Cyber-security and Regulatory Considerations in Information Technology

Contracting for Financial Services Firms

David F. Freeman, Jr., Ellen Kaye Fleishhacker, Susan E. Hendrickson, Thomas A. Magnani, Michael A. Mancusi, Michael I. Raschid, and Nancy L. Perkins

February 2015

Banks, broker-dealers, investment managers, insurance companies and other financial services firms face increasingly sophisticated threats to their data and remote applications. Hacking, once the purview of bored teens and petty criminals, is now a constant threat through the efforts of technically sophisticated international organized criminal groups and sovereign cyber warfare units. Risks range from disruption and downtime, loss of data and confidential consumer information, to theft of money and securities through unauthorized transfers and account access.

At the same time, a new generation of customers demands access to financial accounts through tablets, smart phones, computers and other devices. These customers expect to use mobile devices loaded with user-friendly applications not just to review their accounts, but also to effect transactions and move funds.

Every system and device, from ATMs and point of sale terminals, to customer access devices, to internal wireless networks and routers, is at risk. Financial services firms contract with external vendors for a wide range of systems, support, data and devices to conduct their business. The contracts and relationships with those vendors must be carefully crafted to address cyber-security risks.

Federal and state regulators have taken notice. The Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA) and the bank regulators are engaged in targeted examinations of cyber-security efforts, and the SEC, Federal Financial Institutions Examination Council (FFIEC) and Conference of State Bank Supervisors (CSBS) recently have published guidance on vendor management and security considerations. The New York State Department of Financial Services recently announced that it will be scrutinizing cyber-security as an integral part of its bank examinations, and is asking banks to prepare responses to a specific set of questions and information-requests on their security practices and procedures for purposes of the examinations. Other regulators have issued statements outlining required elements of cyber-security programs, and are closely examining the depth and comprehensiveness of financial firms' programs. Administrative enforcement actions and civil litigation are the foreseeable consequences of programs that fail to measure up. The financial threat is also very real and very large.
Financial firms’ cyber-security programs must be carefully thought through, coordinated internally within the firm and externally with vendors, and conducted with appropriate resources, support, and sustained effort to deal with continuously evolving threats while meeting customer demands. The effort must be conducted at every level of the company, with oversight from the board, leadership from senior management, and involvement from operating business units, rather than simply technology and security departments and compliance personnel. Firms should formalize the corporate governance elements of their strategies by assigning cyber-security and vendor management considerations to a particular board committee through amendment of its charter, as necessary, and adoption of board resolutions. This designated board committee should then appoint specific senior officers to oversee the program, institute a formal reporting line up from the business units, legal, compliance, audit, technology and security departments, and institute regular periodic reporting by management to the committee.

**Mapping and risk assessment**

A first step in the process is creating an inventory of the data, telecom, information technology and internet systems and vendors, and a map of the business units that use them, how the various systems and vendors interact with one another and with customers and counterparties, who has access to them, and who has oversight and control over them. Special attention should be paid to risks associated with remote and other mobile access, transactional and funds transfer systems and devices. An assessment of the technical, financial, legal and regulatory risks involved, and the mechanisms in place to limit those risks is also appropriate and necessary.

**Vendor contracting and oversight**

Firms should take care in selecting, monitoring and reviewing vendors. This requires initial and on-going due diligence in deciding whether to retain a vendor, and whether additional requirements need to be imposed on the vendor to implement improvements that are appropriate to protect the financial institution and its customer. Information, representations and warranties must be obtained from the vendor, and the vendor’s SEC filings, if any, should be reviewed. In addition, it is appropriate to conduct a search for litigation and enforcement history and other public information. Financial firms should conduct diligence on whether the regulators have any "issues" with a vendor’s performance. Major technology changes and contracting relationships should be vetted with the firm’s primary regulator.

The contract should provide specifically for access by examiners and audit personnel, the conduct of system security audits such as SSAE 16, and the sharing of the vendor’s internal audit reports and the
vendor's regulatory documents. These measures provide additional visibility into security considerations at the vendor once the vendor relationship is underway. Consider not only the vendor, but also the vendor's vendors and subcontractors. The essential questions include whether the vendor has the technical capacity, systems, controls, staff, management, experience, financial and other resources, to provide the services or systems in a safe, sound and secure manner that meets the needs of the financial institution and its customers.

In developing the contract with the vendor, conduct an assessment and map the business units and systems with which the vendor and its systems will interact. Be sure to address the technical requirements and business needs of those units and systems in the contract. The business units involved, as well as internal technology, security, compliance and anti-fraud units within the institution, should be consulted during the contracting process to be sure the contract addresses each of their various business, technical and regulatory needs.

