Georgia Law Review

Volume 50 | Number 1 Article 7

2015

Cyber Risks: Emerging Risk Management Concerns for Financial Institutions

Kristin N. Johnson
Seton Hall University School of Law

CYBER RISKS: EMERGING RISK MANAGEMENT CONCERNS FOR FINANCIAL INSTITUTIONS

Kristin N. Johnson[*]

TABLE OF CONTENTS

[*] Professor of Law; Director of the Regulation, Governance and Risk Management Program, Seton Hall University School of Law; Edmund A. Walsh School of Foreign Service, Georgetown University, B.S.; University of Michigan Law School, J.D. For his careful review of earlier drafts, I thank Carlos López. For significant research assistance, I thank my research assistant Sarah Wilbur.

I. INTRODUCTION

Disappointingly, regulatory reform is often backward-looking. While regulators toil to implement rules to prevent the last crisis from reoccurring, new and more perilous threats evade detection. With increasing frequency, cyberattacks threaten critical infrastructure resources such as nuclear centrifuges, electrical grids, and air defense systems. Cyberattacks pose a burgeoning and underexplored universe of emerging concerns impacting areas as diverse as big-box retail stores, casual-dining chains, online retail auctions, and national security. Even if the antics of high school hackers or a Bonnie-and-Clyde-smash-and-grab of sensitive client data is not alarming, a malicious wave of outages executed as an Ocean's Eleven heist that disarms and disables an international securities exchange demands a regulatory response.

Cyber threats designed to disrupt or deny service for the small body of systemically important financial institutions that intermediate global commerce and banking create a special universe of concerns. The financial markets sector is broad, encompassing conventional depository banks, securities, commodities, and derivatives platforms or exchanges; investment banks; hedge, pension, and mutual funds; brokerage firms; and, in some cases, insurance companies.[1] The number of data breaches threatening to interrupt the services offered by these institutions could shock, debilitate, or even (temporarily) paralyze the global economy.[2]

Startling examples underscore these concerns. In 2013, hackers penetrated Citigroup's network and compromised data related to tens of thousands of customer accounts.[3] A year later, JP Morgan Chase endured a similar cyberattack affecting more

---

[1] Kristin N. Johnson, *Addressing Gaps in the Dodd-Frank Act: Directors' Risk Management Oversight Obligations*, 45 U. MICH. J.L. REFORM 55, 64 (2011).

[2] *See Protecting Consumer Information: Can Data Breaches Be Prevented?: Hearing Before the H. Subcomm. on Commerce, Mfg., & Trade*, 113th Cong. 1, 1–2 (2014) (statement of Lisa Madigan, Att'y Gen. of Ill.), *available at* http://docs.house.gov/meetings/IF/IF17/20140205/101714/HMTG-113-IF17-Wstate-MadiganL-20140205.pdf ("Since 2005, there have been over 4,000 data breaches nationally and over 733 million records compromised.").

[3] Randall Smith & Alison Tudor, *Citi, Confirming Breach, to Issue Tens of Thousands of New Cards*, WALL ST. J. (June 9, 2011, 6:22 PM), http://www.wsj.com/articles/SB10001424052702304259304576374713184158184.

than 76 million households.[4] Rumors posit that, within the last two years, hackers caused outages, disrupting service for the two largest securities exchanges in the world—the NASDAQ and the New York Stock Exchange.[5] The significance of the largest financial institutions in the global economy, the interconnectedness of these businesses, and their shared dependence on technology create a new body of systemic risk concerns.[6] If hackers breach the Internet-based communications systems at the heart of international commercial banking infrastructure, the devastation and damage would be difficult, if not impossible, to calculate.

Whether the intruder is a hacker, hacktivist, lone wolf exploring his decryption skills, or a cyberterrorist, the dangers of cyberattacks are indisputable. As cyberattacks multiply exponentially, governments, corporations, and citizens scramble to mount a successful defense. For financial institutions, cyberattacks employing worms, viruses, trojan horses, peripheral devices, electronic transmitters, embedded code, or human operators create the most pernicious emerging risk management concerns.[7] Consequently, the staggering size, sophistication, and diversity of styles of cyber incidents targeting financial institutions and financial intermediaries create systemic risk concerns.

