



**“Mobilizing Our Cyber Defenses:
Securing Critical Infrastructure Against Russian Cyber Threats”**

Testimony of Steven Silberstein, Chief Executive Officer
Financial Services Information Sharing and Analysis Center

Before the

United States House of Representatives
Committee on Homeland Security

March 30, 2022

Chairman Thompson, Ranking Member Katko and Honorable Members of the Committee, thank you for the opportunity to testify at this hearing on “Mobilizing Our Cyber Defenses: Securing Critical Infrastructure Against Russian Cyber Threats.” I am Steven Silberstein, CEO of the Financial Services Information Sharing and Analysis Center, or FS-ISAC.

My statement will illustrate how the strong and effective partnership between the financial sector and the federal government enhances the resilience of this critical sector not only generally, but also specifically with respect to the current geopolitical situation. You should know up front that the sector is well-situated to navigate the current threat environment, but remains highly vigilant, not knowing what may come next. Before sharing these details, I would like to explain the role of the FS-ISAC within the financial sector.

The Role of the FS-ISAC

The FS-ISAC exists to foster the resilience and continuity of the global financial services infrastructure, individual financial institutions and, of course, customers, against acts that could significantly disrupt the sector’s ability to provide services critical to the orderly functioning of the economy. As such, FS-ISAC stands front and center in the face of continued cyberattacks against financial institutions.

The financial sector formed the very first ISAC in 1999 in response to Presidential Decision Directive 63, which in 1998 called for the private sector to establish ISACs and for the public and private sectors to collaborate to protect critical infrastructure from cyber threats and attacks. A private, nonprofit association, the FS-ISAC represents nearly 5,000 financial institution members in nearly 70 countries that, together, have nearly \$100 trillion under management.

Members include commercial banks, credit unions, exchanges, clearing houses, brokerages and investment companies, insurance companies, payments processors, and financial trade associations. Headquartered in Reston, Virginia, we manage this critical network with more than 100 people situated in about 10 countries. The FS-ISAC is the only global cyber intelligence sharing community solely focused on the financial sector, allowing it to take a “follow-the-sun” approach, with staff continuously working with the members.

It might surprise the Committee to learn that a highly competitive industry like financial services can be very collaborative when it comes to cybersecurity. It makes sense, though, because cyber criminals try to

target as many victims as possible with the same attack. In that way they earn a better return on their nefarious investment. Moreover, given the sector's reliance on public trust, an attack on one bank could damage the trust of customers of other banks, a dangerous situation for the financial sector and the public at large.

Thus, if one firm notices that its systems are being targeted, it will share that information with its peers through the FS-ISAC, empowering other members to prepare for and defend against that attack before it happens to them. Our thousands of member financial institutions report cyber activity daily on our secure platform. In turn, our global intelligence team reviews, processes, and analyzes the intelligence and provides members with alerts, updates, and briefings—such as the attached report on cyber challenges in 2022. In addition to the daily intake and dissemination of current threats, we conduct regular threat calls to provide more details and context and provide members with a secure chat capability. There is a wide variety of channels, based on charter—like banking or insurance—geography, incidents, and current issues like the Russian/Ukraine situation. Unlike individual firms, we can see how many institutions experience the same type of threat or attack, allowing us to gauge across the sector its seriousness and sophistication.

We publish executive level reports to arm boards and leadership with a high-level understanding of the cyber threat landscape so they can make strategic business decisions about investing in cybersecurity and resource allocation. Not only does the FS-ISAC monitor intelligence and cyber threats, but it also conducts exercises that simulate attack scenarios based on the current threats. This allows members to practice how they would respond and develop a plan in the event of an incident.

A recent example may illustrate how these capabilities combine to improve resilience. In 2021, the New Zealand Stock exchange was the target of a distributed denial-of-service (DDoS) attack. Such an attack intends to clog a network so as to crash a website or system. This event was part of a wave of DDoS attacks that affected more than 100 financial institutions globally. It is not an exaggeration to say thousands of institutions could have been attacked if not for the intelligence sharing on FS-ISAC's platform, which enabled financial institutions to share critical information needed for members to shore up their defenses to prevent the attack from expanding.

Two important nonprofit subsidiaries of FS-ISAC deserve mention—Sheltered Harbor and the Financial Data Exchange (FDX). Sheltered Harbor protects public confidence in the financial sector if a devastating event like a cyber-attack causes an institution's critical systems and its backups to fail. FDX seeks to unify the financial sector around a common, interoperable and royalty-free standard for the secure access of user-permissioned financial data. Background documents on both nonprofits are attached.

Financial Sector Collaboration

Of course, the FS-ISAC does not perform this role in isolation. On the contrary, the financial sector boasts a history and depth of collaboration among competitors and between it and government that bolsters resilience and ultimately serves the needs and interests of its customers.

Ahead of the Year 2000 Rollover, for example, financial institutions voluntarily graded their readiness and shared scores with regulators on a global basis. This incentivized the entire sector to be prepared. Following 9/11, the financial sector decided to coordinate to enhance its readiness and to more effectively collaborate with the government, forming the Financial Services Sector Coordinating Council (FSSCC) in 2002. This closely followed federal and state financial regulators, which, led by the U.S. Department of the Treasury, formed the Financial and Banking Information Infrastructure Committee (FBIIC) earlier in 2002. More information about FBIIC may be found at fbiic.gov. The financial sector effectively

established its own government and sector coordinating councils well before the creation of the U.S. Department of Homeland Security, illustrating its commitment to partnership, as well as its ability to innovate, to be ahead of the curve on matters like the protection of its own critical infrastructure.

The FSSCC is comprised of the sector's key organizations, through which nearly the entire sector is represented, including the American Bankers Association; the Bank Policy Institute (BPI) and BITS, its technology policy division; the Securities Industry and Financial Markets Association (SIFMA); the Analysis and Resilience Center for Systemic Risk (ARC); the Independent Community Bankers of America and the FS-ISAC. I would like to recognize the current FSSCC Chair and Vice Chair (respectively) for their leadership and partnership: Ron Green, Chief Security Officer of Mastercard; and Chris Feeny, Executive Vice President at BPI and President of BITS. An overview of FSSCC is attached and a full list of members can be found at fsscc.org.

During FSSCC's 20 years, the FS-ISAC evolved into the operational arm of FSSCC, complementing FSSCC's role as the policy arm on critical infrastructure protection matters. The FS-ISAC developed a playbook that outlines how it responds to cyber threats and incidents on a daily basis. It includes a section developed in coordination with FSSCC, SIFMA, and FBIIC that lays out a process for these four sector organizations to come together, if necessary, in response to a significant incident—forming the Core Executive Response Group (CERG), to ensure information is distributed as appropriate across the sector.

The CERG proved valuable during the early phases of COVID-19. As we watched the virus spread at the end of 2019 and beginning of 2020, we recognized the need for the sector, public and private, to discuss how we should respond to it and share ideas for protecting financial institutions and customers alike by keeping critical infrastructure operating. FS-ISAC called together the CERG on January 30, 2020, ahead of most alarm bells going off in the U.S., to be prepared if the inevitable occurred. The CERG participants met for nearly 18 months, sharing information about the virus, addressing common challenges and sharing effective practices for operating in the face of it. During this time, we also tackled SolarWinds, a Microsoft Exchange vulnerability and other incidents that arose while still managing the effects of the COVID-19 pandemic.

Though largely unknown, this CERG experience exemplifies the success of the public/private partnership within the financial sector. Leadership from the Treasury Department and the Cybersecurity and Infrastructure Security Agency (CISA), along with federal and state regulators, met regularly—often multiple times per week—with their counterparts from FS-ISAC, financial trade associations and key financial firms to ensure customers could continue to receive financial products and services through the challenging early phases of the pandemic.

