Key Principles for a Commonly Accepted Penetration Testing Framework

Penetration testing serves as one of the foremost tools in enabling a robust security program within a financial institution. 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. Increased interest by global regulators, however, has led to the creation of many regulator-guided penetration testing initiatives. Though the benefits of penetration testing remain significant, increased public sector involvement may unintentionally increase or exacerbate various risks, including the release of sensitive information to multiple parties, and narrowing firm testing options.

Regulators globally are showing increased interest in penetration testing and other operational assessments such as network scanning and external monitoring of cybersecurity defenses. Such testing is a powerful tool to assess the success of financial institutions in safeguarding customers' data as well as infrastructure critical to the global economy. Regulatory bodies have a vested interest in the execution of the most realistic and rigorous assessments which utilize proven methodologies and yield unbiased data concerning the strengths and weaknesses of a particular firm's defenses. As a result, financial services firms, especially those which operate globally, are faced with an ever increasing demand by regulators for technical insights into how they protect their customers' data, infrastructure and the results of conducted tests.

Risks Posed by Public Sector Involvement in Penetration Testing

Regulatory compliance provides stability and confidence in financial markets that underpins the global economy; as such, the financial services industry has supported regulators' assessing and reviewing of cybersecurity programs. As the need for maintaining a robust cybersecurity defense system has grown, penetration tests and other operational assessments are becoming more focused on the systems themselves, rather than the controls around them, and have grown more complex, thus providing more granular data on firms' infrastructure and security posture. It is clear that the increased use of penetration tests, as well as the depth of the tests, provides a benefit to regulators. However, this

presents a risk to the firms and the firms' clients if the results become public or are inadvertently disclosed or stolen. Additionally, the increased use of disparate, possibly duplicative and prescriptive penetration testing methods and frameworks around the world demands increased resources within the industry to respond appropriately to each and every test; these required resources could be used more efficiently to protect firms and their clients. There are many substantial risks posed by the current state of affairs:

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

A viable approach is needed to address the regulators' need to evaluate security, while satisfying institutions' need to minimize risk as their cyber defenses and infrastructure are tested. The public and private sectors each have an interest in not overwhelming security teams with concurrent requirements, and instead benefit by leveraging testing results to satisfy multiple purposes.

Cooperation between regulators and the industry will promote a safe, scalable and robust testing regime that is supportive of the evolving rules of multiple regulators, without introducing or exacerbating inherent operational and data risks. Regulators need to be provided with high confidence that the industry is meeting regulatory requirements through transparency in all phases. The industry needs a flexible framework established to perform realistic and rigorous penetration tests in a meaningful and efficient manner.

Principles for a Common Framework

The development of a global testing 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. The establishment of a commonly accepted penetration testing framework based on the principles laid out below will minimize risk to financial institutions while enabling the industry and regulators to maximize the benefits of penetration testing. To minimize risks, financial firms would:

- 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.
- Ensure data security by adhering to strict protocols for handling test results data due to the highly sensitive nature of this information.

Conclusion and Next Steps

The industry seeks to actively engage with global regulators to establish a dialogue on developing a commonly accepted framework and recommended procedures for regulatory-guided, firm-led penetration testing. 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.

Our goal is a multi-regulator endorsed framework that enables regulators and firms to maximize the utility and insight of approved penetration testing. We seek to engage the appropriate regulators in the process of defining an acceptable and effective approach.

We look forward to initiating dialogues with regulators internationally to discuss this increasingly pertinent and important topic within the financial services industry.