The contract should clearly define the products, systems and services being provided, and their operating standards. Where appropriate, the contract should address tools used by the vendor to ensure security, including firewalls, separation of environments, anti-virus software, spyware detection, physical security, intrusion detection, network anomaly detection, security information and event management, configuration management and integrity management tools, and what tools, systems and data the vendor will make available to the financial services firm to assess threats and manage and mitigate risks in the system.

Where account information is accessible through the system involved, the protocols developed in the vendor relationship should include secure methods of validation of any changes to customer account name, address, wire and contact information. When funds or securities transactions or transfers are conducted through the system, requirements for heightened levels of access validation are appropriate.

The contract with the vendor should clearly assign responsibilities and define standards of performance, and address key security requirements, including regarding data, customer information, who has access, how that access is controlled, and the means of detecting unauthorized access and patterns of suspicious account activity.

Data and systems vendors to banks and their affiliates are subject to examination and administrative action by the federal bank regulators, under the Bank Service Company Act (12 U.S.C. § 1867). The vendor should expressly acknowledge and agree to this in the contract.
Depending on the nature of the service or system, it may not be sufficient to simply require that the vendor will comply with applicable law. More granularity is required on certain regulatory issues, including:

- Business continuity and disaster recovery plans and back up data and sites;
- Protections against unauthorized use, access and disclosure of customer data;
- Prompt reporting by the vendor to the financial services firm of any security breaches and unauthorized access;
- Conformance to rules on disposal of information and media;
- Periods for maintaining records, the form and format of those records, and return or transfer to a successor vendor at termination;
- For some categories of vendors (particularly those vendors such as clearing brokers and banks that are themselves subject to formal anti-money laundering (AML) and customer identification program (CIP) requirements), detailed representations, warranties and covenants concerning CIP and AML compliance programs are appropriate;
- For other types of vendors that are not themselves subject to formal regulatory requirements to have CIP and AML programs, it is appropriate in the contract to obtain commitments that the vendor will provide appropriate support to the financial institution's AML/CIP efforts.

For customer-facing systems, it is essential to agree upon protocols and responsibilities for review, approval and updating of content, framing and disclosures to meet regulatory requirements. Firms also should consider assigning responsibility for system security issues, detailing requirements on password and other access controls and multi-factor user verification methods, and specifying protocols and access to tools and information for the parties to collaborate in detecting unauthorized access, suspicious activity and fraud.

Processes conducted outside the United States pose particular challenges under U.S. and foreign privacy laws, technology export restrictions, and as a security and oversight matter. The contract and relationship should address approval requirements and protocols for any portions of systems, processes or services conducted or accessible by the vendor or its own vendors/subcontractors from outside the United States.

Issues regarding intellectual property (patents, copyrights, trademarks, trade secrets, database rights, etc.) also should be addressed to help ensure that key data or technology does not fall into the wrong hands, and that clear rights to ownership and use of the intellectual property are established. The
contract should specifically address ownership and licensing of information and improvements developed as part of the process. Ownership and use of customer relationships and information created or enhanced through the vendor relationship should be retained exclusively by the customer. The contract also should be clear on ownership of any customized solutions and improvements developed by or for the customer. In addition, the contract should contain representations, warranties and indemnification obligations on the part of the vendor assuring the customer that it has the right to use the vendor's information, service or technology without fear of any third party claims, including intellectual property infringement claims.

Depending on the nature of the service or technology being provided and the financial health of the vendor, firms also may want to take measures to reduce the impact of a bankruptcy, liquidation, or change of control of the vendor. Such measures can help to prevent the customer from losing control over any sensitive data or technology.

Of course, firms should give careful consideration to contractual limits on liability, warranty disclaimers and provisions on indemnification, standards of care, standards of performance, termination rights, and vendor insurance requirements.

Coordination of data privacy, AML, fraud detection and technology efforts

Various units within a financial institution are generally engaged in similar, but often separate efforts to assess and control threats. These include the anti-money laundering (AML) function (typically focused on the suspicious or unlawful activities of customers and the transactions they conduct involving the financial institution), the fraud prevention unit (typically involved in ferreting out fraudulent activities or access by third parties or the institution's own personnel affecting customer accounts or the institution's assets and accounts), and credit and counterparty risk management (seeking to measure and control risk exposures to customers and counter parties). Data, internet, information technology and telecoms systems all provide new sources of risk in these areas, but also additional methods for identifying and controlling those risks. The efforts of the different groups within a financial institution should be coordinated through the enterprise risk management program to be sure all risks are covered and the efforts complement each other in an effective and efficient way.
Testing and audit

The system security program should be subject to internal audit as well as penetration testing by competent personnel and/or qualified, trusted external vendors. The team should be continuously looking for holes in the defense and covering them off. The criminals and state-sponsored hackers are continuously seeking access and they are very good at it.

