ReedSmith

The business of relationships.℠

The Current State in Financial Services Cybersecurity

July 2013

ReedSmith

White Paper

Finanical Industry Group

If you have questions or would like additional information please contact one of the authors:

Michael E. Bleier
Partner, Pittsburgh
+1 412 288 1567
mbleier@reedsmith.com

Timothy Nagle
Counsel, Washington, D.C.
+1 202 414 9225
tnagle@reedsmith.com

Christopher J. Fatherley
Analyst, New York
+1 212 549 0309
cfatherley@reedsmith.com

The Current State in Financial Services Cybersecurity

Recently, in *A Call to Arms for Banks*, the *Wall Street Journal* described the intensifying push by regulators for Financial Services firms to better protect themselves and the financial system against cyberattacks. The article noted "…the message from Washington [is] that the private sector has primary responsibility for fending off attacks, even from groups the U.S. believes are tied to a foreign government." And, in a June webinar on *The Evolving Cyber Landscape: Awareness, Preparedness and Strategy for Community Banks*, the Office of the Comptroller of the Currency (OCC) warned that the number of cyberattacks continues to grow and that smaller banks are being targeted. Other developments, such as the creation of an interagency cybersecurity working group and the planned release by the National Institute of Standards and Technology of a draft *Cybersecurity Framework* pursuant to President Obama's critical infrastructure executive order (E.O. 13636), will continue to bring regulatory focus on these issues. Any financial institution that does not include cybersecurity among its enterprise risk programs exposes itself to potentially significant compliance, regulatory, and litigation risk.

Reflecting the heightened regulatory priority of bank cybersecurity, the Office of the Comptroller of the Currency (OCC) issued its Spring 2013 Semiannual Risk Perspective on June 18, in which the word "cyber" is mentioned seven times in the opening summary. This is a marked increase from a single mention just six months ago in the same publication's fall 2012 report, released December 20, 2012 (see the OCC's Risk Perspective webpage here).

The Spring 2013 Perspective noted:

- Banks of all sizes (community, midsize, large) must ultimately bear the responsibility of cyber security oversight, even while pursuing outsourced cost-saving strategies
- Cybercriminals continue to target midsized banks
- Large banks in particular must consider cyberthreat mitigation a core element of operational risk and must expect to be held accountable during regulatory reviews

The OCC's overriding message: Cybersecurity is a critical element of a sound risk profile that can no longer be deferred to the largest institutions.

To assist financial institution clients in their cybersecurity planning, we are pleased to present this Reed Smith Financial Institutions Group Briefing Paper. The intent is to provide a general topic primer and industry development review to guide informed discussion within your organization. Reed Smith attorneys draw from a broad range of deep legal and industry experience. We recognize that adapting to risk and regulatory dynamics is only part of a larger equation. Our advisory defines key strategic opportunities that may position organizations for meaningful, long-term success.

Please contact Michael Bleier or Timothy Nagle for assistance with emerging cybersecurity issues, as well as for further information on Reed Smith's global team.

Note: Cyberattack developments are fast-changing. For the latest updates, we encourage readers to regularly consult the selection of industry source links provided within this White Paper. Links and content contained within are current and available as of June 25, 2013.

Critical Infrastructure Executive Order

As previously noted, President Obama issued an Executive Order (E.O. 13636) February 12, 2013, to reinforce the resiliency of the national critical infrastructure and further guard against cyber threats (see Reed Smith's *Addressing the Cyber Threat* client alert). One section of the Order directed the National Institute of Standards and Technology (NIST) to "develop a voluntary framework for reducing cyber risks to critical infrastructure." Part of the Department of Commerce, NIST is a non-regulatory science and technology research body tasked with advancing U.S. technological competitiveness.

As an initial step, NIST issued a public Request for Information (RFI) posted in the Federal Register February 26, 2013. The RFI, *Developing a Framework to Improve Critical Infrastructure Cybersecurity* (78 FR 13024), comment period closed April 8, 2013. During the Framework comment period, more than 250 responses from entities representing many sectors and industries were submitted, ranging from a few paragraphs to submissions in excess of 100 pages.

