

CYBER CHALLENGE: A COMMUNITY BANK CYBER EXERCISE

Purpose: The FDIC created “Cyber Challenge: A Community Bank Cyber Exercise” to encourage community financial institutions to discuss operational risk issues and the potential impact of information technology disruptions on common banking functions. The Cyber Challenge provides institutions with the materials necessary to conduct short exercises or facilitated discussions around four operational risk-related scenarios. The Cyber Challenge is not a regulatory requirement; it is a technical assistance product designed to assist with the assessment of operational readiness capabilities.

Background: Financial institutions face a wide variety of risks. Financial institution management is typically well versed in addressing traditional banking risks such as interest rate, liquidity, and credit risk. However, it may be more challenging to address certain operational risks since threats to information technology and related operations of banks are increasing and evolving. Community financial institutions may be exposed to operational risk through any number of internal or external events ranging from cyber attacks to natural disasters. Regardless of the root cause, operational risks can threaten an institution’s ability to conduct basic business operations, impact customer service, and tarnish an institution’s reputation.

Objectives: The Cyber Challenge exercise is designed to facilitate discussion between financial institution management and staff about operational risk issues. The exercise can provide valuable information about an institution’s current state of preparedness and identify opportunities to strengthen resilience to operational risk.

Overview of the Exercise: The Cyber Challenge consists of four short video vignettes and related challenge questions. Each video vignette depicts a unique scenario. The challenge questions for each vignette are designed to facilitate discussion about how the bank would respond to the scenario. Also included are lists of reference materials where participants can obtain additional information.

- Vignette 1 presents an item processing failure scenario. A new item processing service provider cannot process the volume of transactions generated by the bank.
- Vignette 2 presents a customer account takeover where unauthorized withdrawals occur from a corporate customer’s account.
- Vignette 3 presents a phishing and malware problem. A bank employee receives a phishing email that appears to come from the bank president. The employee opens the email, and the bank’s network is infected with malware.
- Vignette 4 presents a problem with the bank’s technology service provider. Problems occur after the financial institution’s service provider performs an update.

Suggested Ground Rules: Participants in the Cyber Challenge should treat it as a data-gathering event and follow a non-attribution policy. Participants may want to record discussion during the exercise to facilitate the compilation of any lessons learned and identification of possible areas for improvement.