Our sector collaboration also extends beyond the financial sector itself. We are members of the National Council of ISACs, sharing information regularly with other member ISACs, particularly during critical events and incidents. Given financial sector reliance on telecommunications and electricity, FSSCC and FS-ISAC led the development of a tri-sector playbook in 2018. The three sectors exercised the playbook prior to the pandemic and regularly used it during the pandemic to ensure information flowed freely among these three sectors.

The sector's collaboration with the Treasury Department, as our Sector Risk Management Agency (SMRA), constitutes another important component of the partnership. The Treasury Department helps ensure that CISA receives accurate, comprehensive information about current sector operations and any potential incidents. Moreover, the Treasury Department coordinates with the sector and CISA to identify sector risks and then assess and mitigate them through, for example, informing National Critical Functions, conducting regular exercises to test preparedness and emergency planning. The value of the Treasury Department's SRMA role came to the fore ahead of the current geopolitical crisis, which I will address shortly.

I have elaborated at length on the partnerships within the financial sector, because we responded to the crisis of the moment within this context. The FS-ISAC knows well how to promote the resilience of our members, and we do so in conjunction with our financial sector partners, public and private, in a familiar, trusted and effective fashion. As such, the effective role played by our public sector partners must be acknowledged.

Current Collaboration with the U.S. Government

We applaud the Biden-Harris Administration and its various federal government components on the expeditious and early sharing of information throughout the escalating geopolitical situation in Eastern Europe and current Russian invasion of Ukraine. The sector appreciated the paradigm shift from reactive to proactive warnings forecasting Russian military action, the potential for Russia to engage in malicious cyber activity against the U.S. and evolving intelligence that Russia may be exploring options for potential cyberattacks. The repeated, consistent messaging and realistic context provided by CISA, the Federal Bureau of Investigations (FBI), the Treasury Department and other government organizations allowed our sector to prepare for and institute the necessary security precautions, motivating institutions to conduct expeditious reviews of their incident response and regional personnel evacuation plans.

This early and continued sharing of indicators of compromise (IOCs) and warnings by CISA and the Treasury Department prompted the financial sector to open emergency communications channels prior to the 2021 holiday season and activate the sector's CERG on December 15, 2021. On this recurring call, government leadership, including the Treasury Department, CISA, and government regulators, provides updates on emerging vulnerabilities and associated mitigations, as well as current sanctions announcements, and facilitates the regular exchange of preparation activities taken by the sector.

As part of its role as the national coordinator for critical infrastructure security and resilience, CISA has actively engaged with its government and industry partners, including our SRMA, to share classified and unclassified information. The rapid declassification and passage of IOCs and malicious internet protocol (IP) addresses to the sector by the federal government is commended. Financial sector representatives have participated in several broad cross-sector information calls, as well as monthly unclassified and classified briefs hosted by the Treasury Department. There are also weekly intelligence collaboration sessions with the Treasury Department and ARC member firms.

Additionally, the establishment of CISA's "Shields-Up" web page, available at [cisa.gov](https://www.cisa.gov), has proven to be a great awareness tool for critical infrastructure organizations—and the business community as a whole—housing in one place the latest technical products and security guidance and steps organizations, businesses and individuals can take to heighten their security posture and ensure they are prepared for a disruptive cyber incident. In addition to the various alerts, advisories, and insight products, CISA also established a catalog of free services from government partners, the open-source community, and its Joint Cyber Defense Collaborative (JCDC) members to assist with the challenge of identifying resources to address urgent security issues. My organization, as well as our sector's trade associations and other partners, have consistently amplified these information products and resources to thousands of organizations around the country.

Operationally, the FS-ISAC, along with other representatives of the financial services sector, have engaged directly with CISA and the Treasury Department via a dedicated JCDC communications channel to foster near real-time information sharing. The JCDC brings together public and private partners to begin to unify defensive actions and drive down risk in advance of cyber incidents occurring and help strengthen the nation's cyber defenses through planning, preparation, and information sharing. This direct

engagement within the JCDC has also allowed the FS-ISAC analysts to provide sector specific insights and review technical exchanges for sector implications that can then be distributed to the sector at large.

Let me now turn to the current cyber threat and the manner in which the financial sector is handling it.

State of the Sector

As I write this statement, the financial sector has not experienced an increased level of cyberattacks coming from Russia. Of course, we are always tracking “background noise” in terms of low-level cyberattacks, mostly from threat actors scanning for vulnerabilities. However, outside of the conflict zone, we are not seeing any significant uptick in attacks attributable to any specific geography or threat actor. I reiterate that this assessment holds true as I prepare to deliver this statement to the Committee, but we are always on the watch in the event this changes.

Over the last 100 days, the financial sector has taken various precautionary steps to not only ensure our individual organizations, but also the sector as a whole, is as prepared as it can be at this point. As described previously, the sector’s various coordination and information sharing elements have amplified the Administration’s warnings and cyber alerts/advisories to thousands of entities around the world, as well as participated in an assorted array of unclassified and classified stakeholder engagement opportunities. Our recurring CERG calls with leaders from across the sector have ensured we will be aware of any change in the security of the financial system.

Currently, the FS-ISAC Cyber Threat Level (CTL), a barometer of the cyber threat landscape as collectively determined by our member financial firms, is elevated. Elevated is the second level of four levels on the scale; the CTL has not been raised to high or severe, for the reasons noted previously. This means that the financial sector is in a state of heightened cybersecurity awareness and is taking extra steps to strengthen cyber defenses. There is heightened awareness and diligence across most of the globe, given that the adversary is well- practiced and -armed on the cyber side. However, the cybersecurity measures highlighted last week by the Administration are critical baseline practices and should always be implemented to increase preparedness and operational resilience.

Financial institutions, and banks in particular, have always had to protect themselves. Long before cyber threats existed, criminals like Willie Sutton targeted banks because “that was where the money was.” Criminals have since evolved, using sophisticated tools to attack financial institutions, and some nation states have followed suit. Fortunately, the sector’s ability to thwart such attacks has evolved in tandem, and the financial system remains attentive to and is well-prepared to defend against potential sophisticated Russian cyber-attacks.

The FS-ISAC and other sector organizations have been raising the level of cyber resilience within the sector for more than 20 years. Working with thousands of financial firms around the world, we know the tactics, techniques, and procedures used by Russian state and non-state actors up until now. Given that, our members have been preparing to defend themselves by securing networks and servers, ensuring data is properly backed up, patching vulnerabilities, reducing access to systems to the absolute minimum, exercising to practice how to respond in various scenarios, and, of course, heightening vigilance across the board. The financial sector recognizes that preparation is the most important component, as targets do not receive the same type of “heads up” warning with cyber incidents as in a kinetic war. Our organizations always need to be prepared.

Improving Public/Private Collaboration

The public/private partnership is not simply alive and well; it thrives within the financial sector. I cannot speak more highly of the value provided by the Treasury Department, CISA, FBIIC, FBI and U.S. Secret Service to the cause of enhancing resilience. All are to be commended for their contributions. Of course, as in any endeavor, improvements can always be made. To that end, I offer two brief items for enhancing collaboration.

- The Treasury Department and CISA have recently increased the amount of information shared with the sector, and I applaud them for it. With respect to both classified and unclassified information, we encourage this trend to continue and increase, for the greater protection of the sector.
- The highly regulated and global financial sector faces a variety of incident reporting requirements. We urge collaboration to minimize the operational impact of multiple incident reporting requirements unique to the financial sector.

These suggested improvements do not detract from the productive partnership that serves the financial sector and its customers so very well. The sector's secure posture in the light of Russian cyber threats testifies, in no small part, to that partnership.

Conclusion

In closing, I wish to reiterate that the financial sector is currently secure but remains highly vigilant. That we have not yet seen the attacks anticipated does not mean they will not come. If they do, the sector will be prepared. The FS-ISAC and our fellow sector organizations stand ready to work with the Administration, Congress and this Committee in any way we can to protect the financial sector, its customers and economic security. Please do not hesitate to call upon us.

