the Availability Digest

www.availabilitydigest.com

FS-ISAC: Financial Services - Information Sharing & Analysis Center

October 2012

FS-ISAC, the Financial Services – Information Sharing & Analysis Center (www.fsisac.com), is an industry forum for sharing critical security threats facing the financial services industry. FS-ISAC members receive timely notification and authoritative information for protecting their critical systems from physical and cyber attacks.

An example of FS-ISAC in action is reported in our accompanying article, Islamic Hacktivists Attack U.S. Banks.[1] Following initial intense Distributed Denial of Service (DDoS) attacks on some U.S. banks, FS-ISAC raised its cyber threat level from "elevated" to "high" as the attacks continued on other banks.

FS-ISAC was launched in 1999 in response to a presidential directive mandating that the public and private sectors share information about security threats to help protect critical U.S. infrastructure. It collects and authenticates timely information from financial services firms, commercial security firms, federal, state, and local government agencies, and other trusted sources. It also provides an anonymous information-sharing capability across the entire financial services industry.

FS-ISAC is owned by its 4,000 members. Members voluntarily and anonymously submit information to the FS-ISAC database for authentication and analysis. As information is received, it is verified; and the threat level is analyzed. Recommended actions are disseminated to the FS-ISAC membership via FS-ISAC's Critical Infrastructure Notification System (CINS) run by VeriSign.

Membership in FS-ISAC is recommended by the U.S. Department of Treasury, the Office of the Comptroller of Currency, the Department of Homeland Security (DHS), the United States Secret Service, and the Financial Services Sector Coordinating Council. Both Treasury and DHS rely on FS-ISAC to disseminate critical information to the financial services sector in time of crisis.

The FS-ISAC Scope

FS-ISAC is tasked with the following services:

- Utilize the financial sector's people, processes, and technology to aid the entire sector with situational awareness and advanced warning of new cyber and physical threats, incidents, and challenges.

- Provide an infrastructure that enables anonymity, if desired, and information dissemination via member and other trusted source submission.

[1] Islamic Hacktivists Attack U.S. Banks, *Availability Digest*; October 2012. http://www.availabilitydigest.com/public_articles/0710/bank_attacks.pdf

- Have a secure means to disseminate information when noteworthy events occur and evolve.

- Provide a 7x24 team of financial service industry analysts and security professionals to conduct intelligent gathering and research to alert members of evolving or existing threats, incidents, and vulnerabilities.

The FS-ISAC Mission Statement

The mission of FS-ISAC is to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and incidents and to serve as the primary communications channel for the sector. It supports the protection of the U.S. financial services sector by:

- identifying, prioritizing, and coordinating the protection of critical financial services, infrastructure, and key resources.

- facilitating the sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, and protective measures and practices.

The accomplishments of FS-ISAC's mission are achieved via the following strategies:

1. Provide an effective forum for information sharing within the financial services sector, with other Critical Infrastructure/ Key Resource (CI/KR) organizations, and with the U.S. government.

2. Through subject matter expert analysis, provide analysis and sector impact assessment feedback to the Financial Services Sector Coordinating Council (FSSCC) and the Financial and Banking Information Infrastructure Committee (FBIIC) on relevant threats, vulnerabilities and incidents.

3. Identify critical financial services sector operational support issues and requirements and articulate those to the Department of Treasury and the Department of Homeland Security.

4. Serve as the sector communications hub conveying timely and accurate cyber and physical threat information and vulnerability and incident alerts to its membership.

5. Serve as the sector communications hub during emergencies through the delivery of rapid notifications and communications to and among the FS-ISAC and FSSCC members.

6. Identify and implement new services that add value to the membership and support the mission of FS-ISAC.

7. Collaborate with Treasury and the FSSCC to:
   a. Foster awareness of the benefits of information sharing within the sector among other CI/KR organizations and with the government.
   b. Educate the financial services sector on key infrastructure protection issues, vulnerabilities, threats, risk management, and compliance issues.
   c. Coordinate with other public and private sector CI/KR organizations to ensure sector awareness and emergency preparedness.

Membership

Membership in FS-ISAC is open to any regulated financial institution and financial trade association in the United States and in many approved countries. FS-ISAC provides several levels of membership based on the size of the institution:

- Critical Notification Only Participants (CNOP) receive only urgent and critical crisis alerts via email. A CNOP participant is not considered a member.

