



NYU

Case Study: Cybersecurity in the U.S. Financial Services Sector (FSS)

By: Adalberto Trujillo, Krislyn Vara



In this Presentation

Here's what we'll cover:

- Core Background
- Partners Involved
- Partnership Risks
- Success & Failures
- Lessons Learned
- Looking Forward
- Questions to the audience

“The world’s financial system could collapse and create an economic downturn as disastrous as the coronavirus recession or the global financial crisis if growing fears of a devastating cyber-security hack are realized”

- Shane Wright, 2020

The Financial Services Sector (FSS)

The Financial Services Sector (FSS) is a designated Critical Infrastructure (CI)

- There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (Cybersecurity & Infrastructure Security Agency, CISA)
- **The Department of the Treasury** is designated as the Sector Risk Management Agency for the Financial Services Sector
- **Why is cybersecurity in the FSS so critical?**
 - Growing target - According to VMware, the first half of 2020 saw a 238% increase in cyber attacks targeting financial institutions.
 - The US FSS and its deep interconnectedness with the global economy means these consequences will not be confined to the United States
 - The average cost of a data breach in the financial sector in 2021 is \$5.72 million (IBM and the Ponemon Institute)
 - Digital Infrastructure and FinTech
 - The FSS is highly interconnected and many firms depend on the same systems for critical functions including payments clearing and settlement

