FS-ISAC

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 than fewer than 100 customers were hacked.

FS-ISAC Member Survey

April 2021

6% impacted directly

40% impacted suppliers

52% plan to make changes to third-party risk management processes as a result

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

23% impacted by suppliers who were potentially breached

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.

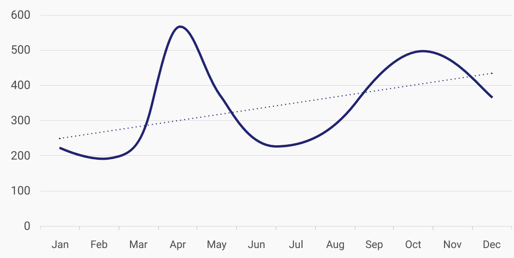
May

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.



Ransomware Compromises in 2021

Scraped from Multiple OSINT Sources

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

June

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.

July

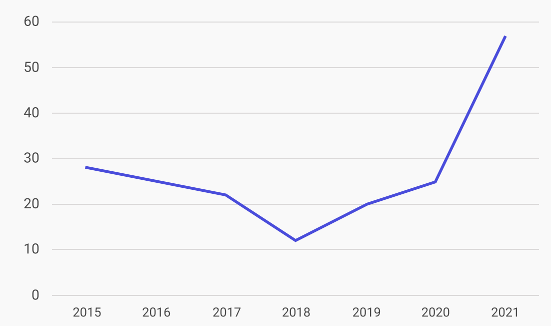
Kaseya

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.

September

Microsoft Vulnerabilities



Patched Zero-Day Vulnerabilities
Data source: googleprojectzero.blogspot.com

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.

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

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

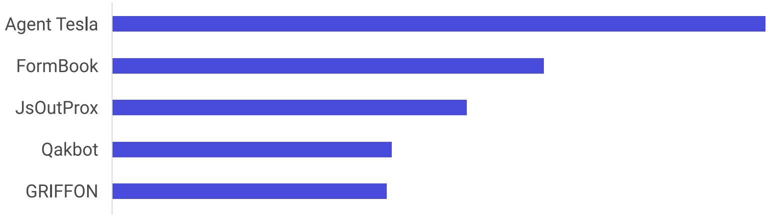
Attacks which attempt to socially engineer victims into clicking malicious links, opening malicious attachments, or divulging sensitive information continue to account for the bulk of FS-ISAC member submissions. In addition to email-based attacks, smishing and vishing campaigns are also on the rise, 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 **$79k USD**

Source: Agari

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.

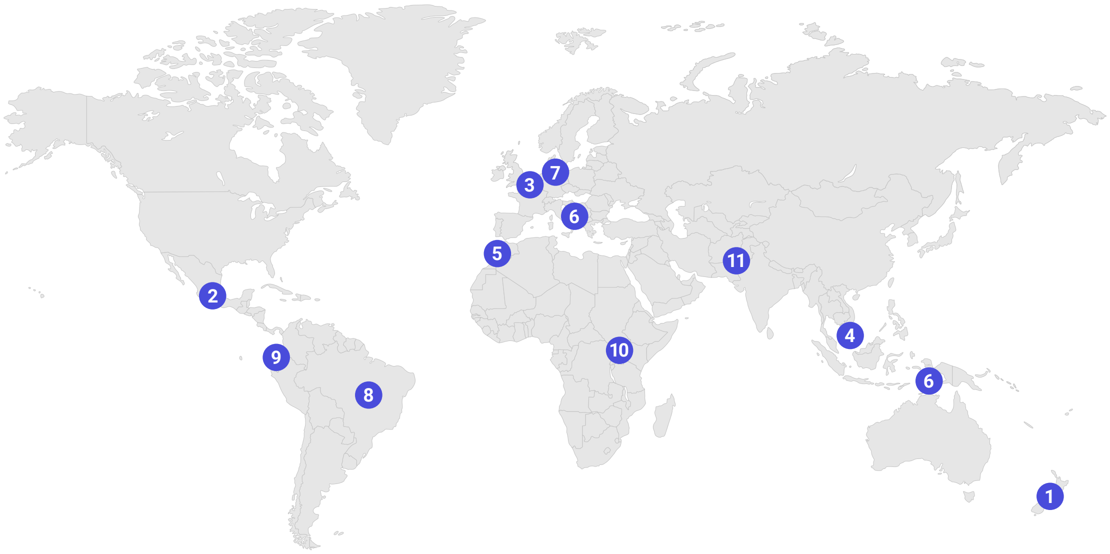
Distributed Denial of Service (DDoS)

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-Württenberg 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

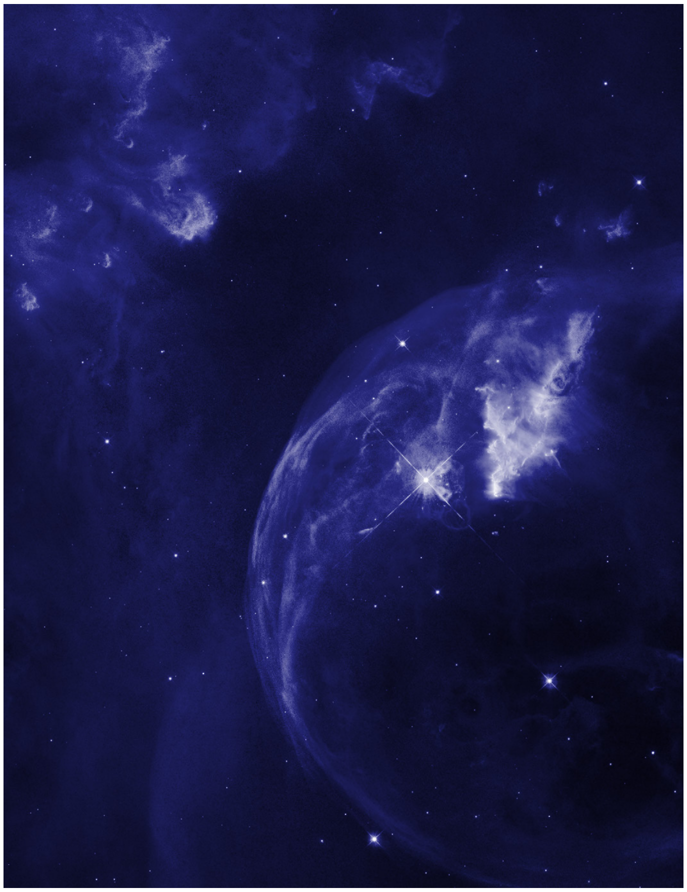
Financial regulators around the world have already begun to issue more stringent guidance on third-party risk management and operational resilience. From the US Securities and Exchange Commission to the European Central Bank to the Monetary Authority of Singapore, authorities have signaled they plan 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.

FS-ISAC

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.