Thank you again for the opportunity to testify before you today. I am happy to answer any questions Members of the Committee may have.

Attachments:

- FS-ISAC Annual Global Intelligence Office Report, "*Navigating Cyber 2022*" (March 2022)
- Financial Services Sector Coordinating Council (FSSCC) Overview
- Sheltered Harbor Overview
- Financial Data Exchange (FDX) Overview



Navigating Cyber 2022

**Annual Cyber Threat
Review and Predictions**



About This Report

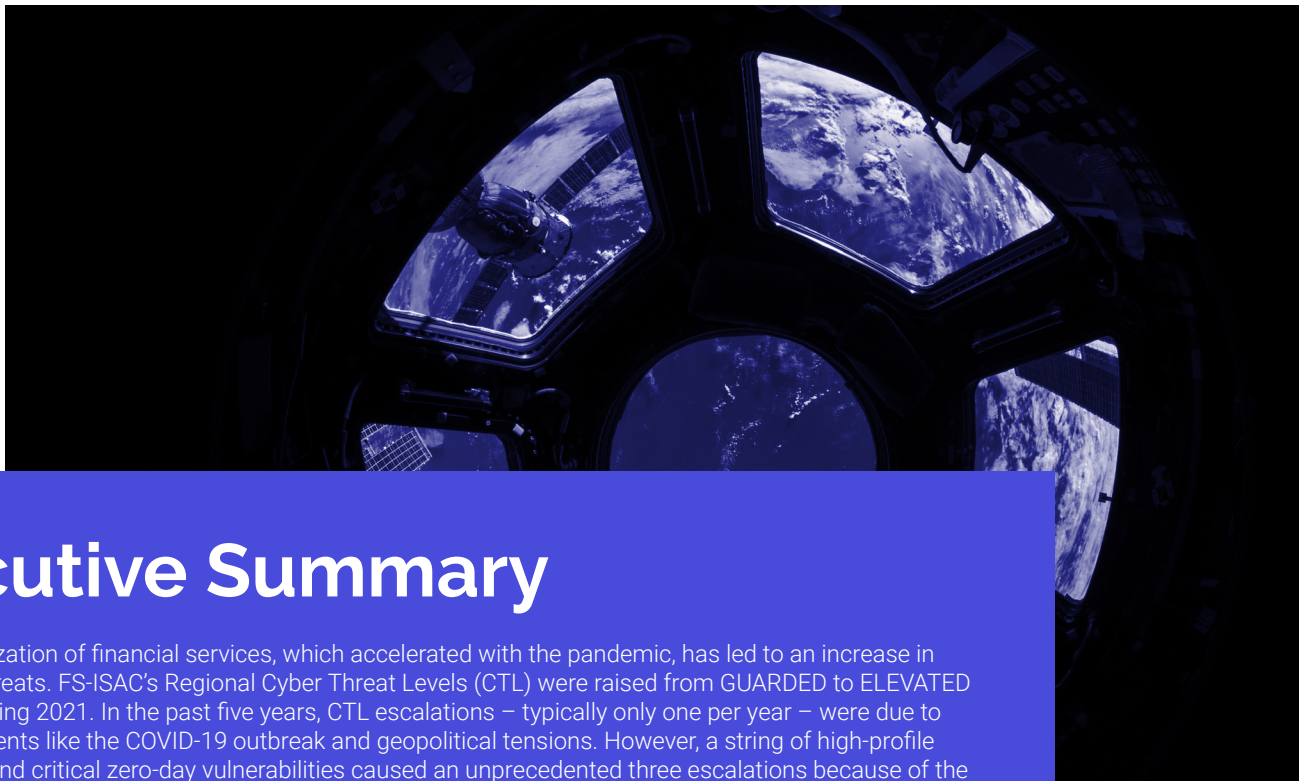
This is a thematic summary of the FS-ISAC Global Intelligence Office's in-depth report of cyber trends in 2021 and predictions for 2022.

The full report is only available to member financial institutions via the *FS-ISAC Intelligence Exchange*.

FS-ISAC membership is **exclusive** to financial institutions headquartered in eligible countries. FS-ISAC's full suite of intelligence products is solely available to members who are **directly** connected to *FS-ISAC Intelligence Exchange*.

As cybersecurity becomes a more pressing issue, the quality of cyber intelligence you receive is paramount. FS-ISAC is the only global cyber intelligence sharing community solely focused on financial services. Make sure you get your cyber intelligence from reputable sources.

If your financial institution is not yet a member of FS-ISAC, apply to become a member [here](#).



Executive Summary

The rapid digitization of financial services, which accelerated with the pandemic, has led to an increase in global cyber threats. FS-ISAC's Regional Cyber Threat Levels (CTL) were raised from GUARDED to ELEVATED three times during 2021. In the past five years, CTL escalations – typically only one per year – were due to major world events like the COVID-19 outbreak and geopolitical tensions. However, a string of high-profile cyber attacks and critical zero-day vulnerabilities caused an unprecedented three escalations because of the ubiquity of the affected parties within the financial sector's supply chain.

Third-party attacks pose significant risks to the financial industry due to our reliance on a myriad of providers and suppliers. Financial institutions typically enjoy a higher security posture than other sectors, with more mature cybersecurity and intelligence programs. Truly impactful cybersecurity incidents within the sector are therefore relatively rare. However, several high-profile third-party incidents have impacted the security and availability of products and services used by many financial firms, with resulting resources expended on assessing exposure, patching, and additional mitigations, as well as increased compliance mandates for third-party operational resilience.

Zero-day vulnerability exploits are increasing due to the increasing attack surface caused by digitization of the sector. The other key factor is the diversification of the kill chain, where criminals specialize in different stages of cyber crime – such as selling malware, access, code, and tech support. It is easy to simply buy (or sell) access to vulnerabilities without needing to know how to find them, resulting in a flourishing market.

Ransomware has effectively become a game of whack-a-mole, where operators shut down when they feel the heat of law enforcement, only to re-open under new names months later. With safe havens such as Russia making it difficult to find the masterminds, global law enforcement often can only apprehend affiliated individuals who participate in the ransomware chain but are not necessarily pivotal to its operations. Cyber criminals increasingly collaborate with each other, and even with nation-state actors when interests align. Merging, mingling, and rebranding to dissociate from past endeavors is a familiar behavior in the business world, and now a key trend in cybercrime as well.

Many of the major incidents over the past year have elements of all three of these trends, with third-party suppliers as the attack surface, zero-day vulnerabilities the key infection vector, and ransomware the end threat; i.e. a zero-day vulnerability of a third-party provider is exploited and used to deploy ransomware.

These high-level trends translate into increased cyber activity for the sector on a daily basis. Member financial firms around the world reported high levels of social engineering such as phishing and business email compromise (the entry point for most attacks), the persistence of some of the most notorious malware strains often used to drop ransomware, and a new level of scale and sophistication of distributed denial of service (DDoS) attacks, resulting in lack of availability of third-party services.

We anticipate that all of these trends will continue, and even increase in 2022. In addition, firms will have to contend with more nation-state cyber activity, including involvement in products and services widely used by the sector.



Cyber Snapshot 2021 Timeline

- Third-Party Risk
- Zero-Day Vulnerabilities
- Ransomware

January

SolarWinds

In December 2020, security vendor FireEye [disclosed](#) that it had been the victim of a breach. Further investigation revealed a widespread supply chain attack leveraging weaponized updates for the Orion product suite from software provider SolarWinds, compromising up to 18,000 organizations, including Fortune 500 companies and US government agencies. Later investigation revealed that fewer than 100 customers were hacked.

FS-ISAC Member Survey

April 2021



February

Accellion

Accellion Inc. reported a security incident related to its legacy File Transfer Appliance (FTA) software; a 20-year-old product that specialized in secure large file transfers. While the vulnerability had already been exploited, once publicly disclosed it was subsequently used by several threat actors to compromise multiple organizations, such as [The Reserve Bank of New Zealand](#), [Singapore Telecommunications](#), and [Qualys](#). Some members are still feeling repercussions.

