PAUL HASTINGS

STAY CURRENT

September 2015

Follow @Paul_Hastings

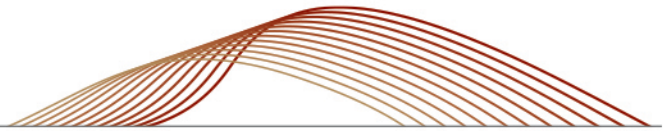
Cybersecurity as a Global Concern in Need of Global Solutions: Some Recent Financial Regulatory Developments

By V. Gerard Comizio, Behnam Dayanim & Laura E. Bain

U.S. financial regulators are increasingly recognizing the threat of cyberattacks as one of "the biggest systemic risk[s] we have facing us."[1] The Financial Stability Oversight Council ("FSOC") has warned that the U.S. financial system is "highly dependent upon" often interconnected information technology systems, service providers operate critical infrastructure resulting in the concentration of key services that create the risk of a single cyber-incident impacting many institutions simultaneously, and malicious actors can infiltrate supply chains and software in ways that are difficult to detect.[2] The real and rising threat of cyberattacks against financial institutions and the potential for significant impact to the economy has caused financial services regulators and law enforcement to become increasingly alert to such risks and to heighten their scrutiny of cybersecurity programs.

Globalization, however, complicates regulators and law enforcements' already complicated challenge. Neither financial institutions nor their technological platforms are confined within the borders of a single country, which cybercriminals have long recognized. A U.S. financial institution may have branches with employees accessing the internet in numerous countries or maintain a physical presence solely in the U.S., but allow its U.S. customers to use online banking. Even an institution with no online presence, if such an institution still exists, may be exposed to cybercrime when it installs compromised software on its internal system—not just to cybercriminals within its own country, but from anywhere. Cyberattacks are a global problem in need of global response.

In May 2015, the U.S. House of Representatives Committee on Financial Services heard testimony from a cybersecurity expert of the possibility of a "rapid spike in truly disruptive attacks by a dangerous adversary, which no longer has a stake in a global financial system," and that "[t]his danger requires immediate contingency planning with the sector and with regulators and other Federal partners, along with ***coordination with our international partners*** particularly in Europe."[3] As cyberattacks pose a significant threat to the global financial system, financial services regulators world-wide are increasingly adopting laws, regulations and policies that focus on cybersecurity. The U.S. for example, has recently issued numerous cybersecurity regulatory guidance bulletins applicable to the banking and financial sector that focus on cyber-resilience, as well as two recent Presidential Executive Orders characterizing cyber-threats as a "national emergency," and calling for increased cyber-resilience standards.[4] It is important for financial services organizations to understand that they face new and evolving cyber regulation on a global basis.



This article provides an overview of recent developments in cybersecurity regulation by 1) the U.S., 2) the UK, and 3) the EU, as well as the movement towards international cooperation, and serves as a guide for financial institutions to develop an effective cyber-risk management program.

I. The United States

As we noted in a previous Stay Current,[5] the U.S. federal government federal banking agencies ("FBAs") have steadily increased their oversight of cybersecurity risks and promulgated cybersecurity guidance. Other financial institution regulators have likewise heightened their regulatory scrutiny and issued their own cybersecurity guidance. For example, in April 2015, the SEC issued cybersecurity guidance for registered investment companies and registered investment advisers, recognizing the investment sector's increasing reliance on information technology and corresponding vulnerability to cyberattacks.[6] The guidance encourages these companies and advisers: (1) to conduct periodic assessment of the nature and sensitivity of the customer information they collect and how they store it, the cybersecurity threats to their systems, the security controls in place, the impact of a breach, and the effectiveness of the "governance structure for the management of cybersecurity risk"; (2) to create a strategy for detecting and responding to cyber-threats; and (3) to implement a compliance program through written policies and procedures and training to officers and employees concerning threat prevention, detection and monitoring. The compliance program should be firm-specific and address the risks of identity theft, data breach, and fraud and service disruption as it relates to the individual firm's business operations and services. The guidance also suggested firms take efforts to educate customers on ways to reduce their cybersecurity exposure with respect to their investment accounts.