Overall, the responses to the RFI were directionally supportive of the Framework proposal, with the following key response points identified by NIST:

- Minimal conflict with existing regulatory requirements
- Refer to existing frameworks, standards, guidelines, and practices
- Modular approach to allow for diverse business contexts, e.g., varying definitions of "critical asset"
- Consider costs associated with legacy (in some cases, up to 30 years) control system compliance
- Encourage stakeholders to practice good "cyber hygiene," e.g., current antivirus software, file backup
- Ensure information sharing includes stringent privacy and civil liberty safeguards
- Follow Fair Information Practice Principles (FIPPs) for impacted parties, e.g., personal disclosure notice

The NIST *Framework to Improve Critical Infrastructure Cybersecurity* follows an iterative protocol along several segments: Engagement, collection, categorization, communication, analysis, selection, preparation, and publishing. Public participation is encouraged. In an effort to represent the interests of all stakeholders, NIST is additionally promoting a series of information gathering and reporting sessions ending in October 2013 with the publication of a preliminary *Framework*.

The following table illustrates the NIST Framework responsibilities and process timeline:

2013 Event Date	Event Title	Comments
October (TBD)	Publish preliminary framework	N/A
September (TBD)	Fourth Framework workshop	N/A
July 10 – 12	Third Framework workshop	• Hosted by University of California, San Diego (UCSD) • Annotated outline of the initial Framework draft presented
July 1	DRAFT Outline - Preliminary Framework	• Guidance to assist overall upcoming Framework events
May 29 – 31	Second Framework workshop	• Hosted by Carnegie Mellon University, Pittsburgh • Presentation of preliminary comment analysis
May 15	Analyze RFI responses	*Common theme groupings* • Framework principles: What the Framework should consider • Common points: ID practices with wide utility and practice • Initial gaps: Identify RFI gaps that do not meet E.O. 13636 goals
April 8	Collect, categorize, post RFI responses	Completed
April 3	First Framework workshop	• Held at Department of Commerce, Washington, D.C. • Framework introduction and goal setting
March 28	Notice of Inquiry (NOI)	• Issued by Secretary of Commerce, following Presidential order • Incentives to participate in voluntary cybersecurity programs • Comment period closed April 29, 2013
February 26	Request for Information (RFI)	• Follows E.O. 13636 • Comprehensive cyber risk review and Framework development
February 12	Presidential Executive Order E.O. 13636	• Identify critical infrastructure security standards and guidelines • Comment period closed April 8, 2013

Source: NIST *Cybersecurity Framework* – see webpage for supporting documentation and updates. Note: Table information as of June 25, 2013.

Many Financial Services firms and industry groups, including American Petroleum Institute, Citigroup, IBM, Microsoft, North American Electric Reliability Corporation (NERC), and Verizon, have participated in the RFI process and subsequent meetings (see NIST RFI Framework full comments here). Given the mature critical infrastructure programs in current practice within the Financial Services industry, the draft Framework will likely reflect many of the standards and processes currently in use within the industry and accepted by regulators.

Cybersecurity Legislation

While the Executive Order (E.O. 13636) was issued in response to the failure of congressional leaders to generate sufficient support for the Lieberman-Collins bill or other cybersecurity legislation, all parties recognize legislation will ultimately be necessary to address issues such as limited protections against liability for private sector entities that share information with the government.

On February 13, 2013, Congressmen Rogers and Ruppersberger reintroduced the *Cyber Intelligence Sharing and Protection Act* (CISPA) (H.R. 624), which was passed by the House of Representatives April 18, 2013 (status as of June 25, 2013). An earlier iteration, the *Cyber Intelligence and Protection Act* (H.R. 3523), failed to pass the Senate in late 2012 but has been reincarnated as H.R. 624.

Financial services industry stakeholders agree with CISPA's intent, but have expressed reservations as to the adequacy of protection from liability for information sharing and the appropriate lead federal agency.

Paul Smocer, Financial Services Roundtable BITS President, presented during House of Representatives testimony February 14, 2013, similar policy opinions with the additional caution that reputational safeguards must be in place to encourage stakeholder buy-in.

President Obama and others have expressed concern that CISPA has the same flaws as its predecessor in that it does not adequately protect the privacy interests of those whose information is shared with the government (see the President's State of Administration Policy here). However, CISPA's language affirms information anonymization or minimization, exemption from liability for entities acting in "good faith," and federal government responsibility for agency privacy violations (see CISPA's original language here).

Proponents of CISPA point out that threat information is comprised primarily of technical network information with only incidental personal information. Their argument is that the privacy interests that are protected by identifying and deleting the small amount of personal information are outweighed by the costs of such activity.

Another recent development that may impact the cyber information-sharing effort is disclosure of the PRISM program under which private sector entities have been providing customer and other information to government agencies pursuant to orders issued under the Foreign Intelligence Surveillance Act (FISA). The debate regarding the proper balance between privacy and national security interests may expand into the larger critical infrastructure protection context. The threats to the national infrastructure, including the financial services networks, electric grid, municipal water supplies, communications networks, and transportation systems, have been repeatedly emphasized by senior government and industry executives. Moreover, sharing threat and network information by and among individual institutions continues to be an effective means of identifying and responding to threats.