February

Microsoft Vulnerabilities

FS-ISAC Member Survey



Microsoft [reported](#) that nation-state adversary HAFNIUM operating out of China used multiple zero-day exploits to attack on-premise versions of Microsoft Exchange Server. This allowed them to access email accounts and install malware to exfiltrate copies of the Active Directory database, dump credentials, add user accounts, and move laterally to additional systems and environments. Signs of compromise were later discovered to date back as far as September 2020. After the announcement, additional actors were reported to take advantage of the vulnerabilities.

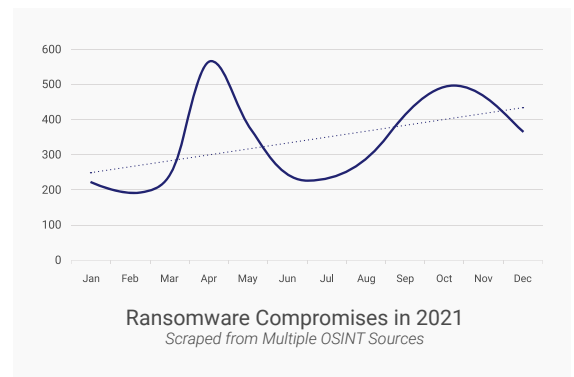
May

Colonial Pipeline

Consistently a top threat to the financial sector, ransomware infrastructure and operators experienced new levels of notoriety after the Colonial Pipeline attack. Government-related responses caused major shifts in ransomware operations but did not stop them.

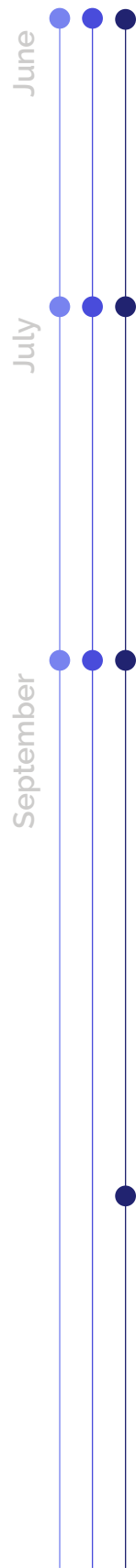
Member submissions of ransomware-related security events increased in the second half of 2021, including mentions on ransomware leak websites that offer exfiltrated data from the victim company.

Available data indicates the financial sector is less prone to successful ransomware attacks due to its increased security awareness and posture. However, the supply chain remains a key attack vector.





- Third-Party Risk
- Zero-Day Vulnerabilities
- Ransomware



Microsoft Vulnerabilities

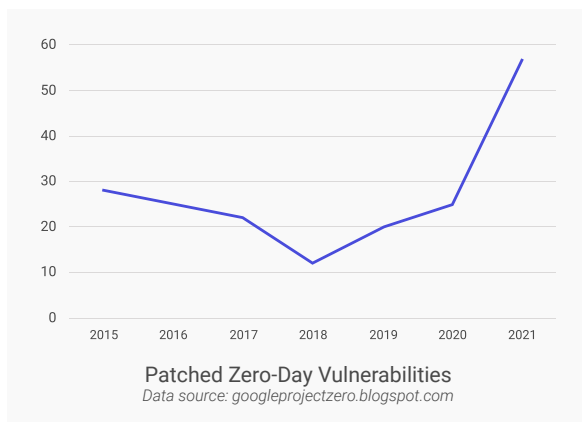
Two remote code execution vulnerabilities (one dubbed PrintNightmare) were [discovered](#) in the Windows Print Spooler service, enabled by default on all Windows servers and clients, that could allow an attacker to run arbitrary code with system-level privileges. Despite a number of patches released by Microsoft and wide-spread mitigation advice based on cyber hygiene principles, in August ransomware gangs Magniber and Vice Society were discovered to be actively leveraging PrintNightmare vulnerabilities to target Windows servers to deploy their payloads.

Kaseya

In July 2021, notorious ransomware gang REvil (aka Sodinokibi) attacked Kaseya's VSA (Virtual System Administrator) platform using zero-day exploits to distribute ransomware to customers. Kaseya [claimed](#) that less than 60 customers were affected, but up to 1500 downstream businesses were affected.

The Dutch Institute for Vulnerability Disclosure had identified the vulnerabilities used in this incident and reported them to Kaseya prior to the REvil exploit. It is likely that the relatively quick containment and low impact of this incident can be attributed in part to the advance warning. This highlights the importance of *responsible disclosure programs* and effective communication between vulnerability researchers and service providers.

Microsoft Vulnerabilities



Microsoft released an [advisory](#) showing that hundreds of organizations have been targeted in attacks seeking to exploit a vulnerability in its MSHTML browser engine. Since the disclosure of the vulnerability's proof-of-concept, multiple threat actors have incorporated the code into their attack kits. Some of the infrastructure used in attacks involving the vulnerability previously has been associated with delivery of Trickbot and BazarLoader backdoors, two highly successful malware variants used to compromise systems and download ransomware and other types of malware.

REvil Rebrands

In July, REvil/Sodinokibi, the ransomware group responsible for the attacks on meatpacker JBS and Kaseya, [went offline](#). However, in September the group's infrastructure and dark web presence, including payment portals and chat functions, resumed. While it is unclear whether operations were taken down by legal action, it is suspected that law enforcement got too close for comfort and caused the group to lay low for a while. This is not the first time the group has disbanded; in 2019, the GandCrab ransomware operators declared they were retiring after 'making enough money.' Similarities in code show that GandCrab and REvil are likely the same people.

There have been several arrests globally in 2021 of individuals purportedly affiliated with REvil activity, dubbed Operation GoldDust. In January 2022, Russian authorities said that they had arrested 14 members of the group. It remains unclear whether these were the main actors or whether REvil will again pop up in another guise.



- Third-Party Risk
- Zero-Day Vulnerabilities
- Ransomware

October

Syniverse

Syniverse, a global telecommunications service provider responsible for the routing of billions of text messages between mobile carriers, [reported](#) that hackers had accessed its information technology and operational technology systems since 2016, with 235 customers affected. The exposed text metadata included sender and recipient phone numbers, locations and device identification information, which could be used for smishing, espionage, and other malicious activity. This multi-year exposure incident further demonstrates cellular text messages should not be relied upon for sensitive transactions including multi-factor authentication.

FS-ISAC Spotlight Calls

When security incidents with potential impact to the financial sector occur, FS-ISAC hosts member-wide webinars, often with speakers directly related to the situation, to provide members with the most current information on the incident, detection and mitigation advice, and discussion on potential impact to the sector.

PAX PoS Terminals

The FBI [raided](#) the Florida office of Shenzhen-headquartered PAX Technology Inc. (PAX) as part of an investigation into unusual network packets being sent from point-of-sales (PoS) payment terminals manufactured by the company. PAX devices, which number 60 million in 120 countries, were discovered as being used both as a malware “dropper” or repository for malicious files, and as “command-and-control” locations for staging attacks and collecting information.

While it is not uncommon for payment terminals to be compromised remotely by cyber criminals, the PAX incident is of unique security concern because the involvement of multiple law enforcement agencies suggested nation-state involvement in espionage on the financial system that is not for financial gain.

A growing number of financial service providers have removed PAX terminals from their payment infrastructure as a precaution. The investigation and the resultant collapse of PAX’s share price and share trading halt placed further strain on already deteriorating relations between China and the United States. PAX initially responded to the FBI raid by claiming that the investigation was racially and politically motivated, and later issued a statement that the unexplained traffic from PAX terminals was related to the optional geolocation feature. A full investigation and explanation is still pending.