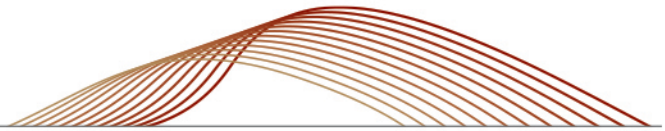
In 2015, FSOC issued a report discussing the emerging threat of cyberterrorism, and stated that financial institutions "should be prepared to mitigate the threat posed by cyberattacks that have the potential to destroy critical data and systems and impair operations."[7] The 2015 report reveals that FSOC expects financial institutions to anticipate attacks and develop "capabilities and procedures to resume operations," to collaborate with government agencies, and to protect their administrative access by requiring two-factor layered authentication for certain accounts and sensitive systems.[8]

A. Unclear Expectations for Information Sharing

However, in addition to FSOC's substantive recommendations, FSOC also indicated an expectation that firms participate in information sharing.[9] As discussed in a previous Stay Current, the extent to which financial institutions may share information regarding cybersecurity risks and data breaches[10] remains unclear. Pending before Congress are various cybersecurity bills that are intended to enable private companies to share cyber-threat information with each other and with the federal government by providing liability protections. The House passed two such proposals, H.R. 1560[11] and H.R. 1731,[12] and they have been pending before the Senate since April 2015. A separate Senate-initiated bill, S. 754, has been pending in the Senate since March 2015.[13] Until Congress clarifies the extent to which financial institutions may, or must, share information regarding cyber-incidents, financial institutions must navigate the potential conflicts between their regulators' expectations and operational/logistical concerns—what information can be disclosed, in what circumstances, before or after consumer notifications, etc.

B. Emerging Cybersecurity Tools

In June 2015, the Federal Financial Institutions Examination Council ("FFIEC") developed and released the Cybersecurity Assessment Tool to assist financial institutions in identifying their risks and



assessing their cybersecurity preparedness.[14] The Cybersecurity Assessment Tool is intended to provide a "repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time,"[15] and is being integrated into the FBAs' IT examinations of banking organizations.[16] As a result, banks must take heed and incorporate this tool into their internal evaluations.

The Cybersecurity Assessment Tool contains a two-part test:

Part 1: Inherent Risk Profile – Part 1 contains a series of charts that allow a financial institution to assess its inherent risk level with respect to five categories: (1) technologies and connection types, (2) delivery channels, (3) online/mobile products and technology services, (4) organizational characteristics, and (5) external threats. Each category contains certain activities and products, and depending on the extent and manner of the institutions involvement with respect to such activities and products its risk level is rated least, minimal, moderate, significant, or most.

- **Technologies and connection types –** For this category, a financial institution considers its risk level for various types of connection and technologies, including among other things: its total number of internet service provider ("ISP") connections, its unsecured external connections, its wireless network access, the extent to which it allows personal devices to connect to its corporate network, the number of third parties (such as vendors and subcontractors) with access to internal systems, and third-party service providers that store and process information that supports critical activities. For example, an institution will assess its risk level with respect to its wireless network access with "least" risk if the institution does not have wireless access and "most" risk if all employees have access and the institution provides access to over 1,000 users via over 100 access points.

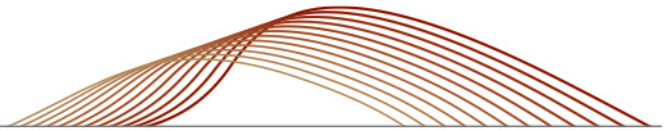
- **Delivery channels –** This category enables financial institutions to assess its risk level based on its online presence, mobile presence, and use of automated teller machines ("ATMs").

- **Online/mobile products and technology services –** This category addresses the risk level associated with certain types of products and services, including, among other things, debit and credit cards, prepaid cards, mobile wallets, person-to-person payments, and correspondent bank services.

- **Organizational characteristics –** For this category, an institution evaluates the risk level associated with its organizational characteristics based on certain factors, such as recent mergers and acquisitions, changes in IT and information security staffing, locations of branches/business presence, and locations of operations.