The extent to which that sharing is expanded past existing frameworks will be affected by the larger national conversation on the balance between privacy and security. Ultimately, resolution of this balance will most likely determine the outcome of the CISPA legislation.

The table below lists a selection of pending and prior legislation as of June 25, 2013, but excludes bills such as the National Defense Authorization Act where cybersecurity is not a primary focus.

Date Introduced	Session	Identifier	Act Title	Sponsor(s)	Status
June 6, 2013	113	H.R. 2281	H.R. 2281: Cyber Economic Espionage Accountability Act	Rep. Rogers	Referred to Committee, 6/6
June 6, 2013	113	S. 1111	Cyber Economic Espionage Accountability Act	Sen. Johnson	Referred to Committee, 6/6
May/June 2013	113	N/A	National Cybersecurity and Critical Infrastructure Protection Act of 2013 (NCCIP Act)	N/A	In discussion draft, see working document here
April 18, 2013	113	H.R. 1640	Cyber Warrior Act of 2013	Rep. Israel	Referred to Committee, 4/18
April 16, 2013	113	H.Res. 164	Providing for consideration of H.R. 624 Cyber Threat info. Sharing	Rep. Woodall	Agreed to, 4/17
April 10, 2013	113	H.R. 1468	Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2013 or SECURE IT	Rep. Blackburn	Referred to Committee, 4/10
March 22, 2013	113	S. 658	Cyber Warrior Act of 2013	Sen. Gillibrand	Referred to Committee, 3/22
February 15, 2013	113	H.R. 756	Cybersecurity Enhancement Act of 2013	Rep. McCaul	Passed House, 4/16
February 13, 2013	113	H.R. 624	Cyber Intelligence Sharing and Protection Act	Rep. Rogers	Passed House, 4/18
January 23, 2013	113	S.68	Secure Chemical Facilities Act	Sen. Lautenberg	Referred to Committee, 1/23
January 22, 2013	113	S. 21	Cybersecurity and American Cyber Competitiveness Act of 2013	Sen. Rockefeller	Referred to Committee, 1/21
January 3, 2013	113	H.R. 86	Cybersecurity Education Enhancement Act of 2013	Rep. Lee	Referred to Committee, 1/3
July 19, 2012	112	S. 3414	Cybersecurity Act of 2012 (CSA2012)	Sen. Lieberman Sen. Collins	Not enacted
June 27, 2012	112	S.3342	Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (SECURE IT)	Sen. McCain	Not enacted
February 15, 2012	112	S. 2111	Cyber Crime Protection Security Act	Sen. Leahy	Not enacted
February 13, 2012	112	S. 2102	Cybersecurity Information Sharing Act of 2012	Sen. Feinstein	Not enacted

Source: GovTrack 113th Congress cybersecurity legislative search webpage.

Financial Services Cybersecurity Infrastructure

Framework As discussed above, the NIST framework will present a flexible, principles-based roadmap based on RFI comments that is structured on scalability, sustainability, innovation, and a reasonable risk versus cost analysis. The framework is expected to incorporate industry models, such as those practiced by Financial Services, which have proved successful in concept and implementation.

Financial Services Sector Coordinating Council (FSSCC) Although the recent bank-directed cyberattacks are cause for alarm, the Financial Services industry has built a leading cybersecurity communication and response network following the events of September 11, 2001. The coordinated effort established by the Financial Services industry is often considered a best-practice model.

For example, the FSSCC, NIST, and the Department of Homeland Security (DHS) signed a Memorandum of Understanding (MOU) December 6, 2010 with "the intent of the parties to expedite the coordinated development and availability of collaborative research, development, and testing activities for cybersecurity technologies and processes based upon the Financial Services sector's needs."

The MOU additionally encouraged an innovative framework with cross-industry application (see complete MOU document here).

Established in 2002, the FSSCC is tasked by President Clinton's 1998 Presidential Decision Directive 63 (PDD 63) to coordinate the Financial Services industry's critical infrastructure and operational risk response. FSSCC is a public-private partnership comprised of more than 50 volunteer Financial Services industry and trade members, including (among others): American Bankers Association, The Financial Services Roundtable (BITS), NYSE Euronext, Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Wells Fargo, US Bank, and Visa USA. Charles Blauner, Citigroup's Global Head of Information Security, is the current FSSCC Chair.

