Regulatory-Mandated Third-Party Penetration Testing

Introduction

In light of the ever-growing cyber threat posed by nation-states, terrorist organizations, and independent criminal actors, we, the undersigned trade associations (the "Trade Associations"), are committed to working with regulators to promote cooperation and stability by developing secure cyber defenses to protect the financial sector. We would like to take this opportunity to open a dialogue concerning the recent regulatory trend toward government and agency-mandated third-party penetration testing ("pen testing"), and red team exercises ("red teaming") within the financial services industry.

NIST (the "National Institute of Standards and Technology")[1] defines pen testing as "[a] test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system."[2] The purpose of a penetration test ("pen test") is to determine the ways in which identified vulnerabilities may be exploited.[3] A penetration tester ("pen tester"), whether internal or external, will attempt to gain access to resources "without knowledge of requisite user names, passwords, and other normal means of access."[4]

Pen testing is frequently supplemented by red teaming. NIST defines red teaming as an actual "simulated adversarial attempt" to compromise organizational functions, in order to create a comprehensive assessment of the target institution's true state of security.[5] Red teaming may include attempts to "compromise organizational missions and business functions" utilizing either technology-focused attacks or social-engineering-focused attacks.[6]

Over the past three years, there has been a consistent trend, globally, of announcements and releases by various regulators, detailed in the Current State of Affairs section below, regarding pen testing. The sector

[1] NIST is a non-regulatory federal agency within the U.S. Department of Commerce, whose mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology." See: NIST, NIST General Information, http://www.nist.gov/public_affairs/general_information.cfm

[2] NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, rev. 4 ("NIST SP 800-53"), Control RA-5

[3] Security Standards Council, PCI-DSS Information Supplement: Penetration Testing Guidance, Mar. 2015 ("PCI-DSS Penetration Testing"), p. 3

[4] SANS Institute InfoSec Reading Room, Penetration Testing: Assessing Your Overall Security Before Attackers Do, ("SANS Penetration Testing"), p. 3

[5] NIST SP 800-53, Control CA-8, See: https://web.nvd.nist.gov/view/800-53/Rev4/control?controlName=CA-8

[6] Technology-focused attacks can include: interactions with hardware, software, or firmware components, and/or mission/business process. Social engineering-focused attacks can include: interactions via email, telephone, shoulder surfing, or personal conversations. See: Id.

has long supported conducting assessments of this type as long as they strike the right balance of disclosure, oversight, protection of sensitive data and real risk-reduction. We write today in an effort to raise awareness of the growing trend, prompt an important dialogue, and work to find the appropriate balance, structure and methodology where we are able to jointly identify and reduce risk to the financial sector.

Current State of Affairs

United Kingdom

In 2013, the Financial Policy Committee (the "FPC"), an official committee of the Bank of England ("BoE") entrusted with monitoring the economy of the United Kingdom (the "UK"), issued a recommendation requesting that Her Majesty's Treasury ("HMT")[7] and national regulators work with the private sector to create a program to improve and test cyber resilience. In response, BoE, FPC, and HMT worked with the Council of Registered Ethical Security Testers ("CREST"), the UK's nonprofit representative of the technical information security industry to launch the CBEST Framework ("CBEST") at a BoE-sponsored event in 2014. CBEST is a framework intended to deliver controlled intelligence-led cybersecurity tests, which "replicate behaviours of threat actors, assessed by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions."[8]

Under CBEST, pen testing is carried out by BoE-approved vendors[9] who must demonstrate, via written application to BoE: (1) CREST membership; (2) personnel qualifications; (3) personnel experience; and (4) verifiable references.[10] Of particular note is the fact that not only is pen testing by third-party vendors mandatory for institutions implementing CBEST, but BoE is directly integrated in the entire testing process. The tests are conducted in partnership with the entity's regulator[11], CBEST is maintained by BoE[12], and the entire testing process takes about six months.[13] After the launch of CBEST, experts identified 35 "core" firms and financial market infrastructures ("FMIs"), and testing was "offered"[14] to these institutions.[15] According to BoE, CBEST remains a voluntary program, but if a firm or FMI decides against participation, their regulator will "assess each case individually and follow-up accordingly."[16]

---

[7] HMT is the United Kingdom's economic and finance ministry, "maintaining control over public spending, setting the direction of the UK's economic policy and working to achieve strong and sustainable economic growth." See: What we do, https://www.gov.uk/government/organisations/hm-treasury

