FINANCIAL SECTOR CYBER EXERCISE TEMPLATE

Exercise Overview

The Financial Sector Cyber Exercise Template provides financial sector companies, especially small and medium-sized institutions, with a scenario-based exercise that highlights strategic business decision points and corresponding technical concerns that should be considered when responding to a significant cybersecurity incident.

The exercise template's customizable format allows companies to tailor the cybersecurity incident scenario to their individual needs. The corresponding discussion questions allow companies to explore their understanding of their cybersecurity risks and the processes they have in place to respond to a significant cybersecurity incident.

How to Use this Exercise Template

- Select an internal exercise facilitator (or engage a qualified third party) to organize and manage the exercise.
- Adapt the exercise to your company's particular needs and circumstances, including identifying the most relevant and useful discussion questions.
- Identify exercise participants, who you should generally select from your executive management and board of directors.
- Distribute the scenario and discussion questions to participants in advance of the scheduled exercise to make the exercise as efficient and effective as possible.

Exercise Structure

The exercise scenario involves four parts:

1. An introductory section that provides companies with an opportunity to review their current cybersecurity incident identification, protection, and detection capabilities, as well as processes for information sharing and relationships with external entities;
2. An escalation section that tests companies' processes for responding to and recovering from a significant cyber incident and poses questions about incident governance;
3. A wrap-up section that guides participants to reflect on their companies' overall ability to identify, protect, detect, respond to, and recover from the exercise scenario; and
4. A next step section that invites participants to identify their companies' necessary after-action steps following the exercise.

The exercise's discussion questions use the lexicon—identify, protect, detect, respond, and recover—introduced by the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and used by the G-7 Fundamental Elements of Cybersecurity for the Financial Sector.

Tips for the Exercise Facilitator

1. **Cybersecurity Scenario Review (5 minutes)**
   - Begin by discussing the expected objectives of the exercise and then briefly summarize the scenario.
2. **Discussion Questions (1-2 hours)**
   - Establish, in advance, the time available to discuss questions.
   - While the exercise provides a suggested order for questions to be discussed, the interests of your board members and executive management should guide the flow of the conversation.
   - Participants may wish to identify new discussion questions as the exercise progresses or may wish to refer to previous questions.
3. **Wrap-up (25 minutes)**
   - One of the most important outcomes of the exercise is identifying gaps in existing processes or other lessons learned during the exercise. Capturing this feedback can occur in several different ways, including:
     - The facilitator summarizing identified findings at the conclusion of the exercise;
     - Each participant identifying key items learned during the exercise; or
     - A spectator observing the exercise and tracking lessons learned throughout the exercise.

Follow-on Work: *Institutions may wish to produce a summary report capturing lessons learned and next steps to close any identified gaps.*

Exercise Scenario: Inject 1

Law enforcement and the Financial Services Information Sharing and Analysis Center (FS-ISAC) have tracked a spike in reports from members of the financial sector indicating increased malicious cyber activity, including targeted scanning and intrusion attempts.

Similarly, the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) recently released a notice to members of the financial sector providing specific indicators of malicious cyber activity of which institutions should be aware.

Questions: Information Sharing

What are our strategies and processes for sharing cyber threat and vulnerability information internally and externally, and who is responsible for these strategies and processes?

- What processes exist for sharing cyber threats and vulnerabilities with law enforcement, regulators, sector information sharing forums, and other stakeholders? Who within the company serves as the primary contact for this sharing?
- What processes are in place to facilitate timely sharing of information generated internally? What are the processes to obtain, disseminate, and use information received from external sources?
- What internal and external triggers exist to notify law enforcement, regulators, sector information sharing forums, and other stakeholders of information on threats and vulnerabilities?

Questions: Monitoring

Who identifies cyber threats and vulnerabilities facing our company and our cybersecurity controls? What capabilities do our personnel or functions have; do they have sufficient resources?

- How do we monitor and report on the effectiveness of our cybersecurity controls?
- Do we use external resources to help us? If so, who are they and what do they do?
- How do we receive, prioritize, and take action in response to information on new threats and vulnerabilities facing the company and our controls?
- When and how does executive management and the board receive information on the results of our monitoring and reporting processes?

Exercise Scenario: Inject 2

While low-level scanning, probing, and intrusion attempts against your company's networks are relatively common, your IT teams and service provider begin to track a systematic increase in malicious cyber activity.

Coordinated spearphishing campaigns have coincided with increasingly sophisticated intrusion attempts targeting key company employees. But you have yet to discover any technical indications of compromise on your company's systems or networks.

Questions: Cybersecurity Strategy & Framework

Have we embedded cybersecurity into our risk management framework? If so, how?

- Do we have a cybersecurity strategy and operating framework? If so, what is it? Is it tailored to our business, and operating and threat environments?
- What informs our cybersecurity strategy and operating framework (e.g., NIST Cybersecurity Framework, Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, the G-7 Fundamental Elements of Cybersecurity for the Financial Sector)?
- Have we documented and communicated our strategy and operating framework to relevant personnel? If so, when and how?

Questions: Governance

Who is responsible for implementing our cybersecurity strategy? What are the respective roles of executive management and the board in overseeing that strategy?

- Have we documented and communicated the respective roles and responsibilities of personnel implementing and managing our strategy? If so, when and how?
- How does executive management and the board oversee the implementation and effectiveness of our cybersecurity strategy?
- During a developing incident, who is in charge? When would the incident get escalated to executive management? The board? Are these escalation procedures documented? If so, where?