Training

Personnel of the financial services firms should be trained on following cyber-security protocols and identifying potential risks. The training program should be formalized and documented, and integrated with the other aspects of the cyber-security program of the institution. External resources and alerts should be incorporated on an on-going basis to address emerging risks and issues.

Meeting regulatory requirements and guidance

State and federal regulators have published guidance on steps needed to control cyber threats. These include FFIEC examination manuals and guidance, FDIC, Federal Reserve, OCC, SEC and FINRA guidance, as well as state regulatory guidelines from the CSBS and individual states including New York and Massachusetts. They contain good advice and ideas and are an important resource in developing and maintaining an effective program for protecting a financial firm and its customers. The regulators are examining firms’ programs and assessing whether they are following the guidance. A firm that fails to adopt and follow a robust program is exposed to examination criticism and potential administrative enforcement action even in the absence of an event.

Working with regulators and peer groups to identify threats and defenses

The regulators are as concerned as financial services firms about cyber-security threats. They see more of what is going on at other institutions and coordinate with law enforcement to identify emerging threats. Close attention to published regulatory guidance and direct communications with regulators can help a financial services firm benchmark its efforts and identify potential gaps and weaknesses to be sure it is consistent with what regulators expect and what peer institutions are doing. The FBI, the US Computer Emergency Readiness Team (US-CERT), and the Secret Service make available information and resources to financial services firms to help combat cyber-security threats. Similarly, attention to trade association best practices and guidance (such as those from the Financial Services Information Sharing
and Analysis Center), and participation in industry-wide working groups and conferences can further help identify areas for improvements. Retention of external consultants and vendors, and hiring and training of experienced staff can also help maintain the best possible defense against cyber threats.

**Insurance coverage**

The financial institution should review its insurance policies, the coverage limits, and the scope and carve-outs for cyber attacks and unauthorized access to confidential information and funds and accounts to be sure there is appropriate coverage commensurate with the risk. In vendor contracts, financial institutions should carefully consider what insurance coverages are appropriate to require the vendor to carry, and address the institutions’ ability to be covered under the vendor's insurance policy.

**Securities disclosures**

Publicly-held financial firms should review their securities filings to assure cyber-risk issues are appropriately described. The SEC's Division of Corporation Finance published disclosure guidance in 2011 regarding disclosure obligations of issuers relating to cyber-security risks and cyber incidents. Investment managers and broker-dealers should consider including appropriate cyber risk disclosures in client and fund investor disclosure documents, and (in the case of registered investment advisers) their Form ADVs/disclosure brochures.

**Preparing for an event and responding**

Chances are, you will experience unauthorized access to your computer systems and data. According to a study released this month by the SEC's Office of Compliance Inspections and Examinations, 88% of the broker-dealers surveyed and 74% of investment advisers surveyed have experienced cyber-attacks. Plan in advance how you will address this eventuality. This includes prompt disclosures to law enforcement, regulators and affected customers, SAR filing requirements as applicable, insurance carrier notifications, communications with vendors, and, depending on the nature and magnitude of the event, public or investor disclosures. The response plan should be integrated with the firm's business continuity and disaster recovery plan. Be prepared for potential class action litigation, regulatory inquiries and administrative enforcement action.

When the event occurs, the specifics of the incident will be a surprise, and the need to assess it and respond will be immediate. Through prior planning and an action plan, and a pre-established response
team and incident response process, the response effort will be more effective and reduce the potential financial and reputational harm to the financial institution.

If you have any questions about any of the topics discussed in this advisory, please contact your Arnold & Porter attorney or any of the following attorneys:

David F. Freeman, Jr.
+1 202.942.5745
David.Freeman@aporter.com

Ellen Kaye Fleishhacker
+1 415.471.3152
Ellen.Fleishhacker@aporter.com

Susan E. Hendrickson
+1 202.942.6751
Susan.Hendrickson@aporter.com

Thomas A. Magnani
+1 415.471.3162
Thomas.Magnani@aporter.com

Michael A. Mancusi
+1 202.942.5302
Michael.Mancusi@aporter.com

Michael I. Raschid
+1 202.942.6757
Michael.Raschid@aporter.com

Nancy L. Perkins
+1 202.942.5065
Nancy.Perkins@aporter.com

© 2015 Arnold & Porter LLP. This Advisory is intended to be a general summary of the law and does not constitute legal advice. You should consult with counsel to determine applicable legal requirements in a specific fact situation.