November

More Ransomware Groups ‘Retire’

After the DarkSide ransomware caused the highly disruptive Colonial Pipeline incident in May 2021, the operators declared they were ceasing operations, likely due to the strong reaction from the White House. Shortly thereafter, they rebranded as BlackMatter and have remained a prolific actor in the ransomware world. In November, BlackMatter announced that they were shutting down their operations after being pursued by law enforcement; however, the operators provided their existing affiliates with decryptor keys to allow for continued extortion attempts.

Other ransomware groups, such as Avaddon, Ragnarok, and SynAck, have also closed down operations in 2021 and publicly released their decryption keys. While the real motives behind declaring shutdown cannot be known, law enforcement pressure is likely a stronger motivator than having made enough money for retirement.

December

Log4j

The Apache Software Foundation disclosed a critical zero-day vulnerability affecting Apache Log4j 2, an open-source Java-based library that allows developers to log data within their application. It is used in countless enterprise applications and numerous cloud services. The vulnerability has been dubbed Log4Shell and scored as a 10.0 on the CVSS rating system (the highest possible rating). The vulnerability is fairly simple to exploit, enabling unauthenticated threat actors to remotely execute code on vulnerable applications by sending a single line of malicious code. It therefore poses considerable threat to financial firms, not just via third-party compromise but also directly.

While most activity reported in relation to this vulnerability is limited to scanning by external actors for vulnerable instances, there has been observed activity of multiple threat actors, botnet operators, and state-sponsored actors exploiting the vulnerability to deploy Cobalt Strike and malware such as cryptominers and ransomware. The installation of Cobalt Strike – a legitimate tool used by security testers - is often a precursor to data exfiltration and ransomware deployment. Data collected by FS-ISAC in December 2021 and January 2022 indicates between 1-3% of members may have experienced successful network infiltration from this exploit.

Emotet Returns

Appearing in 2014, Emotet evolved from a banking trojan into an aggressive platform for spreading other types of malware, including ransomware. It is one of the most prolific malware variants to have ever existed. In January 2021 Operation LadyBird, a joint operation involving multiple law enforcement agencies, resulted in several arrests in Ukraine, as well as the seizure of Emotet infrastructure in the Netherlands. Following this, Emotet activity effectively ceased. In early December 2021 however, Emotet returned, launching spam campaigns delivering malicious macro-laden Word or Excel documents to mailboxes worldwide. As Log4Shell began to impact organizations globally, Emotet was also identified as the initial stage of an attack chain that exploited the vulnerability to deploy Conti ransomware.



Member-Observed Trends

The macro level cyber landscape translates into increased cyber threat activity on a daily basis, as cyber criminals are endlessly inventive on how they gain initial access as well as leverage to extort victims.

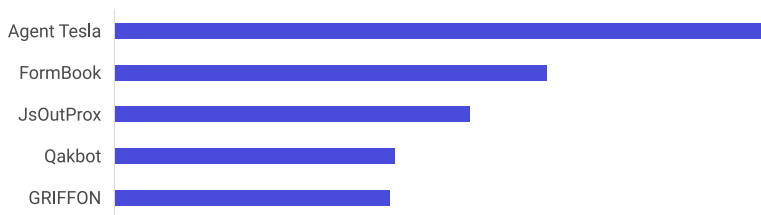
Social Engineering and Fraud

Attacks which attempt to socially engineer victims into clicking malicious links, opening malicious attachments, or divulging sensitive information continue to account for the bulk of FS-ISAC member submissions. In addition to email-based attacks, smishing and vishing campaigns are also on the rise, with smishing being the more prevalent within FS-ISAC member reporting. Compromised business email accounts via phishing are then used to spread further, more convincing phishing, which may result in network compromise or other types of fraud.

24% of member-reported incidents started with employee falling victim to phishing

Average value of attempted BEC fraud
 Source: Agari
\$79k USD

Top 5 Malware Strains



Agent Tesla is a malicious utility being adapted by cyber criminals to replace Emotet, as evident by the large spike observed by members in February. The malware was upgraded with more advanced detection evasion capabilities to be used as a primary entry point.

FormBook is an infostealer that harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to its observed Command and Control (C2) orders.

While OSINT data indicates that FormBook operators often utilize COVID-19-themed lures, member submissions of FormBook campaigns were focused on financial contracts, payments, and other monetary related themes. This is most likely because COVID-19 themes are easily monitored and blocked by financial firms.

The vast majority of malware campaigns reported by members used email as the delivery method. Malspam remains the most used attack vector as cyber criminals, MaaS operators included, can distribute malware to many potential victims with relative ease. This method is a lot more cost effective for cyber criminals than developing zero-day exploits to bypass security measures. Proactive staff training on phishing awareness and basic cyber hygiene, including up-to-date patching, remain the most effective methods of blocking malicious emails from causing successful infiltration.

Distributed Denial of Service (DDoS)

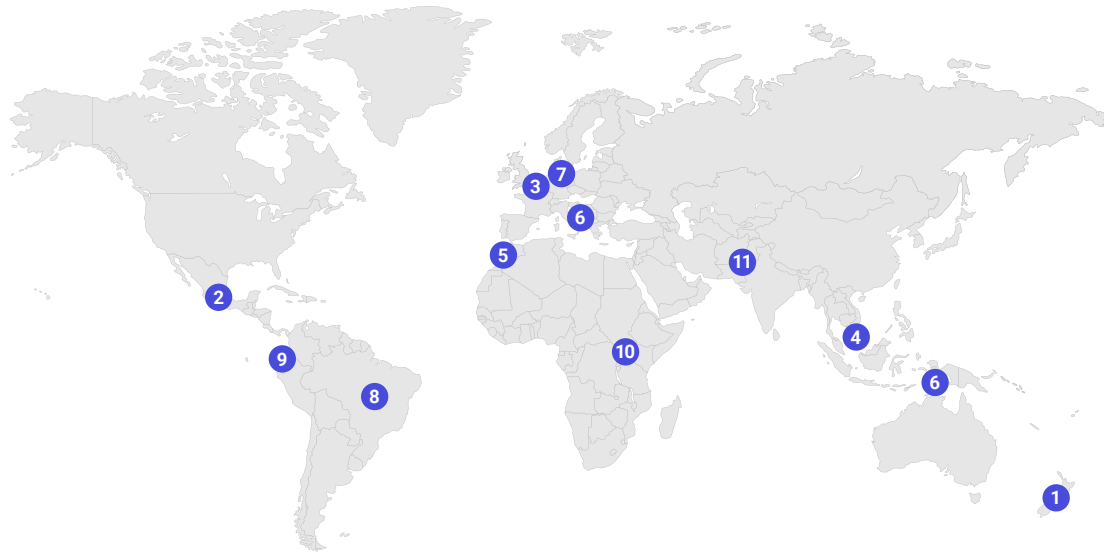
From August 2020 and throughout 2021, FS-ISAC members globally reported threats purportedly from well-known advanced persistent threat (APT) actors threatening a large, distributed denial of service (DDoS) attack unless a ransom is paid. Firms received communications from a variety of APT monikers including the Russian actor groups Cozy Bear (APT 27) and Fancy Bear (APT 28), North Korean-affiliated Lazarus Group, and most recently, a combination of the latter two groups – “Fancy Lazarus.” This activity has been observed on a global scale by multiple sectors.

FS-ISAC maintains its assessment that the actor(s) behind these campaigns are not the APT groups they claim to be but are likely financially motivated cyber criminal actors. Although the actors are likely less capable than the sophisticated APT groups they name, the attacks are larger and more sophisticated than previous DDoS waves similarly claiming to be from known APT groups.

About one percent of FS-ISAC members have reported being targeted by these extortion DDoS activities. While most firms reported no or limited impacts, the demonstrative attacks could present mitigation challenges for some firms. FS-ISAC assesses that DDoS extortion campaigns will continue in the near term.



