CYBER CHALLENGE

Cyber Challenge is a tool banks can use to help assess their readiness to confront operational risks and identify opportunities to strengthen their resilience.

The Challenge is made up of different exercises presented using short video vignettes. Each exercise is designed to be completed in about an hour.

Each vignette represents a standalone operational scenario and has associated challenge questions to help prompt discussion. Participants can play the vignettes in any order they wish. They should discuss how they would address the event today and consider ways to mitigate risk in the future.

Institutions may use a free-flowing or facilitated discussion of the vignettes. Below are suggestions for organizing a facilitated discussion. These suggestions serve as a starting point. The format can be modified to fit the unique structure and character of each institution. *For maximum effectiveness, we recommend that members of senior management participate, along with key representatives from each of the financial institution's business lines.*

Leading a Facilitated Discussion

1. Select a facilitator. The facilitator should:

    - be a neutral party who provides structure to the meeting and the discussion to meet the group's goals and objectives.

    - guide information-sharing among the participants, ensure that all participants have an opportunity to contribute, and help participants clarify their goals and objectives for the discussion.

    - ensure that discussions move forward and are focused on the issue at hand.

2. Limit the number of active participants. Limiting participation will allow for all to contribute while keeping the anticipated discussion time to less than two hours. Because the facilitator is responsible for managing the discussions, he or she generally should not be considered an active participant.

3. Select a video vignette and the accompanying challenge cards for participants to view and discuss. The facilitator may use the perspectives of a character in the vignette as the focal point for the discussion (e.g., the Bank IT Manager).

    - Vignette #1 – Farmers & Merchants Bank of Dauerville Item Processing Failure – A new item processing service provider cannot process the volume of transactions generated by the bank.

    - Vignette #2 – Farmers State Bank of Robertsburgh Customer Account Takeover – A corporate customer reports unauthorized withdrawals on its account.

(over)

FDIC

- Vignette #3 – The State Bank of Town City
  Bank Internal Error/Phishing and Malware Problem – Bank staff receive a phishing email that appears to have been sent by the institution's president.

- Vignette #4 – People's State Bank of Morello
  Technology Service Provider Problem – Problems ensue after the financial institution's service provider updates its system.

- Vignette #5 – Farmers Bank of Westburg
  Distributed Denial of Service (DDoS) Attack – The bank IT manager investigates a possible DDoS attack and discovers a second attack that steals data from the institution.

- Vignette #6 – Farmers State Bank of Robertsburgh
  Automated Teller Machine (ATM) Malware – ATM malware reveals deficiencies in a bank's service provider contract.

- Vignette #7 – People's State Bank of Morello
  Ransomware – A cyber-attack has taken place, and important files are being held for ransom.

- (Added 2018) Vignette #8 – Eau Rapides Bank
  Flood – Communication problems ensue after the bank's data center is flooded.

- (Added 2018) Vignette #9 – Bank of Lieferkette
  Supply Chain – Third-party software update infects the bank's system, disrupting core processing and steals data.

4. Establish ground rules. The facilitator should begin by describing his or her role and asking the group to agree on ground rules.

Suggested Ground Rules

1. Adhere to a non-attribution policy. Comments made during these discussions are often exploratory. To create an environment that encourages openness, comments should not be attributed to individuals outside of the exercise. Comments and opinions expressed during the exercise should not compel or restrict responses to actual events after the exercise.

2. Be fully present during the discussion. Turn off or silence all electronic devices. Participate actively to share all relevant information, ideas, and concerns. Listen carefully and ask questions to clarify inferences, assumptions, or doubts.

3. Show respect for all participants by listening and taking all ideas seriously. Encourage participation of fellow group members. Allow everyone a chance to talk, particularly when the group is brainstorming. All ideas are welcome.

4. Disagree only when appropriate. The facilitator, as the neutral party, should encourage active debate but mediate discussions that become adversarial.

5. Keep the discussion focused on the task or issue at hand by allowing only one person to talk at a time, avoiding side conversations, and not interrupting.

FDIC