[8] CREST, An Introduction to CBEST, ("CBEST Introduction"), p. 1

[9] The following vendors have been assessed against the CBEST criteria and have been CREST approved to supply CBEST penetration testing services: Context Information Security Ltd, Deloitte LLP, Gotham Digital Science Ltd, MWR Infosecurity Ltd, NCC Group, Nettitude Ltd, Pen Test Partners LLP, Portcullis Computer Security Ltd, PwC, and SECFORCE Ltd. See: Members Supplying CBEST Approved Services, http://crest-approved.org/crest-member-companies/members-supplying-cbest-services/index.html

[10] Bank of England, CFTC Briefing 2 June 2015: Cybersecurity Considering Bank of England's CBEST Program, ("CFTC Briefing"), p. 7

[11] Id. at 5

[12] Id. at 9

[13] Id. at 12

[14] Bank of England, Bank of England 2015 Financial Stability Report 37, Section 6, ("BoE 2015 FSR Section 6"), p. 32, See http://www.bankofengland.co.uk/publications/Documents/fsr/2015/fsr37sec6.pdf

[15] Bank of England, CBEST FAQ, June 2015 ("CBEST FAQ"), p. 1

[16] Regulators are nearly at the point of requiring major financial services companies to participate in a cybersecurity testing programme…Directors expressed concern that CBEST testing remained voluntary…that was the formal position, but the supervisors were making participation a clear expectation and in practice it was becoming close to mandatory for the bigger firms." See: The Register, UK Finance Sector: IT Security Testing 'Becoming Close to Mandatory' – Voluntary In Name Only, October 30th, 2015, http://www.theregister.co.uk/2015/10/30/uk_financial_sector_mandatory_cyber_security_testing

United States

In November of 2015, the New York State Department of Financial Services (the "NYDFS"), the New York State government department responsible for regulating financial services and products, issued a letter (the "NYDFS Letter") to members of the Financial and Banking Information Infrastructure Committee (the "FBIIC")[17] concerning potential new regulations aimed at increasing cybersecurity defenses within the financial sector.[18] The NYDFS Letter states that covered entities would be required to implement and maintain written cybersecurity policies relating to twelve named areas including vendor and third-party service provider management.[19] Further, the NYDFS Letter proposes an audit requirement, whereby covered entities would conduct annual pen testing.[20] However, there is no mention of mandatory testing conducted by third-parties.

In December of 2015, the Commodity Futures Trading Commission (the "CFTC"), an independent government agency tasked with regulating the futures and options markets in the United States (the "US") announced a notice of proposed rulemaking (the "Proposals")[21], which would require annual third-party pen testing by derivatives clearing organizations, covered designated contract markets, and swaps data repositories.[22]

In August of 2015, the National Futures Association (the "NFA") released an Interpretive Notice regarding Information Systems Security Programs (the "NFA Interpretive Notice"), which recommends a principles-based approach to pen testing, wherein a NFA member firm may include pen testing of firm systems, dependent upon that firm's size, business, technology, electronic interconnectivity with other entities, and potential threats identified in its risk assessment.[23]

Finally, FINRA noted in its 2015 Report on Cybersecurity Practices (the "FINRA Report"), "[a]n advanced persistent attack may involve an outsider gaining a progressively greater foothold in a firm's environment, effectively becoming an insider in the process. For this reason, it is important to perform pen testing against both external and internal interfaces and systems."[24]

---

[17] Members of the FBIIC include: Federal Reserve Board of Governors; Office of the Comptroller of the Currency (OCC); Commodities Futures Trading Commission (CFTC); U.S. Department of the Treasury; Securities and Exchange Commission (SEC); Federal Deposit Insurance Commission (FDIC); Federal Housing Finance Agency (FHFA); Consumer Financial Protection Bureau (CFPB); National Credit Union Administration (NCUA); Federal Reserve Bank of New York (FRBNY); Federal Reserve Bank of Chicago; National Association of Insurance Commissioner (NAIC); Conference of State Bank Supervisors (CSBS); American Council of State Savings Supervisors; Farm Credit Administration (FCA); National Association of State Credit Union Supervisors (NASCUS); North American Securities Administrators Association (NASAA); Securities Investor Protection Corporation (SIPC)

[18] New York State Department of Financial Services, Re: Potential New NYDFS Cyber Security Regulation Requirements, ("NYDFS Letter") p. 1

[19] Id. at 3

[20] Id. at 4

[21] Commodity Futures Trading Commission, Q&A – Notice of Proposed Rulemaking on System Safeguards Testing Requirements, ("CFTC Rulemaking Q&A"), p. 1, See: http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/syssafeguard_qa121615.pdf

