Frequently Asked Questions and Information

FINANCIAL SERVICES

CAPS 2018

CYBER-ATTACK AGAINST PAYMENT SYSTEMS EXERCISE

What financial institutions can participate? All FS-ISAC members and most regulated financial institutions in North America, Europe, Middle East, Africa and Asia-Pacific. FS-ISAC reserves the right to decline participation for institutions on UN, EU, US or other sanctions list. Membership in FS-ISAC is not required.

What is the cost? There is no cost for regulated financial institutions to participate.

How do I change, cancel or ask questions about my registration? Send an email detailing your request to your regional support mailbox: CAPS-APAC@fsisac.com, CAPS-EMEA@fsisac.com or CAPS-NA@fsisac.com. Include your registration number. **DO NOT** attempt to change or reregister on your own; it creates errors and duplications.

Why participate? Pervasive vulnerabilities and cyber-attacks are a serious source of risk for today's financial enterprise. Security breaches, system compromises and many other cybersecurity issues are common and can be severe. FS-ISAC CAPS enables you to put into practice your processes, plans and resources in response to a cyberbreach. You assess your exercise experience and preparedness, while receiving insights on best practices and readiness at your organization and across the financial services industry.

How does it work? You designate one person as the primary point of contact to register your company. Your primary contact receives all communications about the exercise, including the *FS-ISAC Cyber-Attack Against Payment Systems Pre-Exercise Guide* to help prepare for the exercise. Early each morning of the two-day exercise, your Primary Contact receives an email with instructions, a link to retrieve the exercise for that day and a link to the daily survey. Each day, from your own premises and on your own schedule, your team reviews and discusses the information available and confidentially answers a set of survey questions.

Who should register as primary point of contact? Your primary point of contact acts as the exercise coordinator for your organization. They receive and disseminate all exercise information at your institution. They work through the *2018 FS-ISAC Cyber-Attack Against Payment Systems Pre-Exercise Guide* to help identify those who should be involved, set up the calendar for the Exercise day meetings – in person, via conference call, etc. They or a designee may also act as the facilitator or leader for the team activities.

What is the role of the secondary contact? The secondary contact is only in case of emergency. They **will not** receive a second copy of the communications.

What is the Routing Transit Number required on the North America registration? This confirms you are a financial institution. You can look up your institution's Routing Transit Number at http://routingnumber.aba.com.

What is the Bank Identifier Code (BIC) or SWIFT Code required on the AP and EMEA registration? This confirms you are a financial institution. You can look up your institution's code at BankSwiftCode.org.

Where does the exercise take place? At your premises, with our materials, your staff and your timing.

How long does the exercise take? On average, teams work together for two hours each day of the exercise.

What time is the exercise? Your team may undertake the exercise at any time on each of the two days. You will receive the material early in the day and the survey response is due by midnight local time, so you may plan your schedule for each day to best fit the participants and organization.

Is this a vulnerability test of our system? No, it is a tabletop, simulated exercise. Participating will allow you to privately assess your systems and response plans.

What is the *FS-ISAC Cyber-Attack Against Payment Systems Pre-Exercise Guide*? After receiving your registration confirmations, you will receive an email with a link directing you to documentation that includes detailed information, guidelines and tips to help you successfully prepare for and undertake the exercise. You should read this guide when received, well in advance of the exercise date.

What are the technical compatibility requirements? The exercise is sent as an email attachment. It is an audio-embedded PowerPoint slideshow. The survey is sent in the same email as a link to SurveyMonkey.

What is the survey? Survey answers are private and submitted **anonymously**. You must keep a record of your answers. Responses are analyzed to produce an overall picture of how financial institutions are responding to cyber-attacks and what best practices emerge. Most organizations use the survey internally to assess and improve their incident response. Each team's discussions throughout the exercise and the shared survey input provide them with immediate follow-ups from their experience. Comparing an individual organization's survey response with the aggregate response provides an informal gauge to strengthen an institution's incident response to cyber-attacks.

Frequently Asked Questions - 2018 CAPS Exercises

What is the after-action? In the month following the exercise, the survey results are tabulated for your region and across other regions. You will receive a copy of the results and be invited to a WebEx presentation of the findings, hosted and facilitated by FS-ISAC. Results are also shared at the 2018 FS-ISAC EMEA Summit, 1-3 October in Amsterdam and the 2018 Fall Summit, 11-14 November in Chicago.

How will the results be meaningful for my financial institution? The surveys are completed anonymously, however some general demographic questions such as asset size, country code and industry help us to compile a useful benchmark-type report that most financial institutions find helpful. These results, combined with your extensive team discussions during the exercise, are qualitatively valuable as well.

Who should be Involved? Typically, the exercise includes the financial institution's incident response team who would respond to a cyber-attack affecting customers using payment services. Many institutions include Information Technology (IT), risk management, payment operations, customer service, communications, legal, line of business managers and decision-making incident response executives. Some ask external partners to be available for consultation during the exercise. A helpful list of possible areas is included in the *FS-ISAC Cyber-Attack Against Payment Systems Pre-Exercise Guide*.

How many people do I need to participate? The number of team members will vary by size, type, structure and geography of participant. The *FS-ISAC Cyber-Attack Against Payment Systems Pre-Exercise Guide* recommends the areas from which you might form your exercise group. Smaller organizations may have a handful or more of people who encompass the key incident response areas, while others may have many more.

Do the same people need to participate in Day 1 and Day 2? You may have different participants on the two days. This occurs primarily when you have schedule conflicts that require limited or split participation on the two days and when your team reaches out to add or substitute representatives based on the events of the first day.

Do we need to complete both Day 1 and Day 2? The exercise is continued across the two days, so the full value is derived from completing both days of the exercise and survey.

Can I get a copy of the exercise before it starts? The simulation is most effective when the event scenario is presented with specific, sometimes limited, information and with a limited time in which to address. The exercise is provided early the morning of each day. If you need time to review, prepare, translate, or provide other support to your term internally, we recommend you build time into the exercise day schedule, prior to holding your first team meeting.

Is there an exercise specific to my size financial institution? The exercise is designed to apply to all sizes of financial institutions with each user adapting it as necessary, "as they go," to suit the specific organization participating.

Who takes part? More than 2,000 registered financial institutions registered for the 2017 FS-ISAC CAPS.

What do past participants say? Ninety percent of past FS-ISAC CAPS participants found good or significant value in the exercise and nearly seventy percent identified process improvements.

- "The scenario deployment is really advanced, very detailed and very good and made us think a lot about multiple things that we need to take into consideration. We would like to participate every year."
- "It was a great experience and a very good opportunity to train and improve our procedures."
- "Our business teams learned a lot about IT security and the threats they work against."
- "Overall a good learning experience and has highlighted a few gaps in our existing run book and planning for such scenarios."

Who creates the exercise? FS-ISAC member volunteers work together with FS-ISAC staff to develop scenarios based on current trends and emerging threats; develop questions for discussion and response in the daily feedback survey, to help participating teams assess their preparedness; script and record roles as members of the incident response team meetings presented in the exercise.

Who can I contact if I have specific questions? Please send an email detailing your question to your regional support mail box: CAPS-APAC@fsisac.com, CAPS-EMEA@fsisac.com or CAPS-NA@fsisac.com.

FINANCIAL SERVICES
CAPS 2018
CYBER-ATTACK AGAINST PAYMENT SYSTEMS EXERCISE