In 2010, the FSSCC established four Financial Services objectives:

Strategic Objectives	2010 Goals
Identify Threats and Promote Protection	• Finalize updated Threat Matrix • Disseminate Threat Matrix and build into strategy • Build Threat Matrix into ongoing planning and execution of FSSCC goals
Drive Preparedness	• Establish regularized process for escalating events and disseminating information in the form of actionable intelligence • Establish more direct international relationships • Further the undersea cables work • Develop supply chain frameworks • Disseminate CyberFIRE and Cyberattack against Payment Processes (CAPP) Exercise learning • Support regional coalitions
Collaborate with the Federal Government	• Establish ongoing interaction with (1) the new White House Cybersecurity Coordinator and (2) DHS/National Security Agency (NSA) • Address Internet congestion as part of DHS interaction • Develop Identity Management Principles and request for investment • Implement Government Information Sharing Framework initiative with Department of Defense (DoD) and DHS • Develop sector-wide position on Internet Corporation for Assigned Names and Numbers (ICANN) • Engage in conversation on cyber and critical infrastructure legislation and determine appropriate next steps • Deliver a finance and banking educational session
Coordinate Crisis Response	• Expand and improve crisis management response playbooks • Improve usefulness and mindshare of playbooks

Source: Department of Homeland Security *2010 Sector CIKR Protection Annual Report for the Banking and Finance Sector*, page 3 (CIKR = Critical Infrastructure and Key Resources).

FSSCC's designated Sector Specific Agency (SSA) is part of the Treasury Department. The agency is closely aligned with national interest priorities set forth by the DHS.

The February 12, 2013 Presidential Policy Directive (PPD 21): *Critical Infrastructure Security and Resilience* (which was issued contemporaneous with the executive order) identified Financial Services as one the nation's 16 critical infrastructure sectors. Additional critical sectors include (among others): Chemicals, Dams, Energy, Healthcare and Public Health, Manufacturing, Transportation and Water (see the Designated Critical Infrastructure Sectors and Sector-Specific Agency list on the PPD 21 webpage here).

The FSSCC additionally functions in partnership with Financial Services Information Sharing and Analysis Center (FS-ISAC). Established in 1999, FS-ISAC was similarly formed by 1998's Presidential Decision Directive 63 (PDD 63) and follows a like FSSCC operational path. FS-ISAC is an industry membership organization and considered FSSCC's sister entity.

FS-ISAC partners include (among others): financial industry associations (e.g., American Bankers Association), government agencies (e.g., Department of Homeland Security), payment associations (e.g., Electronics Payments Association), sector specific associations (e.g., Securities Industry and Financial Markets Association), and other industry Information Sharing and Analysis Centers (e.g., Emergency Management and Response ISAC).

Note: ISAC refers to Information Sharing and Analysis Centers (see the National Council of ISACs web page here).

In addition to promoting education and awareness, FS-ISAC's core mission includes:

- Serve as sector communications hub sharing real-time cyber and physical threat information
- Deliver rapid threat notifications to FS-ISAC and FSSCC members
- Provide expert analysis and sector impact assessments to threats, vulnerabilities, and incidents

Employing traffic light protocol (TLP), FS-ISAC distributes threat information with the following classification standards:

FS-ISAC Classification	Target Audience
Red	Information labeled RED should not be shared with anyone outside of a restricted, predetermined group
Yellow	This information may be shared with FS-ISAC members. Generally, alerts with the FS-ISAC Yellow classification will be kept behind the FS-ISAC secure portal
Green	Information within this category may be shared with FS-ISAC members and partners (e.g. DHS, Treasury and other government agencies and ISACs). Information in this category is not to be shared in public forums
White	This information may be shared freely and is subject to standard copyright rules

Source: FS-ISAC *Overview of the FS-ISAC*, page 5.

Financial Banking Information Infrastructure Committee (FBIIC) Chartered in 2001 under the President's Working Group on Financial Markets and currently chaired by the Treasury Department, FBIIC is missioned to facilitate financial regulator communication. The committee comprises 17 government agencies, including (among others):