II. THE MANY FACES OF FINANCIAL MARKET RISK

Financial market participants have a long history of managing risks. Tales of Thales, the Greek philosopher, arranging a

---

[4] Emily Glazer & Danny Yadron, *J.P. Morgan Says About 76 Million Households Affected by Cyber Breach*, WALL ST. J. (Oct. 2, 2014, 9:32 PM), http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372.

[5] *See, e.g.*, Nathaniel Popper, *Wall Street's Exposure to Hacking Laid Bare, Dealbook*, WALL ST. J. (July 25, 2013, 8:34 PM), http://dealbook.nytimes.com/2013/07/25/wall-streets-exposure-to-hacking-laid-bare/?_r=0.

[6] *See generally* Lawrence G. Baxter, *Betting Big: Value, Caution and Accountability in an Era of Large Banks and Complex Finance*, 31 REV. BANKING & FIN. L. 765 (2012) (discussing the costs and benefits of large-scale financial institutions).

[7] *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 442 (2012) (noting three main categories of cyberattacks).

financial agreement to guarantee access to an olive press, or descriptions of the Medici dynasty's structured credit arrangements all illustrate the use of risk calculation and risk management strategies. Long after Aristotle's first descriptions of structured contracts, financial market participants have continued to identify and explore the contours of risk management. Defining even foundational concepts in risk management theory, however, creates consternation. The word "risk" itself is a neutral term and connotes the possibility of either a positive or negative outcome;[8] it simply describes the element of uncertainty with respect to an outcome.[9] Yet, many commonly use the term risk to signal danger.

To describe financial market risks as complex is an understatement. Financial market participants face various classes of risks, including credit, interest rate, market, and liquidity risks.[10] Risk management strategies enable businesses to identify, assess, or mitigate outcomes that could lead to a loss.

---

[8] GEOFFREY PARSONS MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 535 (2014).

[9] Roger Miller & Donald Lessard, *Evolving Strategy: Risk Management and the Shaping of Large Engineering Projects* 4 (MIT Sloan Sch. of Mgmt., Working Paper No. 4639–07, 2007), *available at* http://ssrn.com/abstract=962460 ("Risk is the possibility that events, their resulting impacts, and their dynamic interactions will turn out differently than anticipated. Risk is typically viewed as something that can be described in statistical terms, while uncertainty is viewed as something that applies to situations in which potential outcomes and causal forces are not fully understood.").

[10] ANTHONY SAUNDERS & MARCIA MILLON CORNETT, FINANCIAL MARKETS AND INSTITUTIONS 576 tbl.9-1 (5th ed. 2012). Because the attributes of the business models of financial institutions vary, the risks described here may materialize differently for each type of financial institution. Credit risk, for example, is "the risk that promised cash flows . . . may not be paid in full." *Id.* Liquidity risk may result from unexpected liability that forces a firm "to liquidate assets in a very short period of time and at low prices." *Id.* Interest rate risk is "incurred . . . when the maturities of [a firm's] assets and liabilities are mismatched and interest rates are volatile." *Id.* Longer maturity assets pose increased risk for financial institutions because interest rates can change from year to year. OFFICE OF INVESTOR EDUC. & ADVOCACY, SEC, SEC PUB. NO. 151, INTEREST RATE RISK—WHEN INTEREST RATES GO UP, PRICES OF FIXED-RATE BONDS FALL 4 (2013), http://www.sec.gov/investor/alerts/ib_interestraterisk.pdf. Market risk describes "[t]he risk incurred in trading assets and liabilities due to changes in interest rates, exchange rates, and other asset prices." SAUNDERS & CORNETT, *supra*, at 582. *See generally* BASEL COMM. ON BANKING SUPERVISION, BANK FOR INT'L SETTLEMENTS, AMENDMENT TO THE CAPITAL ACCORD TO INCORPORATE MARKET RISKS (2005), http://www.bis.org/publ/bcbs119.pdf (providing for the measurement of market risk).

Successful risk management strategies may engender a multitude of benefits.

The diversity of risks, however, stymies efforts to outline optimal risk management strategies. To manage risks, business may rely on a wealth of endogenous tools, such as enterprise risk management (ERM) strategies[11] or corporate governance structures, and exogenous solutions, such as minimum capital ratios or living wills.[12] Financial institutions' unique business models typically require customized risk management strategies.[13] While financial institutions grapple with many risk management challenges, none of the tools developed to date promise to eliminate and too few serve to effectively mitigate cyber risks. Addressing cyber risks may remain difficult because theorists, regulators and legislators struggle to define with specificity which acts constitute cyber threats.