[22] Commodity Futures Trading Commission: 17 CFR Part 39, System Safeguards Testing Requirements for Derivatives Clearing Associations, ("CFTC Proposal") p. 13

[23] National Futures Association, 9070 – NFA Compliance Rules 2-9, 2-36 AND 2-49: Information Security Programs, ("NFA Interpretive Notice"), See: https://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9

[24] FINRA, Report on Cybersecurity Practices, Feb. 2015 ("FINRA Report"), p. 1-2

Hong Kong

In July of 2000, the Hong Kong Monetary Authority ("HKMA"), Hong Kong's currency board and central bank, released a guidance note (the "Guidance Note") concerning recommended and mandated practices for Authorized Institutions[25] ("AIs") on managing security risks in electronic banking ("e-banking") services. HKMA states their expectation that independent assessments of an AI's e-banking services security before launch of said services, and at least annual assessments thereafter.[26] The Guidance Note asks firms offering higher risk e-banking services to "consider" including pen testing as a part of their independent assessment.[27]

In May of 2016, the HKMA announced the launch of a Cyber Security Fortification Initiative (the "CFI") at the Cyber Security Summit 2016, and initiated a limited release of the CFI to AIs and other organizations, beginning a three month comment period (the "Draft CFI"). The Draft CFI is a new, comprehensive cybersecurity initiative designed to increase cyber preparedness of banks in Hong Kong via a three-pronged approach: (1) a Cyber Resilience Assessment Framework[28] (the "CFI Framework"); (2) a Professional Development Programme (the "CFI Programme"); and (3) a piece of infrastructure named the Cyber Intelligence Sharing Platform (the "CFI Platform"). [29]

The CFI Framework is shaped by three components: (1) an inherent risk assessment; (2) a maturity assessment; and (3) intelligence-led cyber attack simulation testing (iCAST)."[30] In addition to traditional pen testing, the iCAST component of the CFI will require AIs to engage in intelligence-led simulated cyber test scenarios designed to replicate current real life attacks.[31] At a bare minimum: (1) AIs must undergo independent pen and vulnerability testing; and (2) iCAST assessors and testers must be "competent, qualified and independent."[32] The Draft CFI states that an "independent team" is one which is either an "external consultant" or a colleague "representing an independent internal function."[33] It further states that an "independent assessor" is one which "should be independent from the business units and IT functions being assessed."[34]

Singapore

In May of 2014, the Monetary Authority of Singapore (the "MAS"), Singapore's central bank and financial regulatory authority, released a circular notice (the "Circular Notice") addressed to the CEOs of all financial

---

[25] An "authorized institution" as recognized by the HKMA is "an institution authorized under the Banking Ordinances to carry on the business of taking deposits. Authorized institutions are supervised by the HKMA." See: Hong Kong Monetary Authority, Guide to Hong Kong Monetary and Banking Terms, http://www.hkma.gov.hk/gdbook/eng/a/authorized_institut.htm

[26] Hong Kong Monetary Authority: a Guidance Note, Management of Security Risks in Electronic Banking Services, ("Guidance Note") p. 5

[27] Id. at 5

[28] See: CFI Letter p. 3

[29] The CFI Framework seeks to "establish a common risk-based framework for banks to assess their own risk profiles and determine the level of defense and resilience required;" the CFI Programme is a "training and certification programme…which aims to increase the supply of qualified professionals in cybersecurity;" and the CFI Platform will "allow sharing of cyber threat intelligence among banks…", See: CFI Press Release

[30] Hong Kong Monetary Authority: Letter, HKMA Cybersecurity Fortification Initiative, ("HKMA CFI Letter"), p. 3

[31] Id. at 3

[32] Hong Kong Monetary Authority, Cyber Resilience Assessment Framework: Consultation Draft, ("Draft CFI"), p. 30

[33] Id. at 5

[34] Id. at 30

institutions concerning vulnerability assessments and pen testing.[35] Under the Circular Notice, financial institutions are required to perform at least annual pen tests on their internet facing systems, and may outsource testing activities, so long as outsourcing does not result in weakening or degradation of the institution's control over their outsourced activities.[36]

In July of 2015, the Association of Banks in Singapore (the "ABS") released "Penetration Testing Guidelines for the Financial Industry in Singapore" (the "ABS Guidelines"), which are mandatory for online systems publicly accessible from the Internet, and optional for non-Internet facing services.[37] The ABS Guidelines mandate that testing is carried out by an "independent party" which may be a third-party vendor, or an independent tester within the organization.[38]

In May of 2016, MAS attended the 2016 annual Hong Kong Cybersecurity Summit, and both MAS, and HKMA expressed concern that pen testing approaches generally do not reflect authentic cyber attacks and scenarios, and that threat actors may know which controls have been tested, allowing them to focus on other areas of attack.

