CYBER ATTACK

3 RESPONSE AND RECOVERY CHALLENGES

Many institutions approach cyber-attacks the same way they would address physical attacks. However, cyber-attacks fundamentally differ from physical attacks in three key ways:

DETECTION: A physical attack occurs as a result of an external, visible event, while a cyber-attack may happen imperceptibly, or as a result of a new attack type that may not be immediately known. In addition, cyberattackers often employ methods to cover their tracks.

RESPONSE: The impact of a physical attack is usually realized immediately after the attack, is contained, and is easy to pinpoint. On the contrary, cyber-attacks have the potential to quickly spread and the full extent of the impact is not immediately clear.

RECOVERY: Recovery from physical attacks can be accelerated through use of alternate processes and back-up applications or geographically diverse data centers. Recovery from a cyber-attack needs to balance speed with potential negative consequences resulting from premature resumption (for example, proliferation of malware to additional internal systems or external partners).

Because of these fundamental differences, many traditional business continuity practices become ineffective in the cyber context. Consequently, response and recovery from a cyber-attack can be more challenging compared to a physical attack.

New White Paper Calls for Expanding Cross-Industry Coordination to Mitigate the Systemic Impact of a Major Cyber Attack on the Financial System

Large-Scale Cyber-Attacks on the Financial System: The Case for Better Coordinated Response and Recovery Strategies.

DTCC
Securing Today. Shaping Tomorrow.®

Click here to read the paper