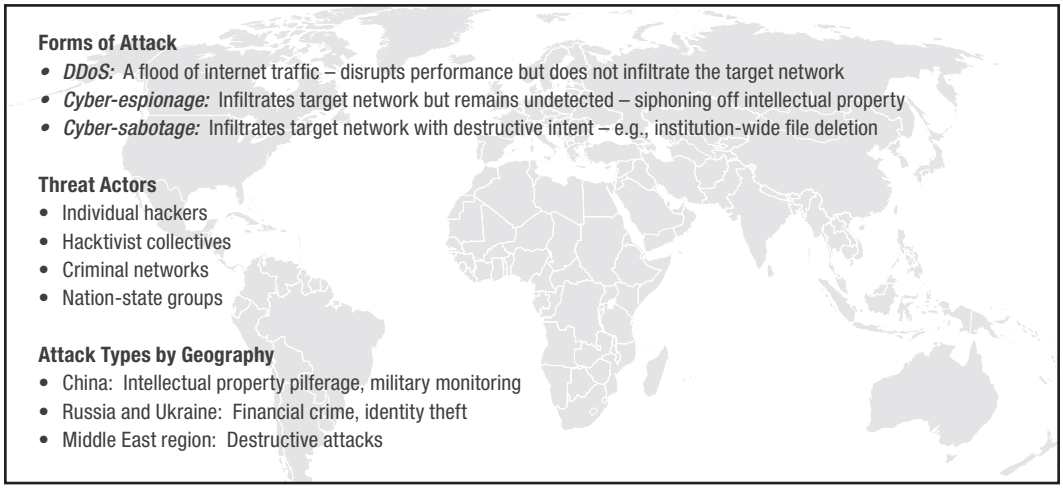
- Department of the Treasury
- Farm Credit Administration
- Federal Deposit Insurance Corporation
- Federal Reserve Board
- National Credit Union Administration
- Office of the Comptroller of the Currency
- Securities and Exchange Commission

Specific FBIIC emergency response actions include:

- Identify critical infrastructure assets and vulnerabilities, and establish systemic prioritization
- Establish secure communications and protocols among U.S. financial regulators
- Ensure sufficient member agency staff (with security clearance) to coordinate classified information

Cyberattack Overview

The Securities Industry and Financial Markets Association (SIFMA) is leading an exercise (Quantum Dawn 2) July 18, 2013, which is intended to replicate a large-scale assault on financial industry information systems and online sites. Financial institutions and government agencies will participate in order to evaluate coordination and decision-making among the participants. While this will support efforts to improve the response to a systemic attack, the threats to individual institutions and the industry come in many forms and from several directions.



Source: Testimony by Kevin Mandia February 14, 2013 before the Permanent Select Committee on Intelligence (as of June 25, 2013, the testimony webcast replay is no longer readily available on Committee webpage).

Distributed Denial of Service (DDoS) DDoS is not necessarily a computer security breach but rather a multitude of remote systems digitally descending on a single target. The flood of Internet traffic overwhelms the target system, essentially leading to system paralysis and a denial of service for authorized users. The net effect compromises the target's internal network security resources and firewall performance. Evidence of this was seen in the recent spate of publicly announced DDoS service disruptions of several major Financial Services organizations (e.g., JPMorgan Chase, Citigroup, PNC Financial).

Although not a DDoS attack, the Anonymous hacktivist collective breached the Federal Reserve's internal systems in January 2013. Proprietary log-in credentials for more than 4,000 U.S. bank and credit union executives were publicly posted on the web. U.S. hacktivists have claimed First Amendment rights as their defense.

Early DDoS attacks utilized flooding tools such as Trinoo (trin00), Tribe Flood Network (TFN), Stacheldraht, and Tribe Flood Network 2K (TFN2K).

Industry estimates suggest that a 24-hour DDoS/Botnet attack outage will cost the average enterprise $6.3 million (Arbor Networks: *Protecting the Data Center, Arbor Pravail Introduction*, page 4).

DDoS attacks follow two primary forms (Arbor Networks: *The Growing Threat of Application-Layer DDoS Attacks*, page 3):

- Volumetric: Consumes bandwidth, causing congestion
- Application-layer: More sophisticated and discreet attacks targeting a specific application or service

Note: Refer to Reed Smith's *OCC Issues Alert in Response to Recent DDoS Events* blog.

Cyber espionage and cyber sabotage Cyber espionage and cyber sabotage have the capacity to infiltrate and destroy a target host network. In a worst-case scenario, coded malware can discreetly pass through target-connected networks in a replicating systemic halo. All of these scenarios can occur from one click on a "spear-phishing" email.

A well-publicized example involved the Kingdom of Saudi Arabia's state-owned petrochemical company, Saudi Aramco. In August 2012, a malicious virus dubbed "Shamoon" infiltrated Saudi Aramco's computer system and erased critical files on some 30,000 company devices. The attack against the world's largest oil company is suspected to be Iranian state-sponsored.

"Spear-phishing" communications are often targeted emails that can include an individual's specific name, role, and professional title. The "spear" side of the equation refers to executive targeting. Industry analysis estimates the majority of targeted attacks utilize "spear-phishing" emails embedded with links to malicious file attachments. These attachments are opened by an unsuspecting user, thereby exposing the target network to Advanced Persistent Threat (APT) infiltration.