Questions: Risk and Control Assessment

Have we done an assessment of cyber risks presented by the functions and activities in which we engage and the products and services we offer; and have we identified and implemented controls to appropriately mitigate and manage those risks?

- Have we identified our critical business operations and accounted for those operations in our cybersecurity strategy and associated information security-related plans?
- Have we identified our high-value assets (e.g., systems, data sets) most in need of protection from malicious cyber actors? How have we prioritized protection of those assets?
- What controls are in place to address our identified cyber risks: multi-factor authentication, limited privileged access, regular maintenance and software patching, effective system scanning, and system segregation?
- How do we manage our residual cyber risk (i.e., the risk that controls cannot mitigate)? Is our residual cyber risk within the cyber risk tolerance set by the board?
- Do any of our third-party service providers or other vendors expose us to cyber risk? If so, which ones and how? Do our contracts with those third-party service providers and vendors address and mitigate that risk? If so, how?

Exercise Scenario: Inject 3

Dozens of customers have begun reporting anomalous activity (i.e., unauthorized transfers, unauthorized transactions, and incorrect account balances). Additionally, employees in offices across the region have reported their inability to access several important internal systems.

Following a security review, your service provider reports that an onsite contractor with privileged access to your network fell victim to a spearphishing campaign, inadvertently providing a malicious actor access to your internal systems.

As the service provider continues its investigation, it discovers a malicious cyber actor established command and control within the network using the contractor as its attack vector. Prior to detection, the actor apparently used illicitly obtained login information for customer account systems. The actor has denied employees access to the accounts in an effort to cover its tracks. The service provider's investigation reveals that this issue impacts a significant number of customer accounts. As a result, questions now exist about the accuracy of the company's internal business information.

Questions: Response

How do we respond to a cyber incident like this? What are our processes end to end?

- What are our processes for assessing the nature, scope, and impact of the incident, and our processes for containing and mitigating that impact?
- To whom have we escalated the incident internally at this point; has the board been notified?
- When and how do we notify our regulators and law enforcement, and who specifically do we contact? What do we tell them?
- Does this incident exceed our in-house technical capability to contain? Do we request technical assistance from the government? If so, how?
- How do we address customer inquiries? Who is leading our customer response efforts?
- Is our service provider or other service providers helping us to respond; are they contractually required to help? If so, how and who internally is responsible for coordinating this help?
- Are our business continuity plans triggered? If so, how?

Questions: Response (continued)

What impact would this incident have on our critical business functions? How long can we operate without reliable customer account information?

- How do we confirm a cyber versus operational incident? Who is responsible for determining and communicating this determination?
- What is the potential impact, if any, on our liquidity? What are our options to access additional liquidity, if needed?
- What is the potential impact, if any, on our ability to meet end-of-day payment or other similar obligations? How do we prioritize these obligations if our ability to fulfill these obligations is compromised?

Exercise Scenario: Inject 4

News of the incident leaks to the media and quickly spreads among your customers.

Questions: Response

How do we respond to these media reports?

- Do we wait to respond until the media makes inquiries? Do we pro-actively issue a press release, or engage in other public outreach? Who is responsible for deciding and leading these efforts?
- What do we say? Do we have sample pre-vetted language that we can tailor to this particular incident? Who is responsible for reviewing and signing off on the language?
- Do we let our regulator know before or after we issue a press release or make a public statement?
- Do we have processes in place to ensure that our public statements are consistent with what we are communicating to customers? If so, what are those processes?

Questions: Recovery

When and how do we prioritize our recovery efforts?

- Can we recover customer account information impacted by malware? How?
- Once we control the contagion or determine that our internal customer accounting systems cannot be restored:
  - How do we respond if we cannot obtain or recreate reliable customer account information or other relevant business data?
  - Do we have enough information to rebuild these systems, or will we have to design new network architecture upon which to recreate these systems?
  - What is the estimated cost of reconstituting these systems?
- During the recovery process are we confident that we will not re-infect our systems? Why?
- What technical recovery plans currently exist for this type of scenario, and when were they last tested? How confident are we about the effectiveness of those plans?

Questions: Recovery

What do we communicate about our recovery efforts?

- To whom internally do we communicate about our recovery efforts? What gets reported to executive management and the board?
- What do we communicate about our recovery efforts to other key stakeholders, e.g., regulators, customers, third-party service providers, shareholders?
- How do we manage our public relations after the incident to remediate our reputation? Who has responsibility for these efforts?

Questions: Continuous Learning

Do we have a process to address any identified gaps and lessons learned from this incident? Is that process documented in writing?

- Do we regularly—and when events warrant—review our cybersecurity strategy and framework to address changes in our cyber risk, allocate resources, identify and remediate gaps, and incorporate lessons learned?
- Do we analyze both successes and failures in responding to cyber incidents?
- Do we periodically reassess the effectiveness of our governance, risk and control assessments, and monitoring activities related to cyber incidents? How?
- When updating our response and recovery plans, do we incorporate new developments and lessons learned from our own and publicly reported incidents? How?
- Do we ensure we are up-to-date on all public sector notifications, information sharing, and assistance resources? How?

Exercise Wrap-Up

Summarize key findings and address any identified gaps for possible follow-up actions. Preparing a summary report could help track lessons learned and provide guidance moving forward.

Additional Resources

- NIST Framework
- G-7 Fundamental Elements of Cybersecurity for the Financial Sector
- PPD-41
  - PPD-41 Incident Severity Schema
  - Cyber Incident Reporting - Key Federal Points of Contact
- US-CERT
- FBI Cyber
- DHS Cyber Incident Reporting Guidelines