- **External threats –** In this category, an institution assesses its vulnerability to external threats based on the number and frequency of past cyberattack attempts.

Part 2: Cybersecurity Maturity – Part 2 enables a financial institution to determine its cybersecurity preparedness across five domains: (1) cyber-risk management and oversight; (2) threat intelligence and collaboration; (3) cybersecurity controls; (4) external dependency management; and (5) cyber-incident management and resilience. Based on various assessment factors, an institution can use the charts in Part 2 to match its cyber-preparedness in each domain to the following levels: baseline, evolving, intermediate, advanced, and innovative.



- **Cyber risk management and oversight –** In this domain, an institution assesses its governance, risk management, resources, and training and culture. For example, an institution's training and culture meets the baseline level if the institution provides annual information security training, makes situational cyber event awareness materials available to employees, has readily available customer awareness materials, and its management holds employees accountable for complying with the information security program. To meet the next level of preparedness, evolving, the institution must meet baseline level expectations and also provide continuing cybersecurity training to cybersecurity staff, provide cybersecurity training to management and business that is tailored to their job responsibilities and particular business risks, require additional training for employees with privileged account permissions, validate the effectiveness of the training, impose formal standards of conduct to hold employees accountable for compliance, actively discuss cyber-risks at business unit meetings, and ensure employees clearly understand how to identify and report potential cybersecurity issues.

- **Threat intelligence and collaboration –** This domain assesses the following factors: threat intelligence, monitoring and analyzing threats, and information sharing.

- **Cybersecurity controls –** For this domain, an institution evaluates its preparedness level based on certain factors, including its preventative controls, detective controls, and corrective controls.

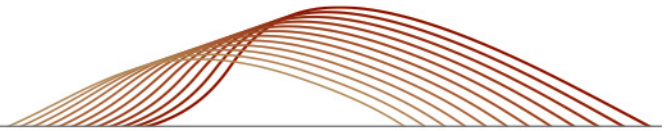
- **External dependency management –** This domain addresses the institution's preparedness level with respect to its technology connections and relationship management.

- **Cyber-incident management and resilience –** The last domain enables an institution to determine its cybersecurity program's maturity based on the sophistication of its incident resilience planning and strategy, detection, response and mitigation, and escalation and reporting.

By completing Part 1, a financial institution can identify its overall risk level, but also specifically identify areas of greatest vulnerability. This enables an institution to understand its risk and create strategies to address areas of cybersecurity weakness. By completing Part 2, a financial institution can evaluate is overall cybersecurity preparedness and determine which areas require additional improvement and resources. The Cybersecurity Assessment Tool thus provides a useful measure for financial institutions to evaluate whether their cybersecurity programs comply with the FBAs' supervisory expectations, as well as significant guidance for identifying and mitigating their cybersecurity risks.

II. The United Kingdom

The UK is often regarded as having the "best developed e-commerce in the world."[17] As such, cyber-threats pose a rather significant concern. According to a recent survey, the average cost of severe cyber-breaches for large companies in the UK starts at £1.46 million.[18] Moreover, "81% of large corporations and 60% of small businesses reported a cyber breach in 2014." [19] In light of the rise of cybercrime and its cost, the UK government is increasingly emphasizing the importance of cyber resilience.



A. Increasing Emphasis on Cyber Resilience

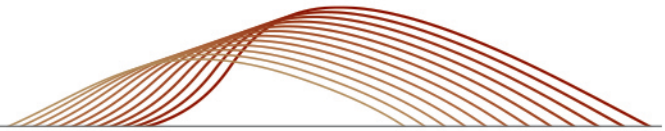
In a significant speech entitled "Cyber in Context" delivered by Andrew Gracie, the Bank of England's Executive Director for Resolution, this July, Mr. Gracie stressed the regulatory priority for the financial services sector to achieve and maintain "operational resilience" with respect to cybersecurity[20]—financial institutions must be able to continue providing critical services "that are important for their own integrity and the function of the [financial services] sector" in the event of a cyber-incident. Further, and perhaps more significantly, Mr. Gracie stated that it is now the responsibility of financial services firms "***first and foremost to ensure that they are resilient to cyber attack***."[21]

The Bank of England's emphasis on cyber-resilience includes an emerging regulatory focus on financial institutions' defensive capabilities, recovery capabilities, and effective governance,[22] as described below.