Incidents Around the World 2021



- 1 January - New Zealand**
Reserve Bank of New Zealand data accessed, exploiting the Accellion file sharing software breach
- 2 March - Mexico**
ATM Jackpotting attacks
- 3 April - Belgium**
DDoS campaigns affecting banks in Europe
- 4 May - Southeast Asia**
Insurance giant AXA hit by Avaddon ransomware, affecting IT operations
- 5 July - Morocco**
"Dr Hex" arrested in an Interpol-led operation. This prolific cyber criminal was responsible for credit card fraud and malware attacks against banks, as well as developing carding and phishing kits for others to facilitate similar fraud
- 6 August - Europe, Oceania**
DDoS attacks possibly linked to REvil
- 7 August - Germany**
Sparkassenverband Baden-Württemberg bank email servers compromised and data threatened to be published unless ransom is paid
- 8 August - Brazil**
Brazilian Treasury hit with ransomware
- 9 October - Ecuador**
Banco Pichincha hit with cyber attack causing ATMs and online banking to go offline
- 10 October - Uganda**
Banks lost almost \$4B to cyber fraud in the past year, according to an Interpol report
- 11 November - Pakistan**
National Bank of Pakistan hit with cyber attack

Europe: Mobile Malware

Mobile devices are used to access email, online banking, other applications which may hold sensitive data, and for multi-factor authentication (MFA). Throughout 2021, the EMEA region, particularly the Nordic countries, were the target of several prominent mobile malware campaigns. The most severe was FluBot, which is spread via fake SMS messages which entice victims into downloading the malware; it then uses screen overlays on top of legitimate banking and cryptocurrency apps to phish victims' credentials. Several other similar malware strains were reported across Europe, the UK, and Turkey.

Latin America and Asia Pacific: Remote Access Trojans

In Latin America, banks have observed an increasing trend in banking RAT-type (Remote Access Trojan) malware, a very difficult threat to detect and control. The newer campaigns indicate criminal intent to bundle malware generation functionalities for easy distribution and use by operators, customers, and affiliates.

JsOutProx, a Javascript-based RAT, was the third-most reported malware by members globally in 2021, and open-source intelligence (OSINT) indicates a large-scale JsOutProx campaign in the APAC region. The malware has modular plugin capabilities and is used for running shell commands, downloading, uploading, and executing files, manipulating the file system, establishing persistence, taking screenshots, and manipulating keyboard and mouse events.



Predictions for 2022 and beyond

We expect current trends to continue, and possibly worsen, over the next year. The trifecta of the expansion of the financial sector's attack surface through third-party suppliers, the growth in zero-day vulnerabilities as an attack vector, and the ability of ransomware groups to adapt and thrive despite increased scrutiny by law enforcement make for an especially challenging cyber threat environment. Cybersecurity is no longer just a back-office cost; cyber threats now pose critical business risks, including:

- **Operational disruption**
- **Material customer loss**
- **Increase in insurance premiums**
- **Lawsuits or fines**
- **Systemic destabilization**
- **Credit downgrade**
- **Reputational damage**

01 Nation-State Campaigns Will Mirror Geopolitical Tensions

Geopolitical tensions around the world have ushered in more cyber activity by both patriotic hackers and nation-states, targeting governments and militaries as well as the private sector. The US Treasury has been especially active imposing sanctions against other governments in the past year, which could draw retaliation from those governments in the cyber space. Military conflict in Ukraine, the ongoing protest activity in Hong Kong, and continued missile launches by North Korea could produce cyber activity – both espionage-related and overt retaliatory attacks – against numerous targets in the US, UK, EU, Australia, South Korea, Japan, and other locations. Possible retaliation could include, but is not limited to, denial of service attacks, spear phishing, brute-force attacks, or vulnerability exploitation attempts. Public-private partnerships should support the timely release of relevant threat intelligence.

02 Nation-States Will Influence the Supply Chain

The PAX PoS terminals incident raises the question of nation-state influence over financial sector suppliers. Members should consider where their products and services are coming from and if there may be any nation-state intervention, currently or in the future. The source of software and location of data are already being considered in the context of regulatory requirements, but even non-sanctioned sources may pose a potential threat. In order to properly manage supply chain risk, organizations will need a holistic view of threat intelligence that includes a real-time understanding of the geopolitical landscape.

03 Ransomware Groups Will Continue to Professionalize

Despite the increased scrutiny in 2021, ransomware attacks are a lucrative business and unlikely to disappear or even decrease. They may re-focus to geographies where there is less public sector activity against them, such as Latin America and Africa. While ransomware infrastructure can be taken down and ransomware affiliates can be arrested, the "big game hunting ransomware" run by Russia-based ransomware groups will likely not be impacted as much due to the lack of major consequences for these actors, and the ease with which they can resume operations with different names and different infrastructure. Coupled with current geopolitical tensions, we anticipate a potential increase in highly targeted ransomware in the coming year.



04 Third-Party Risk Will Continue to Threaten Financial Firms

2021's successful attacks against third-party providers demonstrated that a one-to-many compromise chain is possible. Supply chain threats will undoubtedly persist, especially to target entities who are considered adequately hardened to traditional attack methods, such as financial institutions. Software updates, application programming interfaces (APIs), file transfer services and service management platforms will continue to be targeted due to the level of trust they often receive in the customer environment. Instilling a zero-trust mindset and engaging in threat hunting activities (which assume a level of compromise already) will aid in mitigating against these types of attacks. In response to the heightened threat from suppliers, regulators around the world are tightening guidance on third-party risk management. To aid members in their third-party risk management efforts, FS-ISAC has created the [Critical Providers](#) program to provide a direct line between key providers and the sector to increase dialogue and speed of incident response. FS-ISAC also introduced [Scout](#), a marketplace for cybersecurity service providers which includes ratings and reviews by fellow members.

05 Zero-Day Vulnerabilities Will Increase

Due to the jump in reported zero-day vulnerabilities in 2021 and the continued work-from-home environment, it is possible that more flaws in hardware and software programs will be found in the coming year. Organizations will need to remain vigilant about timely patching but also basic cyber hygiene practices; in some cases in the past year, firewall best practices and segregation prevented certain attack methods even with a newly discovered vulnerability. Responsible disclosure programs can make the difference in allowing a manufacturer to develop patches before vulnerabilities are publicly reported and therefore exploited by a sea of attackers, as was observed with the Microsoft Exchange vulnerability and the Log4j vulnerability.

06 Regulators Will Tighten the Reins

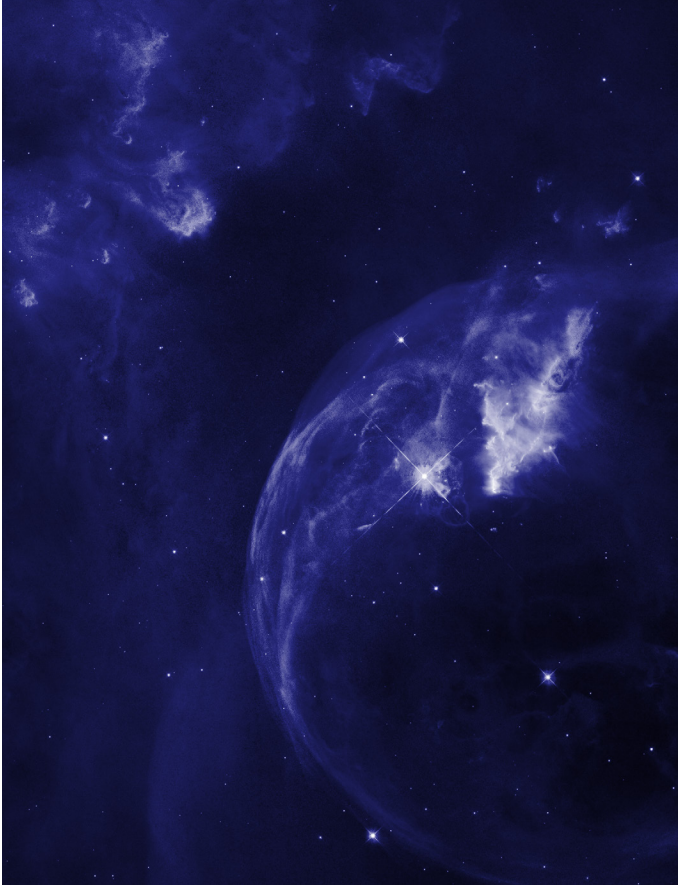
Financial regulators around the world have already begun to issue more stringent guidance on third-party risk management and operational resilience. From the US Securities and Exchange Commission to the European Central Bank to the Monetary Authority of Singapore, authorities have signaled they plan to increase cybersecurity compliance obligations such as mandating cyber risk and incident disclosures, shortening notification windows, and holding firms accountable for service providers' cybersecurity measures. Authorities are getting more involved in information sharing and warnings as geopolitical tensions increasingly play out in the cyber sphere, especially that of critical infrastructure. This will continue, with agencies taking cues and best practices from each other.