Malicious "malware" with seemingly innocuous names:

- Flame: A virus affecting Iran and parts of the Middle East beginning in 2012, a very "complex threat"
- Gauss: Similar structure and date to Flame but with a high concentration of affected users in Lebanon
- Stuxnet: Apparently responsible for a cyberattack against Iranian nuclear facilities beginning in 2010

Industry Reports

Mandiant APT1 Report In February 2013, the Virginia-based information security firm Mandiant took a bold step by publicly detailing the cyber espionage agenda of the Chinese People's Liberation Army (PLA). Reporting to the Communist Party of China (CPC), the PLA is suggested to have direct support from the CPC. CPC is mainland China's ultimate authority in a country well known for Internet surveillance. It is highly unlikely that PLA's robust cyber espionage activities can function without CPC consent.

Mandiant's 70+ page report, "*APT1: Exposing One of China's Cyber Espionage Units*," is unusual in its depth, disclosure, and free availability. The report introduces and details the cyber espionage tactics of APT1, one of the leading global Advanced Persistent Threat (APT) players with a known history of organizational compromise dating back to 2006.

Mandiant provides extrapolated evidence that supports APT1 likely as Unit 61398, a PLA bureau operating from a single location in Pudong New Area of Shanghai. The majority of APT1 targets are headquartered in native English-language locations.

APT1 is an organized group, potentially consisting of hundreds of skilled "human operators" supported by linguists, researchers, malicious code authors, industry experts providing operator guidance, and staff transmitting pilfered intellectual property (IP) information to requestors. Furthering the suspicion of nation sponsorship, documents surfaced describing the state-owned China Telecom's use of company resources to "co-build" fiber optic communications infrastructure with Unit 61398.

Tellingly, the Mandiant analysis reveals "APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan."

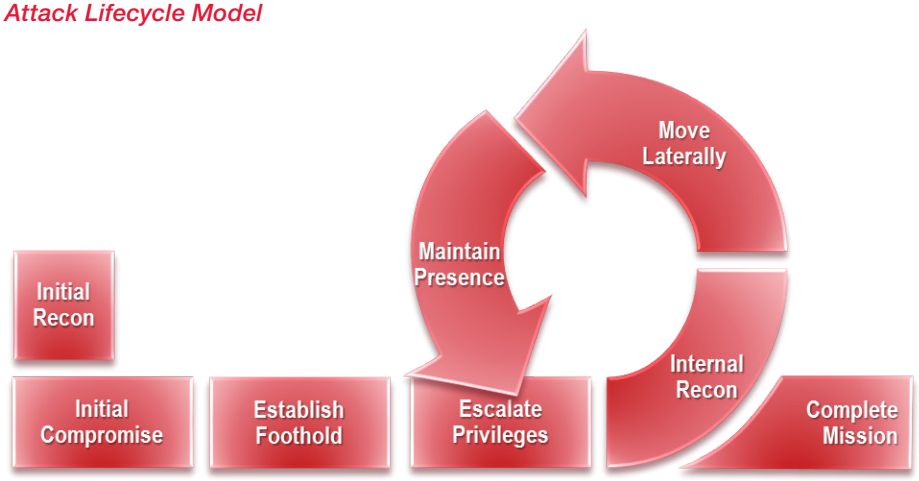
Endorsed by China's National People's Congress March 14, 2011, the Plan prioritizes the following seven industries deemed critical to "national and social development":

Designated Priority Industries	Description
New Energy	Nuclear, Wind, Solar Power
Energy Conservation & Environmental Protection	Energy Reduction Targets
Biotechnology	Drugs and Medical Devices
New Materials	Rare Earths and High-End Semiconductors
New IT	Broadband Networks, Internet Security Infrastructure, Network Convergence
High-End Equipment Manufacturing	Aerospace and Telecom Equipment
Clean Energy Vehicles	N/A

Source: *KPMG China's 12th Five Year Plan: Overview*, page 2, ©KPMG.

APT1's most common attack method utilizes email "spear phishing" as the initial entry point. Once compromised, APT1 establishes residence within the target organization's technology infrastructure and creates a "backdoor" allowing remote command control. At this point, APT1 has the ability to "escalate privileges" permitting a presence that can move about the target system undetected. Company firewalls can defend against external threats but are less effective combating a compromise with an internal "foothold." Mandiant reported the longest compromise on an observed peer set was 4 years and 10 months.

APT1 Attack Lifecycle Model



Source: *Mandiant APT1 Exposing One of China's Cyber Espionage Units*, page 27, ©Mandiant.