- **Defensive capabilities –** Citing to the July 1, 2015 Financial Stability Report by the Financial Policy Committee of the Bank of England, Mr. Gracie described defensive capabilities as capabilities that "enable firms to identify and withstand attack."[23] The Bank of England expects core financial sector firms, as well as their suppliers and firms they do business with, to maintain cybersecurity programs that ensure they are able to manage persistent threats.[24] Cybersecurity programs must:
  - **(1) Recognize the importance of employees –** Cybercriminals do not just exploit potential system and software weaknesses. Often, cybercriminals first target a financial firm's employees, for example through a spear phishing campaign (sending emails will malicious software attached to employees of the institution, which when opened infect the system through otherwise secure access points). Thus, it is critical that financial institutions implement and maintain adequate arrangements to ensure employees firm-wide understand cyber-risks and their responsibilities for reporting and managing those risks.
  - **(2) Adequately invest in staff and resources.**
  - **(3) Regularly test for cybersecurity vulnerability.**
- **Recovery capabilities –** Recognizing that "no network is impenetrable," the Bank of England also expects financial institutions to develop and maintain recovery capabilities that ensure institutions are able to resume secure services upon the occurrence of a cyber-incident.[25] Financial institutions must adapt business continuity planning to address cyber-risks, and should consider imposing greater "segregation between primary and backup systems."[26]
- **Effective governance –** The responsibility for understanding and responding to cyber-risks extends throughout a financial institution, from the board of directors, to senior management in each business unit, to technology specialists, and to employees.

B. Evolving Cybersecurity Guidance

On January 15, 2015, the UK Cabinet Office, Centre for the Protection of National Infrastructure, CESG, and Department for Business Innovation & Skills updated the 10 Steps to Cyber Security, originally published in 2012 and used by approximately two thirds of the largest 350 companies listed



on the London Stock Exchange.[27] This guidance is intended for any business seeking to protect itself from cybercrime.

1. **Implement Information Risk Management Regime –** Companies should assess the vulnerability of their information assets to cyber-risk and establish an enterprise-wide information risk management regime that is supported by board and management, with a risk management policy communicated to all employees and third party service providers.

2. **Ensure Secure Configuration –** Companies should establish secure baseline configurations and manage the use of their information and communications technology systems, including by removing and disabling unnecessary programs and fixing any known software and system flaws/bugs.

3. **Maintain Network Security –** Companies should ensure the networks they use are secure, including by monitoring network traffic or use for "unusual or malicious incoming and outgoing activity that could indicate an attack."

4. **Manage User Privileges –** Companies should provide users with only the privileges necessary to perform their job, limit the number of privileged accounts, and monitor account activity.

5. **Educate Users –** Companies should train employees on cyber-risks, tailored to their roles.

6. **Manage Cyber-Incidents –** Companies should establish "incident response and disaster recovery" plans and regularly test plans to ensure they appropriately address "the full range of incidents that can occur."

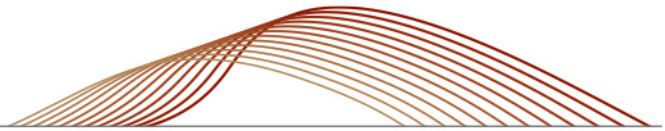
7. **Use Malware Prevention –** Companies should develop policies and procedures to directly address processes that are vulnerable to malware, such as email use. System scans should be conducted regularly and all incoming information and vendor supplied software should be scanned.

8. **Monitor –** Companies should design and maintain a strategy and procedures for continuous cyberattack monitoring that incorporates lessons learned from prior incidents.

9. **Create Controls for Removable Devices and Data –** These controls should include policies that restrict the types of devices that may be used and the types of data that may be transferred.

