

CLM 2018 Cyber Liability Summit

Date: October 11-12, 2018

Location: New York City

Decoding the Human Element of Cyber Risk

In this session, we will discuss how organizations can work together to create a cyber-smart workforce and build an effective risk management strategy to guard against catastrophic events. Although technological defenses are the main tactic applied to combat cyber risk, this is not enough to meet the challenges hackers present. The human element or employees of an organization is often the major source of vulnerability that can allow hackers in an organization's front door, regardless of technological defenses in place.

Cyber IQ matters tremendously in battling cyber threats, thus the importance of building a cyber savvy workforce.

Willis Towers Watson 2017 Cyber Risk Survey revealed that 69% of cyberinsurance claims are related to employee-driven incidents. How does it happen? Why does it happen? And how can organizations mitigate this risk? One thing is for certain –cyber risk is not just an IT issue. It permeates an entire organization. As a result, firms need a fully integrated, comprehensive plan for managing people, capital and technology risks across the enterprise.