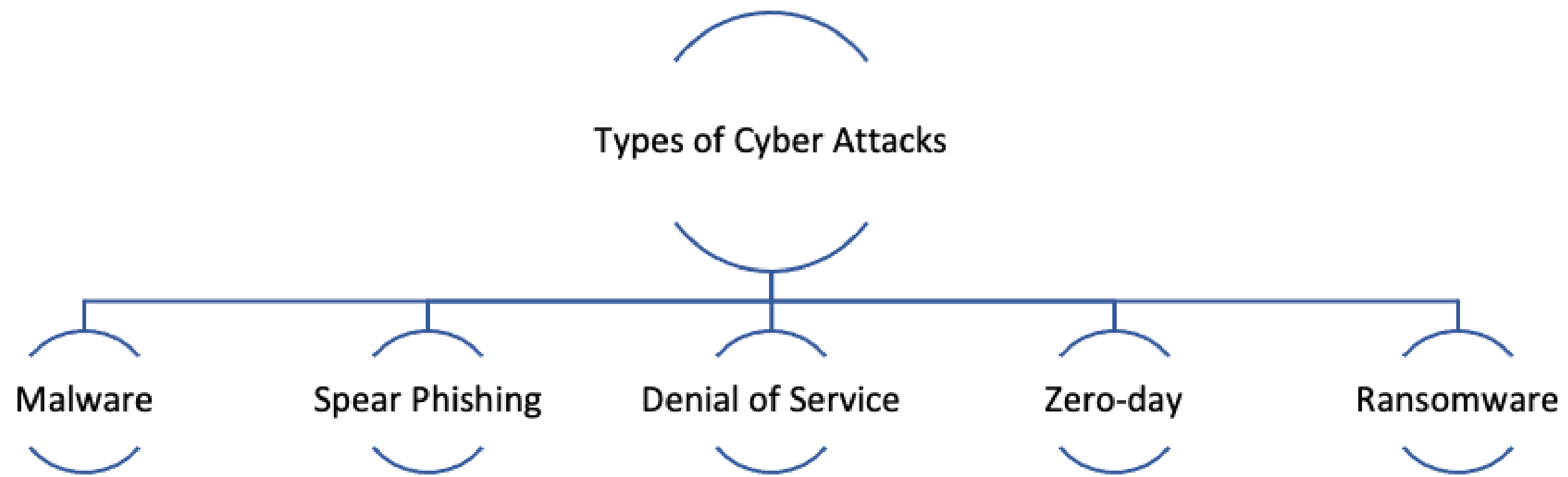


TABLE 1
Threat Actors: Motives, Impact, and Relevance

	Category	Actions	Real/Possible Impact	Frequency
	Nation-states	Monitor other nations' economies for espionage; conduct cyber-attacks in rare cases.	Loss of trust once breach is discovered; disruption to the financial sector.	Espionage—common Destruction—very rare
	Proxy Organizations	Steal information for espionage; possibly conduct destructive attacks.	Loss of trust once breach is discovered; disruption to the financial sector.	Espionage—common Destruction—very rare
	Cybercrime	Steal money from financial sector entities; at times stealing large sums	Affects organizations' profits; loss of trust if breach is publicized but org was silent	Theft—very common
	Hacktivist	Disrupt financial sector operations; attack the brand of individual institutions; data release individual/institutions.	Damaged reputation; loss of trust	Moderately common
	Insider	Steal money; get revenge through destruction or data release.	Affects organizations' profits; damaged reputation	Moderately rare

Critical Infrastructure Sector Partnerships

- Purpose: Partnerships create an environment to share critical threat information, risk mitigation, and other vital information and resources
- The Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) leads the coordinated national effort with public and private sector critical infrastructure partners
- National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience
- Critical Infrastructure Partnership Advisory Council (CIPAC)
- Partnership Structure
 - GCC
 - SCC
 - ISAC

FSS Coordinating Council Partners

The Financial Services Sector pursues a shared security and reliance mission:

"Continuously enhance security and resilience within the Financial Services Sector through a strong community of private companies, government agencies, and international partners that establishes shared awareness of threats and vulnerabilities, continuously enhances baseline security levels, and coordinates rapid response to and recovery from significant incidents as they occur."

GCC: Financial and Banking Information Infrastructure Committee (FBIIIC)

- The Financial and Banking Information Infrastructure Committee (FBIIIC) serves as the government-led member of the coordinating council.
 - Improving coordination and communication among financial regulators, promoting public-private partnerships within the financial sector, and enhancing the resiliency of the financial sector overall
- To fulfill its mission, the FBIIIC:
 - Establishes secure communications capability among the financial regulators and protocols for communicating during an emergency; and
 - Ensures that sufficient staff at each member agency has appropriate security clearances to handle classified information and to coordinate in an emergency
- Collaboration with the financial regulators and Federal Executive Branch agencies
 - Sharing information about cybersecurity and physical risks, supporting and leading incident response and investigation efforts, and developing and sharing best practice recommendations.
- The Sector-Specific Agency: The Department of Treasury

Government Coordinating Council

- American Council of State Savings Supervisors
- Board of Governors of the Federal Reserve System
- Conference of State Bank Supervisors
- Consumer Financial Protection Bureau
- Farm Credit Administration
- Federal Deposit Insurance Corporation
- Federal Housing Finance Agency
- Federal Reserve Bank of Chicago
- Federal Reserve Bank of New York
- National Association of Insurance Commissioners
- National Association of State Credit Union Supervisors
- National Credit Union Administration
- North American Securities Administrators Association
- Securities Investor Protection Corporation
- U.S. Commodity Futures Trading Commission
- U.S. Department of the Treasury
- U.S. Office of the Comptroller of the Currency
- U.S. Securities and Exchange Commission

SCC: Financial and Banking Information Infrastructure Committee (FSSCC)