10. **Assess the Risks of Remote Working –** Companies should review the risks associated with employees connecting to the network remotely and develop appropriate policies to address these risks, including training employees how to ensure the security of their mobile devices.

In addition to these ten steps, the UK government has worked with the financial services industry to develop basic security controls to better protect all companies against the most common forms of cyberattacks.[28] Organizations may download guidance on these basic security controls, and even seek official certification—called a Cyber Essentials Badge—that they comply with these basic security controls upon completing a self-assessment questionnaire and submitting it for independent assessment.[29]



III. The EU

In addition to efforts by individual countries to address global cybersecurity concerns, the EU—the economic and political partnership between various European countries, including the UK—is also taking steps to address cybersecurity concerns. In early 2013, the European Commission published a directive on Network and Information Security ("NIS Directive") that is intended, among other things, to create a legal obligation for EU Member States to develop national cybersecurity strategies and cyber-incident reporting requirements, designate national authorities to monitor the compliance with these strategies and related measures, and encourage cooperation and information sharing with other Member States.[30] The scope of companies that would be subject to cyber-incident reporting requirements as well as whether information sharing between Members States would be mandatory is currently under debate.[31] The final version of the NIS Directive is currently being negotiated by the EU's Council of Ministers and the European Parliament and expected to be finalized this autumn.[32] If adopted, the Member States, including the UK, will have two and a half years to implement the NIS directive into national law.[33]

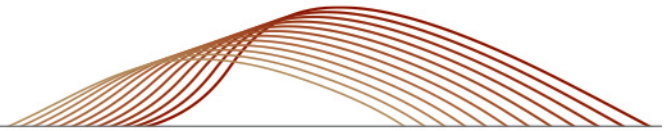
IV. International Cooperation

In addition to the country/region-specific cybersecurity efforts discussed above, governments are increasingly cooperating with each other to address the global threat of cyberattacks. Earlier this year, the U.S. and UK agreed to "bolster" threat information sharing and engage in joint cybersecurity and defense exercises to test and enhance the capacities of both countries' financial institutions and law enforcement to "respond to malicious cyber activity."[34] For example, the U.S. Computer Emergency Readiness Team and the UK Computer Emergency Readiness Team have collaborated and shared information to address and manage cyber-threats; the U.S. National Security Agency ("NSA") and the Federal Bureau of Investigation ("FBI") are working with the UK's Government Communications Headquarters ("GCHQ") and Security Service ("MI5") to establish joint cyber cells—these cells "allow staff from each agency to be co-located" and "focus on specific cyber defense topics and enable cyber threat information and data to be shared at pace and at greater scale."[35]

The U.S. and UK are not the only countries to collaborate. In February 2015, Europol's European Cybercrime Centre coordinated a joint international operation—involving investigators from the UK, Germany, Italy, and the Netherlands as well as industry participants—to shut down a botnet that had compromised 3.2 million computers world-wide.[36] The botnet—a network of infected computers—had been used by cybercriminals to obtain remote access to infected computers, whereby the criminals were able to steal personal and banking information of consumers. By working with private companies, investigators were able to locate and shut down the botnet, and developed and disseminated a remedy for infected computers. This successful operation highlights the importance of governments collaborating amongst each other and with the financial institutions and companies they regulate to address international cyber-incidents and develop a more cyber-resilient global financial system.

V. Action Plan

The increasing danger of cyberattacks and the enhanced regulatory requirements for cybersecurity compliance programs call for a detailed action plan for addressing both cyber-risk and potential regulatory risk related to cybersecurity. It must be stressed that an effective cybersecurity program requires an integrated strategy for both ongoing regulatory compliance as well as a "break glass in case of emergency" response to cyberattacks. This calls for, among other things, integrated



knowledge of bank regulatory, data, and cybersecurity and payment systems law to construct and implement an effective program.

