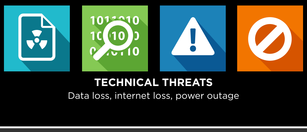
Business Continuity Planning and Cybersecurity for the Financial Industry

Readiness. Response. Recovery.

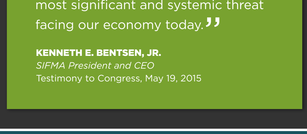
GOAL: IMPROVE MARKET RESILIENCY

SIFMA leads a number of projects and services to help members secure, maintain and recover business operations against disruptions and threats, thereby promoting a safer and more resilient marketplace.

POTENTIAL THREATS TO FINANCIAL MARKETS



NATURAL THREATS
Extreme weather like hurricanes, tornadoes, storms, flooding, earthquakes



HUMAN THREATS
Cyber attacks, pandemic threats, riots

TECHNICAL THREATS
Data loss, internet loss, power outage

> "A large-scale cyber attack is likely the most significant and systemic threat facing our economy today."
>
> **KENNETH E. BENTSEN, JR.**
> *SIFMA President and CEO*
> Testimony to Congress, May 19, 2015

MANAGING THREATS: HOW WE ACHIEVE MARKET RESILIENCY

INFORMATION SHARING

CYBERSECURITY INFORMATION SHARING LEGISLATION (CISA)

SIFMA supports bipartisan legislative measures such as S. 754, the Cybersecurity Information Sharing Act (CISA) of 2015, which was recently signed into law by President Obama to provide the private sector with laws that will enable us to better protect our clients and collaborate with our government partners.

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

SIFMA is actively engaged in coordinating the effort to support a safe, secure information infrastructure, which provides security of customer information and efficient, reliable execution of transactions. SIFMA is continually working with industry and government leaders to identify and communicate cybersecurity best practices for firms of all sizes and capabilities and educate the industry as to the evolving threats and appropriate responses.

PLANNING AND PREPARING

STANDARDS

Principles for Effective Regulatory Guidance

SIFMA has been promoting the use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as a common approach to developing an effective cybersecurity program that is comprehensive, flexible and built on effective standards. SIFMA's Principles ask that regulations be harmonized across agencies for greater effectiveness.

Guidance for Small Firms

Every firm – large or small – has an obligation to be vigilant in our industry's commitment to cybersecurity. SIFMA's Guidance for Small Firms is a summary of guidance to provide small firms with actionable cybersecurity guidance that is risk-based, threat-informed and supportive of their overall business model.

BEST PRACTICES

Insider Threats

SIFMA, leveraging the most effective guidance from both the private and public sector, has created a comprehensive best practices guide to inform firms of insider threats they face and provide a framework to create an effective insider threat mitigation program.

Third Party Risk Management

A consortium of over 50 banks, exchanges, and utilities, along with the top 5 audit firms is working towards streamlining the vendor assessment process by building upon the AICPA SOC-2 criteria, the NIST Cybersecurity Framework and the specific requirements of the industry to create a control framework that is easier to execute, more comprehensive and increases the level of assurance that firms have from their third party providers as it related to cybersecurity.

EXERCISES AND TESTS

Quantum Dawn Exercises

Quantum Dawn is a series of cybersecurity exercises to test incident response, resolution and coordination process for the financial services sector and individual member firms in response to a street-wide cyber attack. Over 650 individuals from approximately 80 entities participated in this year's event. Overall, the industry continues to prove resilient in the face of cyber attacks.

Annual Industry-Wide BCP Tests

SIFMA has coordinated an annual industry-wide test of firms, exchanges and market utilities for over 10 years. This test ensures firms and their providers have connectivity in the event they need to move to back-up systems or facilities. The exercise involved test transactions for equities, options, fixed income, foreign exchange, commercial paper, settlement, payments and market data. The test is supported by all major exchanges, markets and industry utilities. Participants in the SIFMA test included 126 securities firms and 63 market organizations. Approximately 1,056 communications connections were established between securities firms and banks and the exchanges, markets and utilities. Test transactions were successful 98% of the time, underscoring the ability of the securities industry to operate through adverse conditions.

Pandemic Influenza Continuity Exercise Series

SIFMA coordinated with government and private organizations to sponsor a two-year series of pandemic influenza continuity exercises to: mitigate vulnerabilities during a pandemic influenza outbreak; identify gaps or weaknesses in pandemic planning or in organization pandemic influenza continuity plans, policies and procedures; and encourage public and private organizations to jointly plan for, and test, their pandemic influenza plans. The first installment of the exercise was held in November 2013 and had over 500 participants. The second installment was executed in the fall of 2014, covering both firms' internal planning and procedures and developing coordination between the industry and public health authorities.

FS-ISAC PARTICIPATION

SIFMA is increasing participation in the Financial Services Information Sharing and Analysis Center (FS-ISAC), the industry's forum for cyber threat information sharing. SIFMA has funded a one year membership for 181 SIFMA members in the small firm category in order to achieve a near 100% membership overlap with FS-ISAC.

INDUSTRY COMMAND CENTER

SIFMA coordinates market open/close protocols and an Industry Command Center. The Command Center provides a vital forum for information sharing through its relationships with key regulators and government agencies, including a seat at the New York City Office of Emergency Management.

CYBER INSURANCE PROGRAM

SIFMA is pleased to offer our members a best-in-class cyber and privacy insurance policy, provided through DeWitt Stern underwritten by ACE Group.

www.sifma.org/bcp

www.sifma.org/cybersecurity

www.sifmaemergency.org