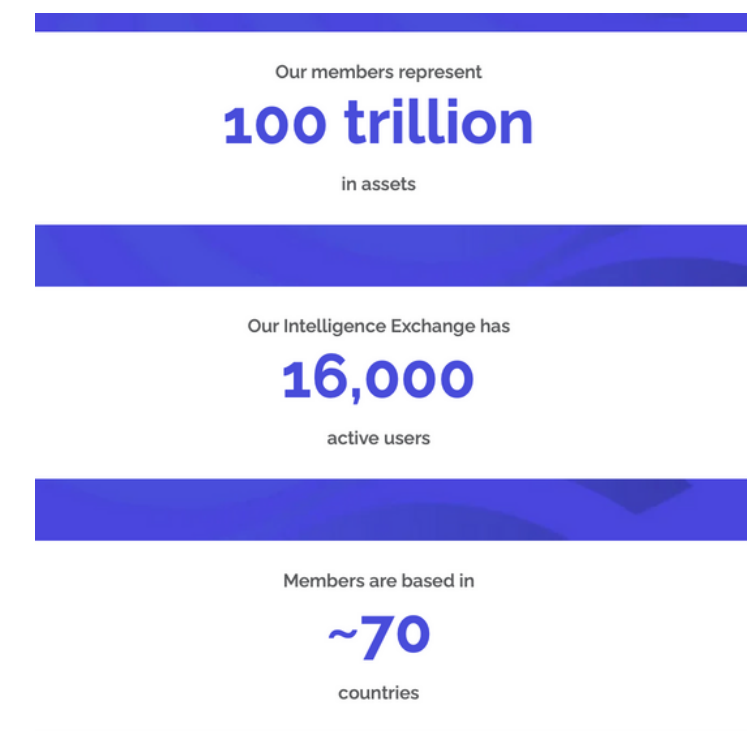
- The FSSCC serves as the Sector Coordinating Council for the Financial Services Sector
- The FSSCC partners with the public sector to promote security and resilience of the FSS through information sharing, incident response, and recovery efforts, and by promoting best practices and the development of effective policies
- Its 70+ members consist of financial trade associations, financial utilities, and the most critical financial firms

Sector Coordinating Council

- AIG
- Ally Bank
- American Bankers Association
- American Council of Life Insurers (ACLI)
- American Express
- American Property Casualty Insurance Association
- ARC Group
- Bank of America
- BNY Mellon
- Bank Policy Institute (BPI)
- BMO
- Capital One
- Charles Schwab Bank
- ChicagoFIRST
- Citi
- CLS Bank
- Comerica
- CME Group
- Credit Suisse
- Credit Union National Association (CUNA)
- Cross River Bank
- Depository Trust & Clearing Corporation, The (DTCC)
- Fannie Mae
- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Goldman Sachs
- Independent Community Bankers of America (ICBA)
- Institute of International Bankers
- Intercontinental Exchange (ICE) / (NYSE)
- JPMorgan Chase
- MasterCard
- Morgan Stanley
- MUFG
- NACHA - The Electronic Payments Association
- National Association of Federal Credit Unions (NAFCU)
- National Futures Association
- Navient
- Northern Trust
- Options Clearing Corporation
- PNC
- Prudential
- Queensborough National Bank & Trust Company (QNBT)
- Raymond James Financial, Inc
- Securities Industry Financial Markets Association (SIFMA)
- SPARK Institute
- State Farm
- State Street Corporation
- TD Bank
- Truist
- UBS
- USAA
- U.S. Bank
- Wells Fargo

Information Sharing: FS-ISAC & FSARC

- The Financial Services Information Sharing and Analysis Center (FS-ISAC) serves as the operational arm of the FSSCC
 - FS-ISAC correlates and analyzes information and collaborates with partners to develop joint reports on threat intelligence, best practices, and mitigation strategies
 - The FS-ISAC is able to identify physical and cybersecurity threat levels to keep the sector informed and prepared
- The ARC is a non-profit, cross-sector organization designed to mitigate systemic risk to the nation's most critical infrastructure from existing and emerging threats
 - The Financial Systemic Analysis & Resilience Center (FSARC) was created by a consortium of financial services firms, to help identify potential risks for financial systems
 - Creators: Bank of America, BNY Mellon, Citi, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street Corp., and Wells Fargo
- FSARC membership is limited mainly to the largest banks
- In comparison to FS-ISAC, the FSARC provides a venue where firms can have systemic-level conversations about state-sponsored threats and through these conversations they have the “ability to translate that information into action”
 - Project Indigo