Challenges and Opportunities

The regulatory interest and movement toward pen testing, and red teaming, is a welcomed and important evolution in understanding risk. Pen testing is one control, out of many, that form a solid foundation of a sound information security assessment program which informs the governance structure within financial entities of their current security posture. As a result, it is critical that the public and private sectors are able to work together, globally, to understand drivers, focus approaches, and requirements. The lack of a unified approach could have adverse consequences, such as:

- Multiple regulatory models may invariably result in inconsistent examinations and results. Where multiple regulators have concurrent vested interest in the same critical economic function, or the supporting systems and business practices, it is imperative that these be harmonized to achieve scale efficiencies, rather than a conflicting agenda which may give rise to fatigue amongst targeted financial institutions as well as an inaccurate picture of their cybersecurity capabilities.
- Initial assessments by regulators have taken up to six months to complete. Conforming to numerous such examinations of such a length of time would excessively burden firm resources by diverting important key talent and resources away from protection activities. Further, the execution of multiple tests of this magnitude has the potential to disrupt regular business, protection, and testing activities.
- Prescriptive assessments with a narrow set of security firms to choose from to conduct pen testing taxes the systems and resources of those companies, as well as creating delays for financial institutions. Overly stringent requirements and limited set of firms can also inadvertently limit the range of attack vectors investigated and stifle institutions' ability to keep pace with the ever evolving threat landscape.
- Regulations which create a closed-class of contractors limit firm choice and may inadvertently increase the cost of services, which can be particularly burdensome for smaller institutions.

[35] Monetary Authority of Singapore: Circular No. SRD TR 01/2014, System Vulnerability Assessments and Penetration Testing, ("Circular Notice") p. 1
[36] Id. at 1-2
[37] The Association of Banks in Singapore, Penetration Testing Guidelines for the Financial Industry in Singapore, ("ABS Guidelines"), p. 3
[38] Id. at 10

- Pen testing and red teaming initiated by a third-party vendor creates a scenario wherein those parties may become threat actor targets for a breach, which, inadvertently, may put a firm and customer information at risk. In addition to firm and customer privacy considerations, firm employee data is also at risk in this scenario. Increasing the number of regulators adopting third-party vendor scenarios increases the number of weak points within the sector's information security infrastructure.

The Associations note that certain authorities do not require pen testing, based upon the size and systemic importance of the financial institution. The Associations support this approach, whereby pen testing requirements are dependent on a financial institution's risk profile, as determined by factors including the entity's size, business, technology, interconnectivity with other entities, and potential threats.

Next Steps

The Associations are committed to working with regulators and governments globally to develop and encourage pen testing approaches and best practices. In furtherance of this goal, we would like to collaborate with our regulator and government partners to discuss the following:

1) Working toward a harmonized pen testing approach jointly developed with the industry, comprised of principles and best practice guidance on satisfying regulator pen testing requirements. [39]
2) Allowing firms to share results from standardized pen tests with multiple regulatory authorities, where appropriate, in order to reduce the need for firms to undertake multiple rounds of duplicative pen tests for different authorities. Recognizing the sensitivity of pen testing results, sharing of critical information about a firm's processes and vulnerabilities should be treated as highly confidential, and may include regulatory authorities reviewing pen testing results on firm premises to ensure limited circulation of results.[40]
3) Allowing firms with robust in-house pen testing or red teaming capabilities or firms who outsource to recognized third-party vendors, to continue to utilize their existing program, while further giving said firms the option to enhance those programs through alignment with the agreed upon harmonized pen testing approach, and the inclusion of critical systems of interest/importance to the corresponding regulator.
4) Offering financial firms which comply with government-mandated pen testing a safe-harbor, or some other form of liability protection.

We are encouraged by the increasing focus regulators and governments from around the world are placing on information security. True information security is a shared responsibility that requires dialogue and collaboration between regulators, government entities and the financial sector. As such, we look forward to working together and achieving a mutually satisfying outcome on this important topic.

[39] By creating a harmonized pen testing standard as discussed herein, firms can ensure they are abiding by industry and regulator-mandated best practices, and avoid duplication of effort.

[40] A cross-regulator agreed harmonized framework should also cover quality assurance standards applicable to the cyber assessment being undertaken in terms of people (skills and experience), process (test methods and risk management practice), and technology.