BUSINESS CONTINUITY PLANNING

Cybersecurity National Action Plan (CNAP) that aims to enhance cybersecurity. Additionally, on February 9, 2016, President Obama announced a new government partners.

Better protect our clients the private sector with President Obama to provide recently signed into law by (CISA) of 2015, which was Information Sharing Act as S. 754, the Cybersecurity legislative measures such insurance policy, provided through DeWitt Stern underwritten by ACE Group.

SIFMA is pleased to offer our members a best-in-class cyber and privacy

HOW WE ACHIEVE MARKET RESILIENCY

Extreme weather like hurricanes, tornadoes, storms, flooding, earthquakes.

POTENTIAL THREATS TO FINANCIAL MARKETS

NATURAL THREATS

Electronic weather/telecommunications/energy/financial infrastructure.

HUMAN THREATS

Cyber attacks, pandemic threats, riots, legal actions.

TECHNICAL THREATS

Data loss, internet loss, power outage.

MANAGING THREATS: HOW WILL WE IMPROVE MARKET RESILIENCY?

In your line of work, you have likely heard the adage: “An ounce of prevention is worth a pound of cure.” While this is a true statement, effective business continuity planning requires more than a strong prevention strategy. Business continuity planning (BCP) is the process of planning for business operations in the event of disruptions. It is critical for all organizations, especially financial markets, to have a solid BCP to ensure that they can continue to operate during unexpected events.

SIFMA is engaged in ongoing discussions with the Department of Homeland Security (DHS) to refine and improve the National Risk Management Standards (NRMS) for the financial sector. SIFMA is also working with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to improve information sharing and collaboration across the financial services industry. These efforts are aimed at strengthening the industry’s ability to manage and respond to threats.

Best practices and exercises:

• SIFMA has been working with the National Cybersecurity and Communications Integration Center (NCCIC) to establish a national incident response framework for the financial services sector. This framework provides a structured approach for managing incidents and coordinating responses across the industry.

• SIFMA is a key participant in the Federal Financial Services Industry Council (FISYSIC), a joint government-industry initiative that focuses on protecting the financial services sector from cyber threats.

• SIFMA has coordinated with government and private organizations to sponsor the Pandemic Influenza Continuity Exercise Series (PICS), a series of exercises designed to test and enhance the industry’s preparedness for pandemic threats.

• SIFMA has also conducted the Quantum Dawn exercises, a series of cybersecurity exercises designed to test incident response capabilities and improve coordination across the industry.

SIFMA is actively engaged in coordinating the effort to support a harmonized framework to align the industry and federal government’s approaches to cybersecurity. SIFMA’s Principles for Effective Regulatory Guidance ask that regulations be risk-based, threat-informed and supportive of the industry’s business model.

SIFMA is working with the Financial Services Technology Council (FSTC) to develop a harmonized framework to align the industry and federal government’s approaches to cybersecurity.

www.sifma.org/bcp

www.sifma.org/cybersecurity

www.sifma.org/mergency