Lastly, Mandiant has made known three APT1 "threat actors" whose identities were revealed by "poor operational security choices":

- Zhang Zhaozhong, a.k.a. "Ugly Gorilla": Tends to "sign" name in the malicious malware code
- DOTA (no attributed name): Often works under variations of DOTA, such as "dota," "DotA," "do. ta." Appears to use Harry Potter references as email security question answers.
- Mei Qiang, a.k.a. "SuperHard" or "SH": A "highly capable" developer with the ability to manipulate the Windows operating system

Note: The above is a brief summary of Mandiant's report – refer to the full document for further details.

Information available from security consultants such as Mandiant and CrowdStrike, government classified and unclassified threat information, and internal industry sources such as the FS-ISAC, describe internal and external threats that are increasing and evolving. Where APT and DDoS used to describe the rare event that affected only global banks, they must now be considered business as usual and factored into security and business continuity planning in the same way that power outages are. With greater industry awareness, unique capabilities that some vendors can provide, and government assistance in the form of threat intelligence and national support, it is possible for financial institutions to adapt their risk profile to address these threats. However, an effective vulnerability management program will include anticipating the next threat that is presented externally or affected through the unintentional or intentional actions of insiders.

Related efforts such as customer and employee awareness, effective vendor management programs, comprehensive security and business continuity/disaster recovery policies and planning, and risk identification, must be sufficiently flexible to accommodate new regulatory or industry guidance in the United States and wherever a financial institution has a presence.

Emerging Developments

European Union Directive The European Union (EU) set forth a member-state Network and Information Security (NIS) directive February 7, 2013. The "cooperation framework" is informed by "An Open, Safe and Secure Cyberspace" strategy. The EU strategy is driven by essentially the same objectives as U.S. efforts.

The European Network and Information Security Agency (ENISA) was established in 2004 and serves to advise, collect and analyze data, promote sound risk management methods, and respond to "computer emergency" incidents. ENISA is considered a "body of expertise" mandated to perform information security technical and scientific research. ENISA additionally assists the European Commission with network and information security legislation.

Questions arise regarding true harmonization across member-states with differing infrastructure capabilities. To this effect, the NIS directive will first establish "common minimum levels" allowing more advanced states to "go beyond minimum requirements" if able. Critics argue the EU effort is aspirational.

Member-states will be required to implement the directive within 18 months of Council and European Parliament adoption (specific date currently unknown).

Note: Refer to Reed Smith's *EU Proposed Directive on Network and Information Security* blog.

Social Media The U.S. Federal Financial Institutions Examination Council (FFIEC) released proposed social media guidelines January 22, 2013 pertaining to banks, savings associations, credit unions, and CFPB state supervised nonbank entities. The FFIEC guidelines are in response to industry and consumer group requests for regulatory guidance. The *Federal Register* comment period closed March 23, 2013.

The proposed guidance acknowledges the sales and service utility of social media but equally suggests potential risks associated with increasing usage.

These include (but are not limited to):

- Money laundering
- Customer and institution privacy leakage
- Insufficient risk controls leading to malicious malware attacks

- Legal and regulatory non-compliance with financial product disclosure, marketing, and sales
- Fraud and brand identity risks

Note: Refer to Reed Smith's *FFIEC Proposes Social Media Risk Management Guidelines* blog.

On the Agenda: What Financial Services Executives Should Be Discussing

In October 2011, the Securities and Exchange Commission (SEC) issued disclosure guidance for "obligations relating to cybersecurity risks and cyber incidents." For an analysis of the guidance and the role it plays in disclosure decisions (refer to the SEC's Corporation Finance Cybersecurity Disclosure Guidance here).

The current regulatory thinking suggests cybersecurity should be one aspect of the enterprise risk and disclosure process. Executives and boards of directors are responsible for including security and privacy in their oversight program under the Gramm-Leach-Bliley Act. The current state of Financial Services cybersecurity may require more active engagement by technology, risk, compliance, audit and line of business managers across the entire institution, regardless of size.

To benchmark firm capabilities, we recommend proactively engaging with the international cybersecurity conversation. Equally, it is risk management best practice to maintain a well-defined Cyber Incident Response Plan (CIRP) that exceeds current minimum regulatory exam guidance (refer to the FFIEC Information Technology Examination Handbook here).

