sifma®

CYBERSECURITY

SMALL FIRMS CYBERSECURITY GUIDANCE

HOW TO CONSUME THREAT INFORMATION FROM THE FS-ISAC

DISCLAIMER

This document was prepared as an account of work within the private and public sector. Neither SIFMA or any of this members, or any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by SIFMA.

EXECUTIVE SUMMARY

The purpose of this guidance is to assist small firms in the financial services industry to efficiently and effectively make use of information from the Financial Services Information Sharing and Analysis Center (FS-ISAC). The target audience for this guidance is small firms that typically have one to two hours per week that can be dedicated to reviewing and evaluating cybersecurity threat information. As information can come from many sources (media, peer-to-peer relationships, law enforcement, trade associations, etc.) and every individual will have their own subjective "go-to" sources.

We feel the FS-ISAC provides the most complete and up-to-date view on the current and future cybersecurity threat picture for the industry. The FS-ISAC derives their data and information from government, security industry sources and their over 4,500 financial industry members. This data has been vetted by cyber security professionals and will bring immediate value without additional need for independent validation thus enabling quick response to those firms with limited resources. SIFMA encourages small firms to join FS-ISAC in order to promote wider information sharing across the financial industry.

However, the extensive coverage and large number of alerts that they provide on a daily basis can prove difficult for a small firm to sort through to find relevant information. Hence the goal of this document is to provide a strategy and some tactical guidance for how a firm and the responsible individual at the firm can effectively triage and consume the data they receive from the FS-ISAC on a daily basis in order to gain an effective understanding of the threats their firm is facing.

THREAT INFORMATION TRIAGE AND CONSUMPTION STRATEGY

In order to maximize the benefit of FS-ISAC information in the space of an hour or two per week, it is suggested, that firms approach the cybersecurity threat information with these areas in mind when assessing criticality and applicability:

- Does the threat pose a potential or direct risk to your company?
- Does the cybersecurity threat have (or is it expected to have) significant media attention/hype-oriented that is or expected to generate inquiries?
- Is this a threat which has resulted in a direct inquiry internally, typically from senior management or the Board?
- Are peer financial institutions seeing heightened or similar threat activity (neighborhood approach to assessment)?

- Is the campaign or threat targeting more than one peer financial institution? What is the level of volume being reported (targeting or success rate)? Is it significant?
- Is a new (novel) social engineering approach being used?
- Does this threat involve previously successful actors, campaigns or tools that have impacted the firm or sector?
- Does this threat involve a new technique, novel malware or actor group of significance?

TOOLS AND INFORMATION AVAILABLE

CYBER THREAT LEVEL

What Is It?

The Cyber Threat Level is designed to assist financial institutions in prioritizing protective measures that they may take to better protect their firm and guide their overall readiness. FS-ISAC members can utilize this system to combine cyber threat information in conjunction with their own internal asset protection plans to better protect their organization and the financial services sector at-large. The cyber threat level indicator follows five levels of severity – low, guarded, elevated, high, and severe – which are color coded and have specific indicators of threat levels to the financial industry.

Cyber Threat Levels	
Level	Threat
Severe	Severe risk of cyber attacks
High	High risk of cyber attacks
Elevated	Significant risk of cyber attacks
Guarded	General risk of cyber attacks
Low	Low risk of cyber attacks

**** Please note the five stage threat level is under review for modification by the FS-ISAC. ****

What Is Most Important?

The advisory levels have clear responses devised by FS-ISAC that firms can take in the case of the raising or lowering of the threat level. The levels and responses can be found in the table below. [1]

