Vendor Risk Management

CFTC Technology Advisory Committee

October 2019

Background

- The sophistication, frequency, and scale of cyber attacks against the financial services sector has moved resiliency to the top of the risk management agenda
- The financial services sector continues to be disrupted by new entrants that provide niche products to financial firms and consumers
- There is a shift from a system-centric view (e.g., system uptime) to a service-centric view (e.g., product and services delivery) which requires resiliency to be implemented throughout the supply chain
- The current approach to managing vendor risks may not be optimally designed to ensure resiliency through the supply chain
- The Subcommittee will provide a new approach to consider to create an ***equitable risk balance*** between the financial institution and the third party vendor

Threats Facing the Financial Services Sector[1]

While there are numerous threats facing the Financial Services Sector, there are three (3) primary threats that face the Sector

- **Geopolitical impacts**

  Political shifts between and within nation states and changes to domestic and foreign policy have led to sanctions, conflicts, and civil outbreaks. The inability to provide attribution to certain attacks may lead to these attacks becoming more prevalent when other diplomatic measures fail to produce the desired results

- **New Technology / Digitalization**

  The speed of new technology drives innovation within the Sector. Cloud, block chain, robotics, and AI are seen as vehicles to lower costs, improve products and product delivery and increase risk management opportunities. Given the pressures of disruption, firms may feel pressure to adopt new tech too fast or legacy systems may prevent adoption

- **EXPANSION OF THE SUPPLY CHAIN**

  The expansion of the supply chain allows firms to optimize costs and provides them with opportunities to introduce new, innovative solutions to the marketplace. The increased reliance on third and fourth parties increase the possible attack surface against the Sector

[1]More information regarding these threats may be found on the World Federation Of Exchanges at: https://focus.world-exchanges.org/articles/cyber-risks-threats-new-frontier

The Rise Of Operational Resiliency

RESILIENCY

The practices and disciplines that enable firms to provide products and services to the marketplace in the face of disruptive events, regardless of the nature or origin of such events by anticipating, preventing, recovering from, and adapting to such events

- Several supervisors have begun to communicate with the Sector through supervisory documents on its view to Resiliency
  - **UK Bank Of England/FCA/PRA:** *Building the UK Financial Sector's Operational Resilience*
  - **Monetary Authority of Singapore:** *TRM Guidelines*
  - **Australian Securities and Investments Commission:** *Market Integrity Rules For Technological and Operational Resilience*

- Additionally standard setting bodies (e.g., G7 Cyber Working Group, IOSCO, FSB) are identifying opportunities to support the Sector in its resiliency efforts

- To achieve the goal of Resiliency, a ***service-centric approach*** of providing products and services must be taken and requires firms and their supervisors to ensure resiliency through the supply chain (i.e., vendors)

Current Vendor Management Supervisory Documents

- Current Supervisory Documents have requirements covering all vendors in use by a firm or FMI to guidance and controls specific to Critical Vendors

- The specificity of Supervisory Documents range from general guidelines (e.g., FRB Guidance on Managing Outsourcing Risks) to granular control requirements (e.g., OCC Third Party Relationships Risk Management Guidance)

- ***Supervisory Documents***[1] cover the vendor management lifecycle[2] and includes the following risk areas:
  - Planning
  - **DUE DILIGENCE AND 3RD PARTY SELECTION**
  - **CONTRACT NEGOTIATION**
  - **ONGOING MONITORING**
  - Oversight and Accountability
  - Termination
  - Documentation and Reporting
  - Independent Review
  - Supervisory Review of Technology Service Providers

- The different breadth and depth of the requirements have created several approaches taken by financial firms to meet the varying requirements

[1]A list of the reviewed third party guidance documents reviewed as part of this review are located in the Appendix.
[2]The definition of each phase of the lifecycle can be found in the Appendix

Current Vendor Management Challenges

- **Risk Visibility / Questionnaire Fatigue**

Questionnaires used to gather information from vendors are susceptible to (1) question misinterpretation (2) Yes/No answers that provide limited context to the risk being mitigated

- **Compliance to Multiple Firm Policies and Standards**

Each financial firm has its own policies and standard with which it requires compliance. Vendors with multiple financial clients cannot meet each firms cybersecurity policies and standards