As recently discussed in our Stay Current Alert Caught in the Crossfire: The Rising Threat of Cyberattacks on Financial Institutions and the Heightened Expectations of Financial Regulators, heightened regulatory expectations—and potential attendant regulatory and reputational risk for noncompliance in a changing regulatory environment—call for, among other things, a high level of corporate governance participation by the board of directors, senior management, and global compliance teams; management will be ultimately responsible for any cyber or regulatory problems, so management oversight is clearly required. The old saying that "an ounce of prevention is worth a pound of cure" is certainly an operative approach to plotting a successful strategy in approaching cyber operational and regulatory challenges in a changing regulatory environment. In addition to the best practices outlined here, financial institutions should:

- Utilize the FFIEC Cybersecurity Assessment Tool to evaluate their cyber-risk profiles and cybersecurity preparedness, and use the assessment results to develop/revise its policies and procedures to address any gaps and vulnerabilities identified by the assessment.

- Evaluate the institution's cybersecurity governance framework—ensure the Board of Directors discusses and understands the institutions' specific cybersecurity risk vulnerabilities and recognizes the importance of allocating sufficient resources to maintaining a robust cybersecurity compliance program, and create a chain of communication that ensures cybersecurity policy decisions reach all employees and news of cyber-incidents reaches the Board.

- Address cybersecurity concerns in all relevant policies and procedures and tailor cybersecurity policies and procedures to each business line and operation unit.

- Conduct cybersecurity training for all employees, with training tailored to each group's specific cyber-risks. It is critical that employees understand and comply with the institution's cybersecurity policies and procedures, are adequately trained to identify red flags for cyber-breaches and suspicious activity or emails, and take appropriate precautions when accessing the institution's system remotely or accessing external sites and applications from the institution's network.

- Monitor systems and controls through network scanning, audits, and independent testing.

- Thoroughly vet third party servicers and software suppliers prior to engaging their services.

- Consider whether to participate in information exchange fora with peer institutions—be sure to discuss this decision with outside counsel possessing expertise in dealing with cyberattacks and related issues such as consumer protection and regulatory compliance.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Atlanta

Todd W. Beauchamp
1.404.815.2154
toddbeauchamp@paulhastings.com

Chris Daniel
1.404.815.2217
chrisdaniel@paulhastings.com

Erica Berg Brennan
1.404.815.2294
ericaberg@paulhastings.com

Heena A. Ali
1.404.815.2393
heenaali@paulhastings.com

Kevin P. Erwin
1.404.815.2312
kevinerwin@paulhastings.com

Meagan E. Griffin
1.404.815.2240
meagangriffin@paulhastings.com

Diane Holden
1.404.815.2326
dianeholden@paulhastings.com

London

Ben Regnard-Weinrabe
44.020.3023.5185
benregnardweinrabe@paulhastings.com

Nikki Johnstone
44.020.3023.5112
nikkijohnstone@paulhastings.com

Miah Ramanathan
44.020.3023.5178
miahramanathan@paulhastings.com

Palo Alto

Cathy S. Beyda
1.650.320.1824
cathybeyda@paulhastings.com

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Stan Koppel
1.415.856.7284
stankoppel@paulhastings.com

Paul M. Schwartz
1.415.856.7090
paulschwartz@paulhastings.com

Molly E. Swartz
1.415.856.7238
mollyswartz@paulhastings.com

Washington, D.C.

V. Gerard Comizio
1.202.551.1272
vgerardcomizio@paulhastings.com

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Lawrence D. Kaplan
1.202.551.1829
lawrencekaplan@paulhastings.com

Gerald S. Sachs
1.202.551.1975
geraldsachs@paulhastings.com

Alexandra L. Anderson
1.202.551.1969
alexandraanderson@paulhastings.com

Laura E. Bain
1.202.551.1828
laurabain@paulhastings.com

Ryan A. Chiachiere
1.202.551.1767
ryanchiachiere@paulhastings.com

Lauren Kelly D. Greenbacker
1.202.551.1985
laurenkellygreenbacker@paulhastings.com

Amanda Kowalski
1.202.551.1976
amandakowalski@paulhastings.com

---

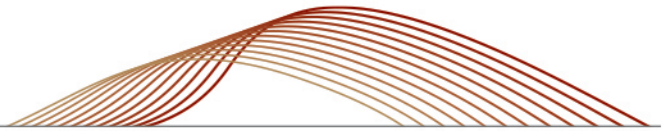
[1] Rachel McTague, *SEC Chair White Affirms Agency Has Tools to Address Risks in Industry,* ICI Viewpoints (May 8, 2015), *available at* https://www.ici.org/viewpoints/view_15_gmm_white (quoting SEC Chairman Jo White at the opening session on the final day of ICI's annual General Membership Meeting).