[1] FS-ISAC Threat Advisory System, 2006, Page 5

Advisory Levels

Level	Response Guidelines
Cyber-GREEN (Low)	1. Have an emergency plan for IT operations: - Ensure all business critical information and information systems (including applications and databases) and their operational importance are identified. - Ensure all points of access and their operational necessity are identified. 2. On a continuing basis, conduct normal security practices. For example: - Conduct education and training for users, administrators, and management. - Ensure an effective password management program is in place. - Conduct periodic internal security reviews and external vulnerability assessments. - Conduct normal auditing, review, and file back-up procedures. - Ensure effective virus protection scanning processes are in place. - Confirm the existence of newly identified vulnerabilities and test and install patches as available. - Periodically review and test higher Threat Alert Level actions and IT recovery plans. 3. Maintain law enforcement liaison-e.g. US Secret Service Electronic Crimes Task Force (see FS/ISAC for local contact information), local FBI, InfraGard, etc.
Cyber-BLUE (Guarded)	4. Implement measures 1-3 if not already implemented. 5. Communicate work force awareness messages to be alert and who to report unusual cyber activities to. 6. Review security and operational plans and procedures and ensure they are up-to-date.
Cyber-YELLOW (Elevated)	7. Implement measures 1-6 if not already implemented. 8. Increase level of auditing, review, and critical file back-up procedures. 9. Conduct internal security review on all critical systems. 10. Increase review of intrusion detection and firewall logs. 11. More frequent checks of cyber security communications for software vulnerability. 12. Identify additional business/site specific measures as appropriate. 13. Increase frequency of measure 3 – include additional instructions as appropriate to your Cyber Alert Level Response Plan.
Cyber-ORANGE (High)	14. Implement measures 1-13, if not already implemented. 15. Conduct immediate internal security review on all critical systems. 16. Determine staffing availability for backup operations and provide notice. 17. Consider increasing physical access restrictions to computer rooms, communications closets, and critical operations areas. 18. Consider account access restrictions-temporarily disable noncritical accounts. 19. Consider delaying scheduled, routine maintenance or non-security sensitive upgrades. 20. Media releases should be reviewed with Cyber Alert Level Coordinator prior to release. 21. Review plan for returning to Alert Advisory Level-Yellow, Blue or Green. 22. Additional business/site specific measures as appropriate.

Cyber-RED (Severe)	23. Implement measures 1-22, if not already implemented. 24. Consider 7/24 emergency tech support staffing. 25. Consider continuous 7/24 monitoring of intrusion detection and firewall logs. 26. Consider continuous 7/24 monitoring of cyber security communications for latest vulnerability information. Contact software vendors for status of software patches and updates. 27. Consider reconfiguring information systems to minimize access points and increase security. 28. Consider rerouting mission-critical communications through unaffected system. 29. Consider disconnecting non-essential network access. 30. Consider alternative modes of communication and disseminate new contact information, as appropriate. 31. Consider activation of the company emergency management team/procedures. 32. Actively monitor communications with all appropriate law enforcement and cyber security agencies for two-way updates on threat status. 33. Review plan for returning to Advisory Alert Level- Orange, Yellow, Blue and Green. 34. Additional business/site specific measures as appropriate.

What Should I Do With It?

SIFMA suggests reviewing the response guidelines in terms of current cybersecurity practices and policy specific to your firm. The focus should remain on preparedness in the event of a cybersecurity incident, either localized or industry-wide. If the threat level changes, specifically if it is raised we suggest firms reevaluate their readiness and protections per the FS-ISAC guidance above.

Where Is It?

Every two weeks the level is reassessed and posted on the FS-ISAC portal and emailed to all members as an alert.

EMAIL ALERTS

What Is It?

FS-ISAC email alerts are produced daily to provide timely information on new threats, vulnerabilities, incidents, mitigation strategies or intelligence analysis that can be used to inform a firm. They follow a standard format, which can be used to easily prioritize the incoming information via email rules.

What Is Most Important?

It should only require five or ten minutes daily to review the email activity from the day prior for anything that may be of interest that is not a high priority (see triage rules below). Emails are all structured in a consistent manner within the subject line, and begin in the form of [Alert_Type][Criticality], which specifies what area the alert pertains to and the numerical level of criticality.

What Should I Do With It?

We suggest you setup rules within your email software that allows you to highlight pertinent cybersecurity related alert types and the highest levels of criticality. That way serious industry issues can be recognized immediately and should be addressed as they arrive. The remaining email alerts of a lower criticality can be kept for daily or weekly reviews. The chart below highlights the alerts specific to cybersecurity along with the highest levels of criticality, and which should require the most attention. This is one suggested method of filtering the information provided by FS-ISAC. Others methods could be considered based on time and risk threshold of a particular firm.

