Aon | Financial Institutions Practice

The New Cyber Risk Environment for Financial Institutions

Listen to the podcast – *Threats, Resilience and Risk Transfer Strategies for FIs* – to access insights from industry experts as they discuss how financial institutions can navigate the rapidly changing cyber risk environment.

Ever-evolving cyber schemes, attacks, malware and ransomware are challenging financial institutions in new ways.

“The tough news on this is that it’s a challenge, a huge challenge,” says Eric Friedberg, co-founder and Co-President of Stroz Friedberg, LLC. “Over the last couple of years there’s been a 500% increase in ransomware alone.”

“As Willie Sutton, the famous bank robber, reportedly said when asked why he robbed banks: ‘that’s where the money is,’” Friedberg explained. “So the financial institution has really been one of the primary industries that have state-sponsored attacks and financially motivated attacks. These attackers are innovating every day.”

Operating environment threats are evolving. The increase in work-from-home arrangements due to the pandemic, and new fintech and digital offerings with changing business models are creating new risks. Add in heightened globalization and geopolitical concerns, and you’ve got an increased “attack surface” in which criminals operate.

The question is not whether outages or failures will happen, according to Friedberg, but how long, how disruptive and how damaging the outage will be.

How are banks and FIs responding?

Firms’ strategies increasingly look beyond a traditional business continuity management program and focus on recovery of assets to the complexity and interconnectivity of their operations. That is, innovative resilience teams are quickly moving from a reactive to a proactive approach, aiming to holistically understand how a disruptive event affects the entire organization including its third parties, both at the point of attack and as it works through the system.

As organizations become more global and interconnected, the future of operational resilience lies in a firm’s ability to mitigate these downstream impacts on not only different divisions within the firm, but also the technologies, third parties, and even fourth parties used by the firm around the world.

Ultimately, banks and other FIs need to invest in cybersecurity infrastructure.

Listen to the podcast **and access the full article on Aon’s Insights Hub.**

Release Date: September 2021

Empower Results®