[2] Financial Stability Oversight Council, 2015 Annual Report (May 19, 2015), *available at* http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf; http://www.treasury.gov/press-center/press-releases/Pages/jl10055.aspx.

[3] Jason Healey's Testimony before the House Financial Institutions and Consumer Credit Subcommittee (May 19, 2015), *available at* http://financialservices.house.gov/uploadedfiles/hhrg-114-ba15-wstate-jhealey-20150519.pdf.

[4] *See* GAO Report to Congressional Requesters, Information Security, *Further Actions Needed to Address Risks to Bank Systems and Data* (January 2009).

Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2015 Paul Hastings LLP.



[5] *See* Caught in the Crossfire: The Rising Threat of cyberattacks in Financial Institutions and the Heightened Expectations of Financial Regulators (April 2015).

[6] SEC, IM Guidance Update No. 2015-02 (Apr. 2015), *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf.

[7] FSOC Expectations: Financial Stability Oversight Council, 2015 Annual Report (May 19, 2015), *available at* http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf; http://www.treasury.gov/press-center/press-releases/Pages/jl10055.aspx.

[8] FSOC Expectations: Financial Stability Oversight Council, 2015 Annual Report (May 19, 2015), *available at* http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf; http://www.treasury.gov/press-center/press-releases/Pages/jl10055.aspx.

[9] FSOC Expectations: Financial Stability Oversight Council, 2015 Annual Report (May 19, 2015), *available at* http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf; http://www.treasury.gov/press-center/press-releases/Pages/jl10055.aspx.

[10] For example, in 2014, Home Depot suffered a breach of its payment data systems, allowing a cybercriminal to gain access to the payment card information of over 50 million customers who used Home Depot's self-checkout systems at U.S. and Canada stores. *See* Home Depot Inc. Form 10-Q (Aug. 24, 2015), *available at* http://www.sec.gov/Archives/edgar/data/354950/000035495015000033/hd_10qx08022015.htm. Upon investigation, Home Depot determined that an intruder had acquired and used a self-checkout system vendor's user name and password to access the systems and deployed "custom-built malware" on the systems, and gained access to 53 million email addresses. As of August 2015, this breach has resulted in the filing of at least 57 class actions in the U.S. and Canada for claims asserted on behalf of customers, payment card issuing banks, and shareholders for damages that allegedly arose from the breach—many of which have since been consolidated for pre-trial proceedings in the U.S. District Court for the Northern District of Georgia. Additionally, state and federal agencies are investigating events related to this breach and may impose enforcement actions or other supervisory actions. According to the company's most recent 10-Q, Home Depot has already incurred over $230 million in expenses as a result of this breach.

[11] The Protecting Cyber Networks Act (H.R. 1560), available at http://intelligence.house.gov/ProtectingCyberNetworksAct; *see also* Michael S. Schmidt, Computer Attacks Spur Congress to Act on Cybersecurity Bill Years in the Making, New York Times (April 22, 2015), *available at* http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html.

[12] The National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731), *available at* https://www.congress.gov/bill/114th-congress/house-bill/1731; *see also* Cory Bennett & Cristina Marcos, House Passes Cybersecurity Bill, The Hill (April 22, 2015), *available at* http://thehill.com/blogs/floor-action/house/239756-house-passes-cybersecurity-bill.

[13] The Cybersecurity Information Sharing Act of 2015 (S. 754), *available at* https://www.congress.gov/bill/114th-congress/senate-bill/754.

[14] FFIEC, Cybersecurity Assessment Tool, https://www.ffiec.gov/cyberassessmenttool.htm.