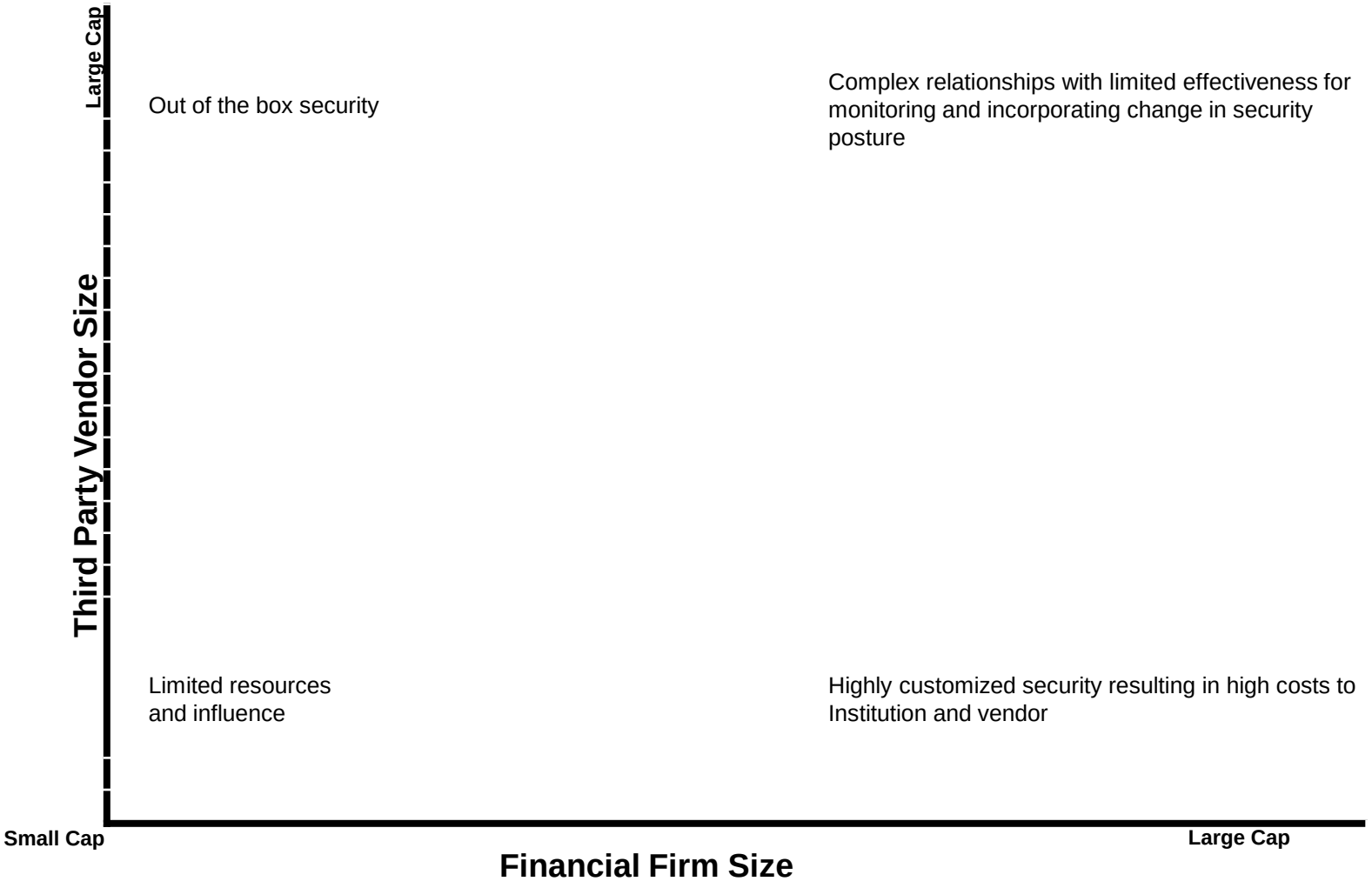
- **Intellectual Property (IP) Protection**

Vendors may be hesitant to disclose technical details or design vulnerabilities of their applications/services as this information may negatively impact their IP used to expose the application/service to attack

- **Contractual Leverage**

There is an uneven contractual leverage between small and large vendors and small and large financial firms

Vendor vs Financial Firm Relationship – Contractual Challenges



Vendor Management Potential New Approaches

Given the challenges with the current model of vendor management, ***the subcommittee should consider a different approach to vendor management***

- **INDUSTRY CERTIFICATION**

Vendors that engage in business with the financial services sector need to be certified or accredited against a recognized, industry standard where the requirements and frequency of the certification is dependent on the size of the vendor and the level of risk that is inherent to the financial marketplace

BENEFITS

- Reduce Questionnaire Fatigue from firms and vendors
- Common agreed industry certification harmonizes the requirements from multiple firms
- Simplifies Contractual Language relative to cybersecurity
- Provides a greater level of resiliency assurance than the current vendor management model

CHALLENGES

- Requires a high level of collaboration between firms, vendors, supervisors and standards setting bodies

APPENDIX

Vendor Management Supervisor Documents

Federal Reserve Board: Guidance on Managing Outsourcing Risk

Office of the Comptroller of the Currency: Third Party Relationships Guidance

Bureau Of Consumer Financial Protection: Bulletin on Service Providers

Committee On Payment and Settlement Systems: Assessment Methodology For The Oversight Expectations Applicable To Critical Service Providers

FFIEC IT Handbook: Supervision of Technology Service Providers

FINRA Regulatory Notice 11-14: Third Party Service Providers

Investment Industry Regulatory Organization of Canada: Outsourcing Arrangements

IOSCO: Principles Of Outsourcing PD 187

Investment Company Institute: Financial Intermediary Controls and Compliance Assessment Engagements

Federal Reserve SR 14-1: Principles and Practices For Recovery and Resolution Preparedness

Financial Conduct Authority (FCA): Outsourcing In The Asset Management Industry

SEC Risk Alert: OCIE Cybersecurity Initiative

New York State Department Of Financial Services: Cybersecurity Requirements For Financial Services Companies

Monetary Authority Of Singapore: Guidelines On Outsourcing

FFIEC Information Security Handbook

FCA: Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services

European Banking Authority: Guidelines On Outsourcing Arrangements

Vendor Risk Management Lifecycle Phases and Definitions

Vendor Risk Management Phases	Definition
Planning	The plan used to manage the vendor relationship and the first step of the vendor risk management process
Due Diligence and Third Party Selection	The reviews conducted prior to signing the contact to ensure that the firm understand and controls the risks posed by the relationship
Contract Negotiation	Development of a contract that defines the expectations and responsibilities of the 3rd Party, limits the firms liability and mitigates performance disputes
Ongoing Monitoring	The activities that are used to provide oversight of the vendor during the course of the contract
Termination	Development of a contingency plan to ensure that the firm can transition the activities to another 3rd party, bring the activities in-house, or discontinue the activities when a contract expires
Oversight and Accountability	Assigning clear roles and responsibilities for managing 3rd party relationships
Documentation and Reporting	Proper documentation and reporting facilitates oversight, accountability, monitoring and risk management with 3rd party relationships
Independent Reviews	Conducting periodic independent reviews of the risk management process enables management to assess whether the process aligns with the firm's strategy and effectively manages risk