07 Incident Response Will Mature

With incidents becoming more frequent and severe, the entire ecosystem around incident response, from internal teams and processes, to integrated technologies, tools, and platforms, to external legal and communications firms, will evolve to help streamline and mature incident response. A shared Word document will no longer suffice as a playbook; boards, auditors, and regulators will demand that firms level up. Incident response teams will have a higher profile within the business. Third-party providers of incident response tooling and services are poised for success.



Global Intelligence Office



The Financial Services Information Sharing and Analysis Center (FS-ISAC) is the only global cyber intelligence sharing community solely focused on financial services. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyber threats. FS-ISAC members represent over \$35 trillion in assets under management, with 16,000 users in 65 countries. Headquartered in the United States, the organization has offices in the United Kingdom, the Netherlands, and Singapore. To learn more, visit fsisac.com. To get clarity and perspective on the future of finance, data and cybersecurity from top C-level executives around the world, visit [FS-ISAC Insights](#).

The FS-ISAC Global Intelligence Office (GIO) coordinates and disseminates analysis of member-submitted intelligence as well as threat alerts to its member financial institutions around the world. GIO regularly issues reports and convenes member calls as well as spotlight calls on emergent issues to ensure members are prepared for current threats.

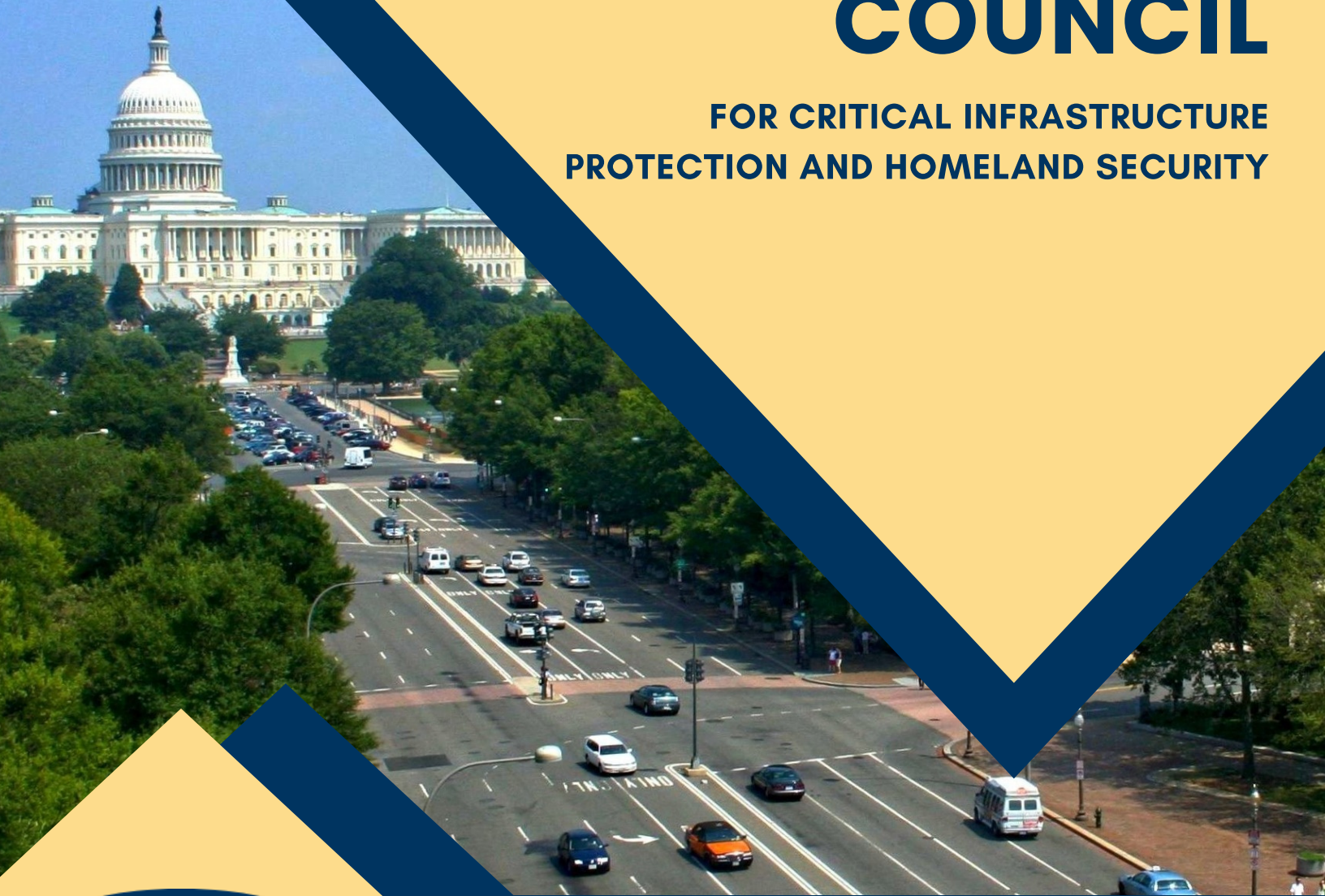
GIO also coordinates with other cybersecurity organizations, companies, and agencies around the world to ensure actionable and timely cyber intelligence is disseminated to our members. GIO is a 24-7, follow-the-sun operation with teams in Singapore, the Netherlands, UK, and US.

If your financial institution is not yet a member of FS-ISAC, apply to become a member [here](#).

The FS-ISAC® brands and trademarks constitute the intellectual property of FS-ISAC, Inc. Nothing contained on this report should be construed as granting, by implication, estoppel, or otherwise, any license or right to use the brand, trademarks, or any other intellectual property contained therein without written permission of FS-ISAC. FS-ISAC reserves all rights in and to the report and its content. The report and all of its content, including but not limited to text, design, graphics, and the selection and arrangement thereof, is protected under the copyright laws of the United States and other countries.

FINANCIAL SERVICES SECTOR COORDINATING COUNCIL

**FOR CRITICAL INFRASTRUCTURE
PROTECTION AND HOMELAND SECURITY**



Protecting Critical Financial Infrastructure

The financial sector faces one of the most complex regulatory environments with respect to policy, cybersecurity, and resiliency. With over a dozen regulatory bodies and federal agencies that either oversee or shape policies, programs, and market infrastructures for banks, insurers, and other financial institutions. The scale and scope of these requirements has at times caused firms to divert resources away from keeping up with threats and implementing next generation security tools, to responding to compliance questionnaires or duplicative requests for information.

The Financial Services Sector Coordinating Council, or FSSCC for short, was established in 2002 by financial institutions to work collaboratively with key government agencies while coordinating critical infrastructure and homeland security activities within the financial services industry.

We are an industry-led non-profit organization and our mission is to bring together our members from financial services, trade associations, and other industry leaders to assist the sector's response to natural disasters, threats from terrorists, and cybersecurity issues of all types.

The FSSCC partners with the public sector on policy issues to enhance the security and resiliency of the United States financial system.