Below is a suggested CIRP component starting list:

- Ensure corporate governance is properly aligned with forward-thinking risk-management policies
- Firms with global operations, ensure cybersecurity defenses are consistently managed across the regional footprint – fluency in all local laws, regulations, and standards
- Planning must include critical supply chains – vendors may have limited cybersecurity resources
- Cybersecurity vendor loss-share liabilities – capabilities assessment, what exactly is "guaranteed"
- Cyber liability insurance is recommended – ensure coverage is consistent with the firm's operational profile, including social media and mobile devices (see Reed Smith's *Enhancing the Brave New World of Cyber Liabilities and Insurance Coverage* brief here, requires ABA subscription) or (see The Department of Homeland Security's *Cybersecurity Insurance Read Out Report* here)
- Regular firmwide awareness training of attack prevention and immediate action protocols
- Retain a well-qualified cybersecurity staff informed by ongoing training
- Offer competitive cybersecurity staff compensation packages
- FSSCC and FS-ISAC membership

The threshold for responding to cyberthreats will continue to rise, with regulators, shareholders, and customers expecting financial institutions to weather the storms presented by threats such as DDoS, state-sponsored or global criminal enterprises, and greater online presence. Financial institutions of all sizes must have adequate information security programs in place to protect customer, proprietary, institutional client, and employee information from loss or compromise. The greater responsibility will likely be borne by the larger financial institutions because of their significant connectivity to critical infrastructure. However, an opportunity to engage with the entire industry constituent landscape (including community, small, and regional institutions) on shared risk exists, and should not be ignored. This national and global conversation is certain to continue with urgency for the foreseeable future.

Reed Smith Cybersecurity Alerts and Blogs

Client Alerts

- Addressing the Cyber Threat: Cybersecurity Executive Order Issued and CISPA Introduced
- EU Proposed Directive on Network and Information Security
- Too Important to Lose? Draft Executive Order on Cybersecurity and Critical Infrastructure Reaches New Industries

Note: Refer to Reed Smith's Data Privacy, Security & Management Client Alerts webpage here for additional discussion.

Global Regulatory Enforcement Law Blogs

- Cybersecurity Executive Order and CISPA to Solve Cyber Threat?
- Cybersecurity Executive Order: A Shift to Implementation Over Participation
- Defense Contractors Are Now Subject to Notice Requirements for Hacked Systems
- FFIEC Proposes Social Media Risk Management Guidelines
- OCC Issues Alert in Response to Recent DDoS Events

Note: Refer to Reed Smith's Global Regulatory Enforcement Law Blog here for additional discussion.

About Reed Smith

Reed Smith's Financial Industry Group is comprised of more than 220 attorneys organized on a cross-border, cross-discipline basis, and dedicated to representing clients involved in the financial sector, advising most of the top financial institutions in the world.

As well as being authorities in their areas of law, FIG lawyers have a particular understanding of the Financial Services industry, enabling them to more effectively evaluate risks, and to anticipate and identify the legal support needed by clients.

FIG lawyers advise on transactional finance covering the full spectrum of financial products, litigation, commercial restructuring, bankruptcy, investment management, M&A, consumer compliance, and bank regulation, including all aspects of regulatory issues, such as examinations, enforcement, and expansion proposals.

Reed Smith's *Global Data Privacy, Security & Management Group* is comprised of more than 35 attorneys worldwide with deep experience in compliance, regulatory, litigation defense, technology, contracting, and data analysis for financial institutions. Our team's diverse experience includes engineers, software developers, cybersecurity, and other technology professionals. Credentials include in-house legal experience at global banks, asset managers, and insurers. Additionally, our team includes former regulators from the Federal Reserve Board, the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Office of the Attorney General of Illinois, and the UK Financial Services Authority.

Reed Smith's *Data Privacy, Security & Management* experience includes:

- Compliance Experience: Our data protection team provides practical, risk-based advice for building comprehensive compliance programs and contingency plans for immediate response to emergency situations and threats.
- Litigation & Regulatory Results: Our privacy litigators have defended more than 70 class actions arising from alleged privacy violations, data thefts, and breaches, as well as claims of data misuse involving websites, specialized data bases and targeted advertising.
- Innovative Use of Data: Privacy compliance isn't just about minimizing liability. An effective information management program enables the identification, analysis and use of valuable proprietary and personal information in innovative ways. Our team helps clients identify and execute on revenue opportunities in a manner that respects their obligations as custodians of the personal, proprietary, and business information of their customers and partners.

ReedSmith

NEW YORK
LONDON
HONG KONG
CHICAGO
WASHINGTON, D.C.
BEIJING
PARIS
LOS ANGELES
SAN FRANCISCO
PHILADELPHIA
SHANGHAI
PITTSBURGH
HOUSTON
SINGAPORE
MUNICH
ABU DHABI
PRINCETON
N. VIRGINIA
WILMINGTON
SILICON VALLEY
DUBAI
CENTURY CITY
RICHMOND
GREECE
KAZAKHSTAN