Levels of Email Alerts		
Type of Alert	Symbol	Suggested Criticality
Announcements	ANC	8-10
Cyber Vulnerabilitie	CYV	10
Cyber Threats	CYT	10
Cyber Incidents	CYI	4 & 5
Collective Intelligence	COI	10
Physical Threats	PHT	10
Physical Incidents	PHI	4 & 5

For Cyber Incidents and Physical Incidents the "Suggested Critically" ranges from 1-5 and is meant to denote severity of impact with 5 = "severe".
For all other alert types the "Suggested Criticality" ranges from 1-10 with 8-9 denoting a urgent alert and 10 denoting a crisis alert.

Where Is It?

Email alerts are sent directly to the member's accounts, which can then be accessed from the portal depending on their classification.

FS-ISAC PORTAL

What Is It?

The FS-ISAC Portal serves as the primary mechanism to securely share and disseminate relevant, timely, and actionable alerts associated with physical and cyber incidents, threats, vulnerabilities, and solutions associated with the sector's critical infrastructures and technologies.

What Is Most Important?

The main page of the portal provides the current threat level and additional information about the portal itself. The Intelligence Viewer tab contains the current and historical threat information submitted to and distributed by the FS-ISAC. The portal also provides access to documents and white papers written by and for FS-ISAC on a wide range of subjects.

What Should I Do With It?

Small firms can remain up-to-date on FS-ISAC programs, events, and information from within the portal. Further, firms can share their own threats with the broader community. Most email alerts will link back to the Portal in order to access the details of an alert.

Where Is It?

The FS-ISAC Portal can be found from the main FS-ISAC webpage or from this link:
https://portal.fsisac.com/web/fs-isac

EMAIL LISTS (CYBER INTEL LIST)[2]

What Is It?

The cyber intelligence (CyberIntel) mailing list is an attributable, open discussion mailing list that facilitates the rapid dissemination of cyber intelligence, assisting with uncovering a specific threat or incident as it unfolds. The CyberIntel mailing list is a widely adopted mode of communication that is open to all FS-ISAC members.

What Is Most Important?

It is highly encouraged for all members to join this mailing list upon initiation of membership to receive information that can be used immediately in the current threat environment. Further, activity will increase in response to specific cybersecurity issues, such as Heartbleed, so the number of emails received may be used as a leading indicator that a far reaching incident may have occurred.

What Should I Do With It?

This peer-to-peer information sharing platform enables members to learn what others are doing tactically to combat threats and what threats firms are facing. In addition, it can be a good forum to ask questions of industry subject matter experts.

Where Is It?

Information on joining the mailing list can be found in the membership guide and on the FS-ISAC portal.

PROVIDING INFORMATION

Information sharing is a critical part of the FS-ISAC operation. Cybersecurity threats are continually changing and adapting, and what may appear to be a targeted, limited event may be part of a larger, more systemic threat. To promote sharing, the portal on the FS-ISAC website has a dedicated section for members to submit threats and issues according to category and type. Any incident that is shared becomes available to the wider FS-ISAC membership, however it is not shared with any regulatory or government agency. Information provided to FS-ISAC is anonymous and the scope of dissemination is in accordance with the traffic light protocol that the submitter sets.

TRAFFIC LIGHT PROTOCOL (TLP CLASSIFICATION)

The FS-ISAC follows strict information handling procedures using the Traffic Light Protocol (TLP). All information submitted, processed, stored, archived, or disposed of is classified and handled in accordance with the following classification. Unless otherwise specified, all information is treated as confidential information (Amber) and is not disclosed to parties outside of the FS-ISAC without the permission of the originator.

The table below describes the classifications of information and intended audiences.

[2] FS-ISAC Membership Guide, June 2014, Page 8

TLP Classification

Classification	Target Audience
FS-ISAC Red	Restricted to a defined group (e.g., only those present in a meeting.) Information labeled RED should not be shared with anyone outside of the group.
FS-ISAC Amber	This information may be shared with FS-ISAC members only and should be considered confidential.
FS-ISAC Green	Information within this category may be shared with FS-ISAC members and partners (e.g., government agencies and ISACs.) Information in this category is not to be shared in public forums.
FS-ISAC White	This information may be shared freely and is subject to standard copyright rules.

MEMBERSHIP

Information on becoming a member and the services provided by FS-ISAC can be found on their website, https://www.fsisac.com/join.

FEEDBACK

Please direct any questions or comments about this product to the Operations, Technology and Business Continuity team at SIFMA via Tom Wagner at twagner@sifma.org.

WWW.SIFMA.ORG