

OCTOBER-DECEMBER 2022



Practice Cyber Attack Response for Better Protection

Cyber security is critical every nano-second of every day, and keeping your data, systems and facilities secure takes a multi-pronged strategy encompassing every level of the organization, from network firewalls to employee access to data to customer passwords.

“Cyber security is a lot like a sinking ship with multiple holes – one plug won’t guarantee safety,” says Naomi Bauman, FCCS Director of Claims & Loss Prevention. “And while policyholders may build strong barriers to keep their environment safe, it’s just as important that employees in the office and offsite, and even customers, are practicing good cyber hygiene to keep data and systems secure.” [Click here for guidance to share with your customers.](#)

A cornerstone of an effective cyber security strategy is an Incident Response Plan (IRP) that details exactly who should do and say what in the event of each type of anticipated cyber attack. And since a plan is only useful if it works, and staging a full, simulated attack untenable, the most effective way to test a planned response to a cyber attack is a tabletop exercise.

While it may seem like simple “play-acting,” a cyber tabletop exercise is a comprehensive run-through of a specific scenario, involving all the key individuals who would be involved in a legitimate attack, as detailed in the IRP: risk management, legal, IT, facilities, communications, accounting and others, depending on the plan. After the scenario is completed, an in-depth discussion identifies successes and areas for improvement.

“A cyber tabletop exercise identifies specific improvements to the Incident Response Plan, including addressing new risks identified through the process,” says Naomi. “It also reminds key individuals of the importance of cyber security and prepares them to respond in case of a real attack.”

A cyber tabletop exercise takes four to six weeks to plan, and around half a day to enact. FCCS offers free planning and execution support to members of the Farm Credit Captive Insurance Company, including identifying coverage implications of the IRP, such as not notifying the carrier as quickly as required or engaging an unapproved vendor.

“The Captive’s goal is to help strengthen the cyber security of each association and bank in the System,” says Brian Clanton, FCCS Senior Vice President, Risk Management and Insurance. “Tabletop exercises focus attention on cyber security, even in the midst of regular business pressures or during the complexity of a merger or consolidation.”

“The Captive’s goal is to help strengthen the cyber security of each association and bank in the System.”

— **BRIAN CLANTON**
SVP, RISK MANAGEMENT
AND INSURANCE, FCCS

For more information about cyber tabletop exercises, or coverage provided through the Captive Insurance Company, contact Brian Clanton at 303.721.3281 or [via email](#); or Naomi Bauman at 303.721.3263 or [via email](#).