[15] FFIEC, Cybersecurity Assessment Tool, https://www.ffiec.gov/cyberassessmenttool.htm.

[16] Letter from OCC Comptroller Curry to Government Accountability Office (June 15, 2015), *available at* http://op.bna.com/bar.nsf/id/jbar-9y2m67/$File/gao.

[17] UK Government Policy paper: 2010 to 2015 government policy: cyber security (May 8, 2015), *available at* https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security.

[18] UK Department for Business, Innovation & Skills, Press Release, *Government urges business to take action as cost of cyber security breaches doubles* (June 2, 2015), *available at* https://www.gov.uk/government/news/government-urges-business-to-take-action-as-cost-of-cyber-security-breaches-doubles.

[19] UK Government Policy paper: 2010 to 2015 government policy: cyber security (May 8, 2015), *available at* https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security.

[20] Andrew Gracie, *Cyber in Context*, speech given at the UK Financial Services Cyber Security Summit, London on July 2, 2015, *available at* http://www.bankofengland.co.uk/publications/Pages/speeches/2015/835.aspx.

[21] Andrew Gracie, *Cyber in Context*, speech given at the UK Financial Services Cyber Security Summit, London on July 2, 2015, *available at* http://www.bankofengland.co.uk/publications/Pages/speeches/2015/835.aspx.

[22] Andrew Gracie, *Cyber in Context*, speech given at the UK Financial Services Cyber Security Summit, London on July 2, 2015, *available at* http://www.bankofengland.co.uk/publications/Pages/speeches/2015/835.aspx.

[23] Andrew Gracie, *Cyber in Context*, speech given at the UK Financial Services Cyber Security Summit, London on July 2, 2015, *available at* http://www.bankofengland.co.uk/publications/Pages/speeches/2015/835.aspx.

[24] Andrew Gracie, *Cyber in Context*, speech given at the UK Financial Services Cyber Security Summit, London on July 2, 2015, *available at* http://www.bankofengland.co.uk/publications/Pages/speeches/2015/835.aspx.

[25] Andrew Gracie, *Cyber in Context*, speech given at the UK Financial Services Cyber Security Summit, London on July 2, 2015, *available at* http://www.bankofengland.co.uk/publications/Pages/speeches/2015/835.aspx.

[26] Andrew Gracie, *Cyber in Context*, speech given at the UK Financial Services Cyber Security Summit, London on July 2, 2015, *available at* http://www.bankofengland.co.uk/publications/Pages/speeches/2015/835.aspx.

[27] UK Government, *Guidance: 10 Steps: Summary* (Updated Jan. 16, 2015), *available at* https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary.

[28] https://www.cyberstreetwise.com/cyberessentials/.

[29] https://www.cyberstreetwise.com/cyberessentials/.

[30] Rachael Bishop, Update on Negotiation of NIS Directive, Bank of England (June 5, 2015), *available at* http://www.bankofengland.co.uk/financialstability/fsc/Documents/nisupdatejune2015.pdf.

[31] Rachael Bishop, Update on Negotiation of NIS Directive, Bank of England (June 5, 2015), *available at* http://www.bankofengland.co.uk/financialstability/fsc/Documents/nisupdatejune2015.pdf.

[32] Rachael Bishop, Update on Negotiation of NIS Directive, Bank of England (June 5, 2015), *available at* http://www.bankofengland.co.uk/financialstability/fsc/Documents/nisupdatejune2015.pdf.

[33] Rachael Bishop, Update on Negotiation of NIS Directive, Bank of England (June 5, 2015), *available at* http://www.bankofengland.co.uk/financialstability/fsc/Documents/nisupdatejune2015.pdf.

[34] U.S. White House Office of the Press Secretary, Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation (Jan. 16, 2015), https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

[35] U.S. White House Office of the Press Secretary, Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation (Jan. 16, 2015), https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

[36] EUROPOL, *Botnet taken down through international law enforcement cooperation* (Feb. 25, 2015), *available at* https://www.europol.europa.eu/newsletter/botnet-taken-down-through-international-law-enforcement-cooperation.