- Basic Members receive urgent and critical crisis alerts via email and can submit anonymous or attributable information.

- Core Members ($1 to $10 billion in assets) receive the services applicable to Basic Members and, in addition, can access actionable alerts from partner and government member sources.

- Standard Members ($10 to $20 billion in assets) receive the services provided to Core Members. They can also participate in threat conference calls.

- Premier Members ($20 to $100 billion in assets) receive all the services provided to Standard Members and the ability to participate on FS-ISAC committees and work-groups. They can also attend annual meetings at no cost.

- Gold Members ($100 to $250 billion in assets) receive all the services provided to Premier Members and can attend some Board meetings.

- Platinum Members (more than $250 billion in assets) receive all the services provided to Gold Members and have other benefits for an additional fee.

The Cornerstones of FS-ISAC

The foundation upon which the FS-ISAC Board of Directors manages effective information sharing include:

- Submission Anonymity: The submitting member can have faith that its submission will not pose a competitive disadvantage and will be without attribution if it is submitted anonymously.

- Authenticated Sharing of Information: Recipients of alerts and information on events, incidents, vulnerabilities, resolutions, and solutions can be confident that the information is from an authorized and vetted source.

- Industry Owned and Operated: The database and all information is owned by the members and managed by a professional staff that reports to the member-elected Board of Directors

- No Freedom of Information Act Access: The control of the information by the private sector ensures that the information contained in the FS-ISAC database is not subject to requests from the press or others that are not members of FS-ISAC.

Criticality Classification of Submissions

Members classify their submissions into one of three levels of criticality:

- Crisis: The participant believes that the information is very critical to it and/or the financial services sector. This information will be posted to the FS-ISAC database, and members and CNOP participants will receive a Crisis Alert notification from FS-ISAC.

- Urgent: The participant believes that the information is important to other members and needs immediate attention. This information will be posted to the FS-ISAC database, and members and CNOP participants will receive an Urgent Alert notification from FS-ISAC.

- Normal: Information will be posted to the FS-ISAC database. Members will receive an Alert email notification.

Furthermore, information will be classified according to a *Traffic Light Protocol*:

- Red information is restricted to a defined group such as those present at a meeting.
- Amber information may be shared with other FS-ISAC members.
- Green information may be shared with FS-ISAC members and partners such as Treasury and DHS. It cannot be shared in public forums.
- White information may be shared freely.

Security Threat Levels

FS-ISAC maintains a Cyber Threat Advisory and a Physical Threat Advisory. The current threat of a cyber or physical attack is rated in order of severity level as Severe, High, Elevated, Guarded, or Low.

Other FS-ISAC Activities

FS-ISAC schedules several types of calls to allow members to coordinate with one another. These include:

- Bi-weekly Threat calls: IT security, physical security, and business resilience professionals discuss the latest threats against the financial services industry.
- Payment Processor Information Sharing Council (PPISC): These are monthly calls to allow card processors to share information about attacks.
- Payments Risk Council (PRC): These are monthly calls that allow ACH, wire and check operations, and risk management professionals to share information about attacks.
- Cyber Attack against Payment Processes (CAPP) Exercise: These are weekly planning calls to develop a three-day exercise to simulate attacks against the financial institutions, payment processors, and business users of online payment products.

FS-ISAC runs multiday spring and fall annual conferences and sponsors weekly webinars on a variety of security issues. It also publishes a monthly newsletter.

Summary

FS-ISAC has been operating out of the public view for over a decade protecting our financial services industry. It played a particularly important role in the recent DDoS attacks which disabled the online banking portals of many major banks, including Bank of America, JPMorgan Chase, U.S. Bank, Wells Fargo, PNC Bank, Capital One, SunTrust Banks, and Regions Financial.

Further information on FS-ISAC may be found in its document entitled “Financial Services Information Sharing & Analysis Center (FS-ISAC) Operating Rules.[2]

[2] Financial Services Information Sharing & Analysis Center (FS-ISAC) Operating Rules, *FS-ISAC White Paper*; March 14, 2011. http://www.fsisac.com/files/FS-ISAC_OperatingRules_2012.pdf