include senior financial sector executives, including CEOs, CROs, COOs and CAOs.
- Engaging executives from other critical infrastructure sectors such as electrical power grid companies and telecommunications companies.
Looking Ahead

• Cyber risks not abating. Likely to be more complicated and challenging.

• Financial regulators are intensifying their focus on cyber.
  – Downside: creating more documentation work for organizations and less time for fixing problems
  – “Framework” fatigue

• Increasing government involvement
  – Examples include:
    • US Federal Reserve System leading payments modernization initiative
    • US President Obama has issued numerous executive orders resulting in NIST Cybersecurity Framework, increased government and private sector information sharing

• US “think tanks” and commissions preparing recommendations for policy officials

• International bodies striving to develop international cyber norms of behavior
Looking Ahead (cont’d)

• Expand and grow existing services:
  – Information Sharing and Analysis
  – Education and Tools
  – Conferences/Education/Training
  – Communications (e.g., monthly senior executive brief)
  – Automation/“Soltra”

• Increase response readiness
  – Exercises (e.g., senior leadership exercises, payments)
  – Cross-sector exercises planned
  – Enhanced crisis management response (e.g., all hazards crisis management playbook, media response)
  – Continue public-private partnerships

• Increased support for others sectors (e.g., retail, real estate, oil and natural gas, law firms)

• Increasing global presence - through international offices and more partnerships
Contact Information

John Carlson
Chief of Staff, FS-ISAC
Vice Chairman, FSSCC
jcarlson@fsisac.com

Ray Irving
Managing Director, Global Business Services
M: +41 76 303 50 70
rirving@fsisac.eu

Join online: https://www.fsisac.com/join
Email us: marketing@fsisac.us
Call us: 877-612-2622, prompt 3
Other information: www.fsisac.com