Similar to the difficulties that arise in financial market risk theory, defining cyber risks creates a threshold dilemma for risk management strategists. Notwithstanding the popularity of concepts such as "cyber-incident," "cybercrime," and "cyberattack," there are no universally adopted definitions for these terms. Generally, a cyber-incident refers to an unauthorized act that enables a technology user to access proprietary systems or infrastructure or to review, download, manipulate, or extract

---

[11] *See* Kristin N. Johnson, *Macroprudential Regulation: A Sustainable Approach to Regulating Financial Markets*, 2013 W. ILL. L. REV. 881, 899 (describing the complexity of the risk management strategies businesses adopt, including CRMs, which "attempt to comprehensively measure risks").

[12] *See* Victoria McGrane & James Sterngold, *Fed Sets Tough New Capital Rule for Big Banks*, WALL ST. J. (Dec. 9, 2014, 8:43 PM), http://www.wsj.com/articles/fed-proposes-extra-capital-requirement-for-8-biggest-u-s-banks-1418154076 (noting regulatory imposition of "fatter capital cushions . . . to make the financial system less risky"); Ryan Tracy & Victoria McGrane, *Big U.S. Banks Refile 'Living Wills' After Regulatory Rebuke*, WALL ST. J. (July 6, 2015, 10:53 PM), http://www.wsj.com/articles/big-u-s-banks-refile-living-wills-after-regulatory-rebuke-1436212747 (reporting that, among others, J.P. Morgan Chase & Co. re-submitted plans for reorganization to help mitigate damage in the event of their financial failure). *See generally* RENÉ M. STULZ, RISK MANAGEMENT & DERIVATIVES (2003) (providing insight into the way businesses can maximize corporate value through various risk management techniques).

[13] *See* Johnson, *supra* note 1, at 61 (explaining that financial institutions must deal with risks associated with "sophisticated investment decisions").

confidential or sensitive data.[14] Theorists refer to a cybercrime as "any crime that is facilitated or committed using a computer, network, or hardware device."[15] Not all cyber incidents rise to the level of criminality. Consequently, criminal law may not serve as an effective mechanism for identifying cyber threats. Moreover, categories of cyber-activities can be both over- and under-inclusive.

Commentators offer many definitions for the term "cyberattack." Military strategists, for example, use the term to describe hostile acts against a territorially sovereign nation,[16] an approach that is less useful for private businesses such as international banking and payment institutions with affiliates domiciled in countries around the world. Because of the variety and complexity of cyberincidents identified by commentators, defining the term cyberattack may prove to be difficult and controversial.

One might define "cyberattack" based on the identity of the perpetrator. Hackers, foreign agents engaged in espionage, or terrorists may penetrate firewalls, access confidential information, manipulate accounts, and disrupt key institutions.[17] Thus, the definition may envelope a broad spectrum of gifted teenagers,

---

[14] *See, e.g.*, *Report Cyber Incidents*, DEP'T OF HOMELAND SEC. (July 20, 2015), http://dhs.gov/how-do-i/report-cyber-incidents (defining cyber incident).

[15] Sarah Gordon & Richard Ford, *On the Definition and Classification of Cybercrime*, 2 J. COMPUTER VIROLOGY 13, 14 (2006); *see also* Convention on Cybercrime, pmbl., Nov. 23, 2001, C.E.T.S. No. 185 (entered into force July 1, 2004), *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (targeting an "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data").

[16] Memorandum from Gen. James E. Cartwright, Vice Chair, Joint Chiefs of Staff, U.S. Dep't of Def., for the Chiefs of the Military Servs., Commanders of the Combatant Commands & Dirs. of the Joint Staff Directorates 5 (2010), *available at* http://info.publicintelligence.net/DoD-JointCyberTerms.pdf ("Cyber Attack: A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.").

[17] *See* FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES 4 (2015), *available at* https://www.finra.org/file/report-cybersecurity-practices (listing the top cyber threats to large firms).

political activists, greedy criminals, or fame-seeking hackers. A forthcoming article explains the merits of a broad definition that invokes principles of international law while eschewing the limits of the international rule-making processes.[18] The article encourages drawing from domestic national security, criminal, intellectual property, and securities law to outline a comprehensive legal framework for regulating cyber risks in financial markets.