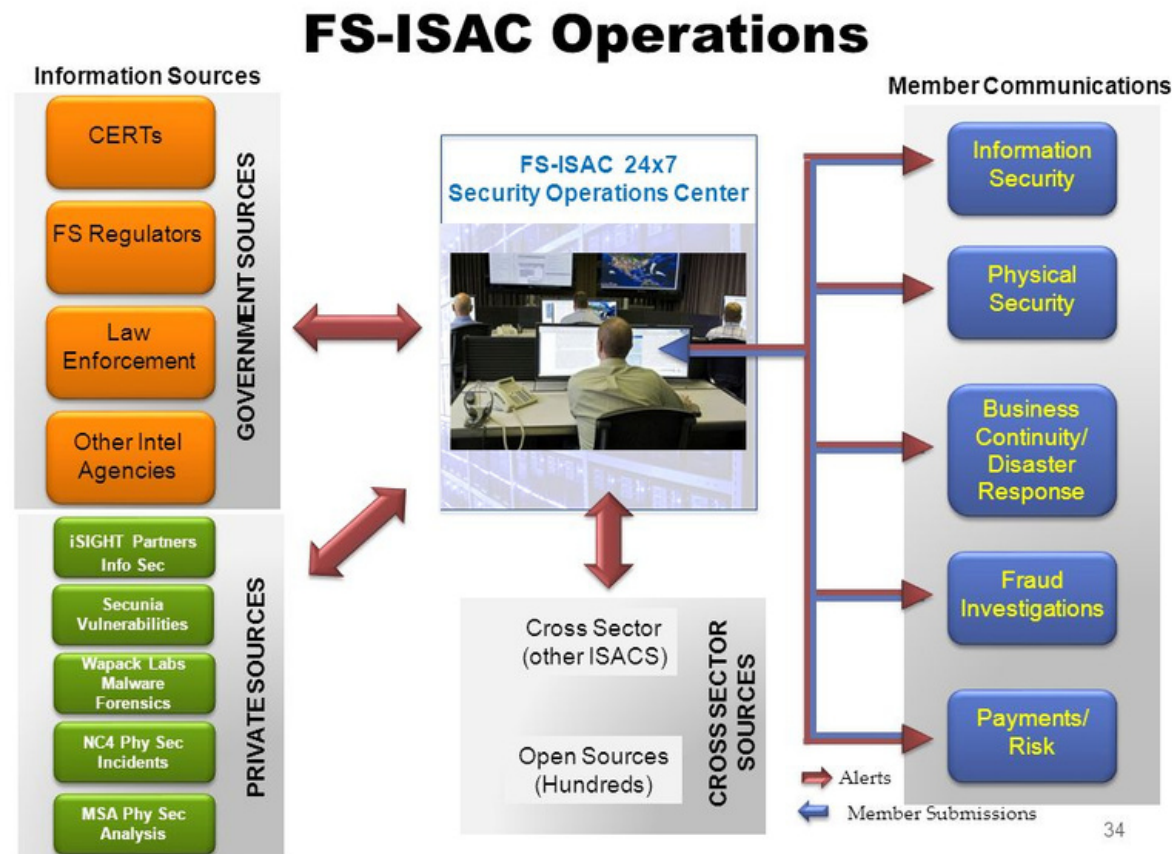
Annual Dues

Annual dues are determined based on your firm's exposure, informed by criteria such as assets, revenue, assets under management, and clearing customers.

Eligibility

Financial firms of the following types are eligible for membership:

- Bank & Credit Union
- Core Back Office Supplier
- Critical Utility
- Exchange
- Fintech
- Insurance
- Investments & Securities
- MSSP
- Payments
- Trade Association



34



Inside 'Project Indigo,' the quiet info-sharing program between banks and U.S. Cyber Command

The broad purpose of Project Indigo is to help inform U.S. Cyber Command about nation-state hacking aimed at banks. In practice, this intelligence is independently evaluated and, if appropriate, Cyber Command responds under its own unique authorities.

Partnership Risks

Partnership Risks

- **Government Risks:**
 - Government agencies are reluctant to share classified information about threats with a large number of individuals.
- **Private Sector Risks:**
 - Private sector firms are reticent about sharing information with the government that could lead to audits from regulators.
 - Most FSS firms are market competitors and are hesitant in sharing information.
- **Industry-run, not-for-profit entity risk:**
 - FSARC affiliated banks risk their reputation if the partnership doesn't work out



Success & Failures

Without FSS Partnerships

Weak and uncoordinated regulatory approach with limited information sharing with the government, no operational coordination and moderate information sharing with the industry

Regulation and audits were focused on the traditional classic checklist-based style compliance approach, preventing firms from focusing on the big cybersecurity picture of the most important threats

