BankDirector.com CHARTING A COURSE FOR AMERICA'S BANKING LEADERS

# Cybersecurity Risk Preparedness: Practical Steps for Financial Firms in the Face of Threats

By: *David Freeman, Nancy Perkins* | MARCH 20TH, 2015


Banks and other financial services firms face increasingly sophisticated threats to their data systems and remote applications. Every system and device—ATMs, point-of-sale terminals, customer access devices, internal wireless networks and routers—can be a source of vulnerability. The risks include system disruption, loss of proprietary data and confidential consumer information, theft of money and securities through unauthorized transfers and account access, class action litigation, and damaged reputation.

Regulators are taking aggressive actions in response. The Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), and the federal banking regulators are engaged in targeted examinations of cyber-security efforts. The New York Department of Financial Services has declared that it will be scrutinizing cybersecurity as an integral part of its bank examinations. Other regulators too are closely examining the depth and comprehensiveness of financial firms' data security programs. **Administrative enforcement actions and civil litigation are the foreseeable consequences of programs that fail to measure up.**

So what are the practical steps a financial firm should take to mitigate cybersecurity risks?

**Get the Board and Senior Management Involved**
Proper oversight starts with the board. Assign cybersecurity and vendor management to a specific board committee with responsibility to appoint senior officers to oversee the cybersecurity program and institute a formal reporting line up from business units and the legal, compliance, audit and technology departments.

**Map the Risks**
Create an inventory of database, telecommunications, 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. Scrutinize particularly the risks of remote access, transactional and funds transfer systems and devices.

**Coordinate Compliance Plans**
Various units within a financial institution are generally engaged in simultaneous efforts to assess and control threats though, e.g., anti-money laundering (AML) controls, fraud prevention, and credit and counterparty risk management. Coordinate these efforts with the cybersecurity plan through an enterprise-wide risk-management program.

**Test and Audit**
Conduct regular internal audits of system security and, at least annually, engage external vendors to do penetration testing.

**Train Personnel**
Create a formal personnel training program on cyber-security protocols and how to identify potential risks. Document participation in the training. Incorporate external resources and alerts on an on-going basis to address emerging issues.

**Manage Vendor Risks**
Regulators are expecting banks to oversee vendors. Control risks through both careful vendor selection and subsequent oversight.

- **Selection**
  - Require prospective vendors to verify cyber risk-prevention preparedness.
  - Review vendors' SEC filings.
  - Search for the vendor's litigation and enforcement history.

- **Contracting**
  The vendor contract should specifically provide for:
  - **Oversight access:** rights to conduct system security audits such as SSAE 16 and to receive reports of vendor internal audits.
  - **Specific risk-control tools:** e.g., firewalls, anti-virus software, spyware detection, physical security, intrusion detection, network anomaly detection, security information and event management, configuration management; business continuity plans and back-up systems.
  - **Internal management:** specification of who has data system access, how that access is controlled, and the means of detecting unauthorized access and patterns of suspicious account activity.
  - **Reporting:** prompt vendor reporting of any security risk incidents.
  - **Data Retention:** periods for maintaining data, methods for data disposal, return or transfer.
  - **Liability; Indemnification; Insurance:** limits on liability, indemnification provisions, standards of care and performance, rights of termination, and requirements for vendor insurance.

For vendors outside of the United States, the contract should address applicable legal requirements and protocols for any portions of a system, process or services conducted or accessible by the vendor or its sub-vendors from outside the United States.

**Obtain Adequate Insurance**
Review your insurance coverage for the scope and carve-outs for cyberattacks and unauthorized access to confidential information and funds and accounts.

**Prepare For a Breach**
Be ready for a security breach. Prepare now for making prompt disclosures to law enforcement, regulators and affected customers, SAR filings (as applicable), insurance carrier notifications, communications with vendors, and, depending on the nature and magnitude of the event, public or investor disclosures. Line up counsel to handle potential class action litigation and administrative enforcement actions.

**Work With Regulators and Peer Groups**
Close attention to published regulatory guidance and direct communications with regulators can help identify potential gaps and weaknesses in a cybersecurity plan. Similarly, attention to trade association best practices and guidance (such as the Financial Services Information Sharing and Analysis Center), and participation in industry-wide working groups and conferences can further help identify areas for improvements.

David Freeman is a Partner and head of the firm's Financial Services practice group. He represents financial institutions, investment managers, and broker-dealers on a variety of matters including banking and securities regulatory issues, legislation, mergers and acquisitions, private investment funds, and new product development and documentation.

Nancy Perkins, counsel in the Washington, DC office, focuses her practice on litigation, regulatory compliance, and consulting on emerging policy issues, with a principal focus on data privacy and security.