III. CYBER RISKS AND FINANCIAL MARKETS

Recent turmoil in financial markets[19] casts a spotlight on the perils of systemic risk—the concern that a single shock or series of shocks may trigger the insolvency of one or more systemically important financial institutions.[20] Efforts to regulate systemic risk pose indisputable challenges. First, mitigating systemic risk requires properly identifying the sources of systemic risk. Second, regulation must be well-tailored to mitigate the threat of systemic risks. Finally, engineering effective regulation involves ensuring competent oversight and enforcement. Focusing solely on the first step in this process, the evidence demonstrates that cyber risks have the potential to create systemic risks.

Credit and capital markets are critical infrastructure resources.[21] Similar to other pseudo-commons, assets in

---

[18] Kristin Johnson, *Managing Cyber Risks*, 50 GA. L. REV. (forthcoming 2016).

[19] *See, e.g.*, FIN. CRISIS INQUIRY COMM'N, THE FINANCIAL CRISIS INQUIRY REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON THE CAUSES OF THE FINANCIAL AND ECONOMIC CRISIS IN THE UNITED STATES, at xv (2011), *available at* http://fcic-static.law.stanford.edu/cdn_media/fcic-reports/fcic_final_report_conclusions.pdf ("As this report goes to print, there are more than 26 million Americans who are out of work, cannot find full-time work, or have given up looking for work. About four million families have lost their homes to foreclosure and another four and a half million have slipped into the foreclosure process or are seriously behind on their mortgage payments. Nearly $11 trillion in household wealth has vanished, with retirement accounts and life savings swept away.").

[20] *See* Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193, 204 (2008) (defining systemic risk as the threat that "(i) an economic shock such as market or institutional failure triggers (through a panic or otherwise) either (X) the failure of a chain of markets or institutions or (Y) a chain of significant losses to financial institutions, (ii) resulting in increases in the cost of capital or decreases in its availability, often evidenced by substantial financial-market price volatility").

[21] *See* John C. Coffee, Jr., *Extraterritorial Financial Regulation: Why E.T. Can't Come Home*, 99 CORNELL L. REV. 1259, 1269–70 (2014) (noting the relevance of "commons"

international commerce flow through openly-accessible, nonrival, and nonexcludable markets as businesses, individuals, and governments transact with counterparties around the world.[22] A network of exchanges, clearinghouses, and payment systems enable financial market participants to transfer cash, securities, commodities, and other assets across territorial borders in seconds.[23] Technological innovations enable financial market participants to execute transactions with little regard to territorial boundaries.[24] These institutions provide critical benefits, enhance market efficiency, permit more accurate price discovery, and promote greater portfolio diversification.[25]

---

literature to the regulation of financial institutions). John Coffee, Kristin Johnson, and Steven Schwarz are among a pioneering group of scholars exploring the application of Garrett Hardin's tragedy of the commons to international financial markets. *Id.*; *see also* Iman Anabtawi & Steven L. Schwarcz, *Regulating* Ex Post*: How Law Can Address the Inevitability of Financial Failure*, 92 TEX. L. REV. 75, 90 (2013) (acknowledging that financial markets can suffer from "a type of tragedy of the commons in which finite capital resources are exploited"); Steven L. Schwarcz, *Protecting Financial Markets: Lessons from the Subprime Mortgage Meltdown*, 93 MINN. L. REV. 373, 386 (2008) (comparing the exploitation of scare resources in a tragedy of the commons to the exploitation of scare resources in a financial system); Kristin N. Johnson, *Things Fall Apart: Regulating the Credit Default Swap Commons*, 82 U. COLO. L. REV. 167, 174 (2011) (applying the tragedy of the commons to modern financial markets). The innovative application of the tragedy of the commons parable to financial markets offers a point of departure for considering alternative solutions to regulatory questions prompted by cross-border transactions or financial market sectors characterized by market participants executing transactions through trading institutions operating in multiple jurisdictions.

[22] Johnson, *supra* note 22, at 174–75.