With FSS Partnerships

Strong investment and collaboration within the industry and government

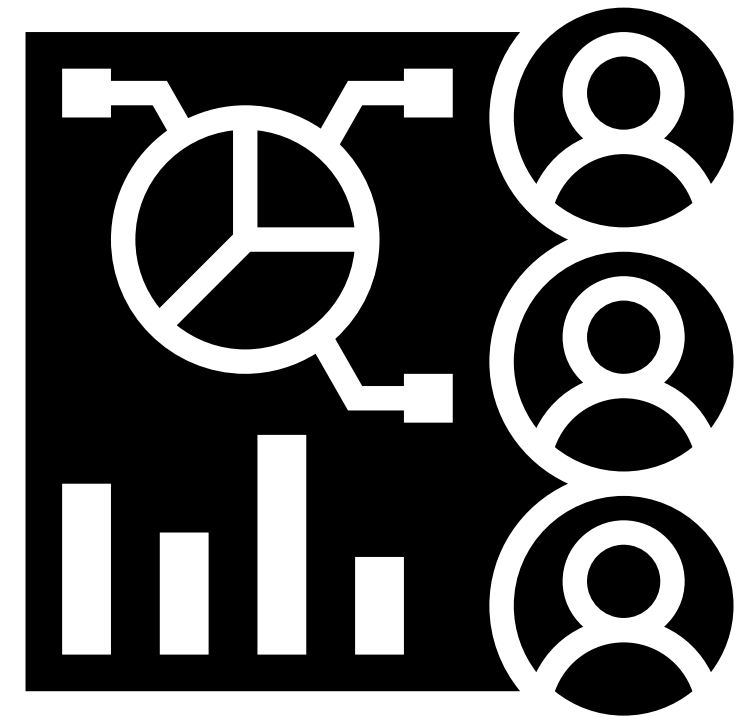
Effective regulatory relationships led to forcing firms to adopt standards by highlighting the potential liability that firms might face if cybersecurity was neglected

Significant improvement in information sharing with industry, largest firms, and governmental operational coordination (FSARC)

Lessons Learned

Lessons Learned From Financial Services Sector

- **Government:**
 - Must ensure regulatory and collaborative approaches work well where trust among all parties is essential to success.
- **Private Sector:**
 - Addressing cross-sector threats in a growing interdependence of sectors on one another, directly or through the internet is key to success.
 - Build trust with the government
- **Industry-run, not-for-profit entity:**
 - The importance of industry-wide awareness is critical when faced with nation-state threats.
 - Leads to a coordinated sector-wide response to state-run cyber operations.



“If you are protecting everything, you are protecting nothing”

- Clint Mixon, Deputy Chief of Strategy, NYC3

Call For Actions: Recommendations



- Refining the quantity and quality of information sharing across the sector can help better understand the threat landscape being targetted in the Financial Services Sector (FSS)
- Expanding investigations in other countries might reveal other FSS factors at work and a degree of systematic risk
- Continue to drive and shape the FSS efforts as it turns attention to areas of improvement for government and industry leaders; this includes:
 - Information sharing that provides a more timely and actionable awareness of the threat landscape
 - Improving operational coordination within the FSS sector, government entities, and operational partnerships with the largest firms and critical infrastructure sectors that the FSS relies on.

Call For Actions: Recommendations



International Wide Partnership

- Establish an international wide partnership with G20 governments to build a cybersecurity capacity building for the Financial Services Sector (FSS):
 - It will consist of global central banks and will be managed by The International Monetary Fund (IMF)
 - Promote strong collaboration to better protect global financial systems and infrastructure from cybercriminals
 - The international wide partnership will deal with intercepting and preventing cybercriminals from using global financial systems and services to fund their organization and illegal operations

Q&A

Q&A

1. *TRIVIA* Can anyone identify the other 15 Critical Infrastructure Sectors?
2. Can you identify any other critical infrastructure sectors that have the same cybersecurity risk profile as the Financial Services Sector?
3. Do you think it's beneficial for the private sector and public sector to help underdeveloped countries strengthen their cybersecurity posture within the Financial Services Sector?