TAC CYBERSECURITY SUBCOMMITTEE

CLOUD RECOMMENDATIONS

CONTEXT

"Cyber security is critically important to protecting infrastructure and financial markets around the world. I feel strongly that it is the most important single issue facing our markets today in terms of market integrity and financial stability."

Chairman Giancarlo, May 2018 testimony before House Appropriations Committee

- CFTC maintains robust cybersecurity regulation based on strong principles applied by member firms in various environments
- Cloud based Infrastructure as a Service (IaaS) is a growing trend for member firms, creating new challenges in a shared-responsibilities environment
- With the adoption of Cloud based platforms, as member firms, we want to continue to work closely with CFTC to evolve cybersecurity practices and ensure relevance in a forward looking environment
  - The same cybersecurity requirements will apply, as supported by FSSCC Cybersecurity Profile; however, they may be implemented in different ways
- The following recommendations should be considered for CFTC cybersecurity exam priorities, new member questionnaire, and to inform thinking on the next generation of system safeguards

SAME CONTROLS, DIFFERENT IMPLEMENTATION

Responsibility	SaaS	PaaS	IaaS	On-prem	
Data management and rights management					Always retained by customer
Client endpoints					
Account and access management					
Identity and directory infrastructure					Varies by Service Type
Application					
Network controls					
Operating system					
Physical hosts					Transfers to Cloud Provider
Physical network					
Physical datacenter					

Cloud Provider | Customer | Software as a Service | Platform as a Service | Infrastructure as a Service

PREPARING FOR CLOUD MIGRATION: INFRASTRUCTURE

- Adoption should be executed using a thoughtful and deliberate approach. Speed is not necessarily your friend when moving into a shared-responsibilities environment, especially with regulated apps and data.

- A strong foundation (infrastructure) prior to migrating services is necessary and minimally include:
  - Data protection and encryption
  - Service and application segmentation
  - Intrusion Detection and Prevention (IDS/IPS) capabilities
  - Security information and event management (SIEM)
  - Vulnerability Management Strategy - Inventory tracking (CMDB)

PREPARING FOR CLOUD MIGRATION: AUTHENTICATION, AUTHORIZATION

- Proper authentication and authorization controls required include:
  - Federation for authentication (e.g. SAML)
  - Role Based Access (RBAC) for service enablement and consumption
  - “Least Privilege” model
  - Ephemeral credentialing
  - Just in time, logged access

PREPARING FOR CLOUD MIGRATION: DEPLOYMENT STRATEGIES

- New service strategies should be considered, including:
  - Containerization, to help reduce vendor lock-in
  - Application and service re-architecture (Micro/Mini services)
  - Full automation of deployment and environmental builds.
    - Remember cloud services are infrastructure as code!

PREPARING FOR CLOUD MIGRATION: GOVERNANCE

- Verify the providers processes, procedures, and security.
  - A Cloud deployment is a shared responsibility, built on the foundation of your provider.
  - The provider's environment, processes, and procedures will suffice for their auditors and regulators; however, those guarantees are not transitive to your regulators' requirements.
    - For example, just because the provider is PCI-certified, that would only apply to their underlying environment. What you build is your responsibility.
- Finally, ensure proper governance has been implemented around the adoption effort, including but not limited to:
  - A plan to review new services and security capabilities. Remember that the environment and services offered are not static in nature.
  - A plan to re-review existing services and security capabilities around them.
  - Development of Critical Standards, e.g. Network Segmentation, IDS/IPS, Micro-Services, IAM, Availability and Business Continuity (to name a few)
  - Access approval & review SOPs

GOVERNANCE: PHYSICAL INFRASTRUCTURE & THIRD PARTIES

- Control of physical infrastructure
  - It can be difficult to know where the physical machines reside, let alone who, specifically, can access them. If physical access is a threat vector for your specific context, consider mitigations using means like encryption.
- Operational resiliency planning should consider 3rd-party dependencies
  - Just because a service is “in the cloud”, doesn’t necessarily mean it’s guaranteed to provide DR and HA. As applicable, special efforts should be made to understand what the provider guarantees in this context. Further, the function of the service requires the vendor (and their chosen cloud platform) to be up and running. Your HA and DR plans should address the risk of your provider having an outage, or going out of business.