The U.S. Department of Homeland Security recognizes the FSSCC as a member of the Critical Infrastructure Partnership Advisory Council on behalf of the banking and finance sector.



The Mission

The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats, promoting protection, driving preparedness, collaborating with the U.S. Federal government, and coordinating crisis response - for the benefit of the Financial Services sector, consumers and the USA.

FSSCC has identified the following objectives to expand upon the mission statement:

- Foster collaboration and awareness between the Financial Services Sector, the public sector, and other critical infrastructure sectors.
- Facilitate public-private partnerships to address resiliency for the U.S. Financial Services Sector.
- Strengthen the Financial Services Sector through intra-industry coordination.
- Collaborate on operational risk initiatives with financial services trade association members and other entities.
- Develop and foster a strategic vision to address the convergence of cyber security and resiliency within the broader operational risk landscape.



Our Members & Our Partners

► Our Members

Our 70+ members consist of financial trade associations, financial utilities, and the most critical financial firms. The FSSCC coordinates the development of critical infrastructure strategies and initiatives with its financial services members, trade associations, and other industry sectors.



► Our Partners

FSSCC partners with the public sector on policy issues concerning the resilience of the sector.

The Department of the Treasury is the Sector Specific Agency assigned to financial services. The FSSCC and Treasury have developed a strong public-private partnership with the shared goal of maintaining a robust and resilient financial services sector.

Over the years, the FSSCC has also built and maintained relationships with the U.S. Department of Homeland Security, all the federal financial regulatory agencies and law enforcement agencies. Through these relationships, the FSSCC directly assists the sector's response to natural disasters, threats from terrorists, and cybersecurity issues of all types.



FSSCC Committees

- Management Committee
- Joint Exercise Committee
- Joint Intelligence Collaboration & Information Sharing Committee
- International Committee
- Policy Committee
- Digital Identity Committee
- Research & Development Committee
- Joint Workforce Working Group





SHELTERED HARBOR

WHAT IS SHELTERED HARBOR?

Sheltered Harbor was created to protect customers, financial institutions, and public confidence in the financial system if a catastrophic event like a cyberattack causes critical systems - including backups - to fail. Implementing Sheltered Harbor is key to adopting a comprehensive operational resiliency strategy that focuses on continuity of critical customer-facing business services.

Sheltered Harbor is not a vendor, product or service. It is a not-for-profit, industry-led initiative comprising financial institutions, core service providers, national trade associations, alliance partners, and solution providers dedicated to enhancing financial sector stability and resiliency.

INDUSTRY PARTICIPATION

Participants can leverage an ecosystem and community of qualified trusted partners that provide the services, technology, software and solutions for isolated backups and recovery to ensure adherence to Sheltered Harbor standards.



ORIGINS

Sheltered Harbor was launched in 2015 by the U.S. financial sector following the Hamilton Series of public-private cybersecurity exercises facilitated by the U.S. Department of the Treasury.

The conclusion of the exercises was that the financial services industry — and the U.S. economy — could be vulnerable if a cyberattack disabling one or more financial institutions leads to a loss of public confidence.

In response, the industry created Sheltered Harbor to promote the stability of U.S. financial markets by protecting critical account information of market participants in order to facilitate recovery of such information.

SHELTERED HARBOR'S MISSION

To protect public confidence in the U.S. financial system if a devastating event like a cyberattack causes an institution's critical systems - including backups - to fail.

HOW IT WORKS: CORE ELEMENTS

1 Data Vaulting

Institutions back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups.

2 Resiliency Planning

Institutions prepare the business and technical processes and key decision arrangements to be activated in the case of a Sheltered Harbor event; where all other options to restore critical systems - including backups - have failed.

They also designate a restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible.

3 Certification

Certification is a critical component of the Sheltered Harbor initiative. Participants adopt a robust set of prescribed safeguards and controls, which are independently audited for compliance with the Sheltered Harbor standard.

Upon completing the requirements for Data Vaulting, the institution will be awarded Sheltered Harbor certification and an accompanying seal, communicating that their customer account data is protected.



ECOSYSTEM

From the beginning, Sheltered Harbor has enjoyed critical industry support:

- American Bankers Association (ABA)
- BITS, Bank Policy Institute (BITS/BPI)
- Credit Union National Association (CUNA)
- Financial Services Forum (FSF)
- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Independent Community Bankers of America (ICBA)
- National Association of Federal Credit Unions (NAFCU)
- Securities Industry and Financial Markets Association (SIFMA)
- The Clearing House (TCH)

Several hundred subject matter experts and industry professionals contributed to the development of the solution and actively participate in the initiative's workgroups to ensure Sheltered Harbor remains the gold standard in operational resiliency.

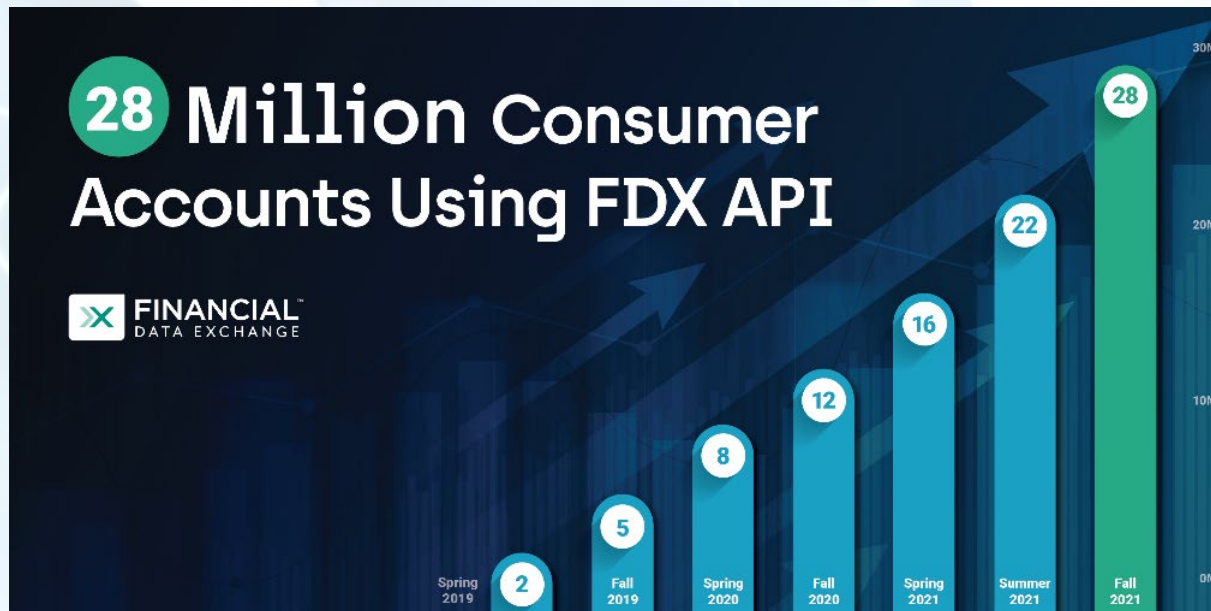
Sheltered Harbor has engaged a community of specialized trusted partners who provide the services, technology and solutions necessary to help our participants implement the Sheltered Harbor standard. The number and scope of these partnerships expands as the initiative matures.

FDX is an international, nonprofit technical standards body *dedicated to unifying the financial industry* around a common, interoperable, royalty-free standard for the secure access of permissioned consumer and business financial data, the FDX API.


Our members: **> 200 members | ¼ of members are Fin-Tech firms | 2/3 are *not* banks**

Our leadership: **Our Board comprises 12 Financial Institutions, 5 Permissioned Parties, 5 Aggregators, 2 Industry Groups, FS-ISAC, 1 Canadian Fintech, and 1 Consumer Advocacy Group observer.**

Our adoption:



FDX Specifications

-  API & Data Structures
-  User Experience
-  Security
-  Certification