Press Release

11/12/2017

GFMA Publishes Key Principles for a Commonly Accepted Cybersecurity Penetration Testing Framework

Global Trade Organization Aims to Facilitate Global Regulatory and Industry Coordination on Cybersecurity

HONG KONG, LONDON and WASHINGTON, 11 December 2017 – The Global Financial Markets Association (GFMA) today published a set of principles to guide the development of a commonly accepted framework for cybersecurity penetration testing. In furtherance of our collective goal to increase security and resiliency, and given increased regulatory interest in penetration testing requirements, GFMA's goal is to encourage dialogue and share insights between the industry and regulators that would result in a globally coordinated approach to the regulatory use of penetration testing. Specifically, GFMA aims to facilitate a multi-regulator endorsed approach that enables regulators to drive consistent supervisory objectives and allows firms to maximize the utility and insight of approved penetration testing while minimizing risk.

Penetration testing serves as one of the foremost tools in enabling a robust security program for financial institutions. Such testing allows firms to evaluate their systems and the controls that protect them in order to identify and remediate vulnerabilities, thereby strengthening their infrastructure against cyber threats.

It is clear that the increased use of penetration tests provides a benefit to regulators and financial institutions as part of cyber preparedness. However, this also leads to risks that must be considered, including:

- Multiple regulatory frameworks can result in unnecessary duplication of sensitive information, putting financial firms, their clients, and other downstream third-parties at unknowable risk;
- Testing insights are reduced when regulators narrow options for test personnel and testing methods;
- Increasing regulatory demands requires testing teams spend more time complying with requests, reducing efficiency gains that could be better used increasing security of the sector, business partners, the supply chain and operational controls;
- Multiple regulatory frameworks can result in inconsistent reporting and the inability to develop a credible assessment of the sector due to lack of comparability;
- Penetration testing of critical systems in production creates the significant potential to disrupt firm operations; and

- Creation of multiple one-size-fits-all penetration testing frameworks disproportionately impacts midsize and smaller financial institutions.

A number of jurisdictions around the world already leverage penetration testing in their regulatory regime. The goal of the GFMA proposal is not to compete with existing frameworks but rather to coordinate their development and use to ensure that financial institutions are able to safely, securely and efficiently comply with their supervisory requirements. The GFMA penetration testing framework is similarly aligned with the G-7's broader recommendations on how institutions can conduct effective cybersecurity assessments, promoting safe and effective testing methods.

The industry needs a flexible coordination framework established to perform realistic and rigorous penetration tests in a meaningful and efficient manner. GFMA's principles for a commonly accepted penetration testing approach include:

- Provide regulators the ability to guide penetration testing programs, based on recent threat intelligence, to meet supervisory objectives through the use of common risk-based scenarios and agreed upon scheduling and scoping of testing activities;
- Provide regulators high confidence that penetration testing is conducted by trained, certified personnel with sophisticated tools and techniques to accurately emulate adversaries;
- Provide regulators transparency into financial firm governance processes to provide assurance that identified weaknesses are properly addressed;
- Ensure testing activities are conducted in a manner that minimizes operational risks; and
- Ensure data security by adhering to strict protocols for handling test results data due to the highly sensitive nature of this information.

"The development of a global penetration testing coordination framework can address the respective needs of regulators and the financial industry, allowing for the continued confidence and growth of the world's financial markets and economy," said Mark Austen, chief executive officer of GFMA and chief executive officer of ASIFMA. "We hope these principles provide a foundation for continued dialogue and engagement between the public and private sector, and look forward to input from our regulators. The industry continues to believe that regulatory harmonization is critical to efficient and effective cybersecurity."

As first steps in the process, the industry suggests:

- Agreeing upon independent governance and assurance standards sponsored by an existing, identified voluntary international industry consensus standards body;
- Identifying qualification standards to rigorously certify individual assessors, teams of assessors and assessor organizations, all of which are equally accessible for in-house resources as well as third-party vendors; and
- Identifying quality standards for the technical delivery, evidence collection and reporting for all associated assessment methodologies to ensure they are performed to appropriate levels.

The full Principles document is available here: http://gfma.org/uploadedFiles/News/GFMA_in_the_News/2017/GFMA-Penetration-Testing-Principles.pdf.

-ENDS-

Contact

Corliss Ruggles	+852 9359 6996	cruggles@asifma.org
Rebecca Hansford	+ 44 (0)20 3828 2693	rebecca.hansford@afme.eu
Liz Pierce	+1 (212) 313-1173	lpierce@sifma.org

Notes:

1. The Global Financial Markets Association (GFMA) brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, visit http://www.gfma.org.