GOVERNANCE: DATA AND DATABASES

- Ensure you understand the providers' capability and the risks (e.g., lack of Database Activity Monitoring (DAM)
- Monitoring of access to data.
  - It is a good idea to analyze the data expected to flow through the cloud, specifically to ascertain adequate protections of confidential information and information barriers. You should understand what members of the provider's team might have access your data, and what auditing capabilities you have of such access.
- Removal of data.
  - It is a good idea to understand whether data can be guaranteed removed from the cloud provider. Specifically, helps with GDPR compliance.

VENDOR MANAGEMENT: PROVIDER INDEPENDENCE

- If using a cloud product, it's often good to ensure that:
  - An equivalent open-source version of that product is available (example: Amazon RDS can use PostgreSQL or MySQL; Google Memorystore has a Redis interface)
  - The interface between your application and the cloud product remains the same regardless of whether you're facing the hosted cloud product, or its open-source version
- Consider the tradeoffs of closed-source vs open-source and document your thought process. Some considerations:
  - Risk of vendor failure/product decommissioning
  - Potential urgent need to update your application based on vendor activity
  - Non-public source means fewer eyes looking for vulnerabilities

VULNERABILITY SCANNING

- Update network vulnerability scan requirements to focus on the platform environment (for example, the cloud) in addition to internal networks
  - Require evidence of client isolation in office networks
    - e.g., should only be able to print via cloud

TAC CYBERSECURITY SUBCOMMITTEE

VENDOR RISK MANAGEMENT

BACKGROUND

- The evolving threat landscape, the emergence of new technology, and the expansion of the supply chain have increased the risks faced by the financial services sector

- Global supervisors, regulators, and standards setting bodies have issued numerous rules, rules interpretations, guidance, and questionnaires ('***Supervisory Documents***') on how firms and financial market infrastructures (FMIs) should manage vendor relationships

- Numerous firms and FMIs aim to put information security requirements and oversight expectations into their contracts with third parties to ensure ongoing adherence to security controls

- The Cybersecurity subcommittee is reviewing existing ***Supervisory Documents*** to determine the recommendation to the Technology Advisory Committee

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*** cover the vendor management lifecycle and includes the following risk areas:
  - Planning
  - Due Diligence
  - Contract Negotiation
  - Ongoing Monitoring
  - Oversight and Accountability
  - Termination
  - Documentation and Reporting
  - Independent Review
  - Supervisory Review of Technology Service Providers

- There are currently 15+ ***Supervisory Documents*** covering Vendor Management including most recently the 2019 draft of the Monetary Authority of Singapore TRM Guidelines

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

NEXT STEPS

- Review existing ***Supervisory Documents***[1] on Vendor Management
- Identify potential opportunities to strengthen existing guidance
- Develop and review a recommendation proposal for the Technology Advisory Committee
- Present findings and proposal to the TAC

[1]The links to the existing ***Supervisory Guidance*** under review can be found in the Appendix.

CFTC TAC DIRECTIONAL QUESTIONS

- Given the differences in the approach by different regulatory authorities between principles-based and prescriptive requirements, does the Committee have a preference in the type of recommendation it wishes to receive?

- ***Currently the Subcommittee is looking to provide principles-based guidance back to the committee.***

- Numerous ***Supervisory Documents*** have been developed for Critical Vendors. This guidance was largely created prior to 2014. Is the Committee open to a different approach to determine the controls that should be put in place and how criticality is determined?

- ***The Committee is currently reviewing a nuanced classification approach. The classification would then define those controls that would be required to manage the vendor risk***