[23] *See* JAMES MANYIKA ET AL., MCKINSEY GLOBAL INST., GLOBAL FLOWS IN A DIGITAL AGE: HOW TRADE, FINANCE, PEOPLE, AND DATA CONNECT THE WORLD ECONOMY 23, 61 (2014) (discussing the increasingly international nature of commercial transactions); Chris Brummer, *Post-American Securities Regulation*, 98 CAL. L. REV. 327, 346 (2010) (discussing how "innovations like the Internet" have drastically improved the rapidity and accuracy of international sales transactions).

[24] *See* Stavros Gadinis & Howell E. Jackson, *Markets as Regulators: A Survey*, 80 S. CAL. L. REV. 1239, 1257–58, 1298 (2007) (concluding that many stock exchanges are "expanding their operations across national borders").

[25] *See* Jeremy C. Kress, *Credit Default Swaps, Clearinghouses, and Systemic Risk: Why Centralized Counterparties Must Have Access to Central Bank Liquidity*, 48 HARV. J. LEGIS. 49, 65 (2011) ("The benefits of [clearinghouses] include loss mutualization and credit risk homogenization, multilateral netting, and information aggregation."); Jerry W. Markham & Daniel J. Harty, *For Whom the Bell Tolls: The Demise of Exchange Trading Floors and the Growth of ECNs*, 33 J. CORP. L. 865, 882 (2008) (stating that the transparency of modern stock exchanges "provides a price discovery mechanism"); Kristin N. Johnson, *Governing Financial Markets: Regulating Conflicts*, 88 WASH. L. REV. 185, 189, 209 (2013) (noting that self-regulatory organizations, including financial institutions such as the British Banker's

Cyberattacks of sufficient magnitude may create shocks that trigger systemic risks. The Financial Industry Regulatory Authority (FINRA) reports frequent and sophisticated cyber attacks on financial institutions.[26] Cybersecurity concerns for these businesses threaten the stability of financial markets; the loss of billions of dollars; and breaches of private data related to the banking, savings, and commercial accounts and wire-transfers or transactions of millions of clients, including businesses, governments, municipalities, non-profit organizations, and individuals. According to the New York State Department of Financial Services, cyberattacks pose an ominous risk to financial markets and may "wreak serious havoc on the financial lives of consumers."[27] The Department of Homeland Security recognizes financial institutions and financial market intermediaries as a critical infrastructure system deserving the highest level of protection against cyberattacks.[28]

IV. SOLUTIONS TO CYBER THREATS IN FINANCIAL MARKETS

No single domestic or international law or regulator addresses cyberthreats. Cyberspace is governed by a patchwork of state, federal, and international regulations—leaving significant regulatory gaps. Cyber risk-management often involves time-sensitive questions and concerns; delegating regulation to legislators' slow-moving rule-making processes may leave financial markets exposed to preventable cyberattacks. The best path forward may be found in amending and clarifying existing

---

Association, "frequently adopt and implement industry standards that enhance efficiency and organization," and that complex financial instruments, such as credit derivative agreements, help diversify investor portfolios).

[26] FIN. INDUS. REGULATORY AUTH., *supra* note 17, at 1.

[27] Press Release, N.Y. Dep't of Fin. Servs., NYDFS Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments (Dec. 10, 2014), http://www.dfs.ny.gov/about/press/pr1412101.htm.

[28] *See What Is Critical Infrastructure?*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/what-critical-infrastructure (last published Sept. 17, 2015) ("The nation's critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health.").

regulation rather than negotiating new agreements specifically designed to achieve cyberpeace.[29]

Three leading regulators in financial markets have released influential cybersecurity guidelines. FINRA recommends firms voluntarily implement the following cybersecurity best practices: (1) adopt a defense-in-depth strategy, layering several independent security controls throughout their IT system; (2) limit users' and employees' access to the firm's data and systems; (3) encrypt data to protect confidentiality and information integrity; (4) simulate third-party attempts to penetrate the firm's system to test any potential cybersecurity weaknesses; and (5) monitor third party vendors' cyber security standards.[30] While the FINRA standards will prove an invaluable contribution in identifying, preventing, and addressing cyber threats, the guidelines are not mandatory. The challenges with self-regulation accomplished through voluntary standards in the financial services sector are well documented.[31]

The Securities Exchange Commission's (SEC) Division of Corporation Finance published disclosure guidance requiring companies registering securities for sale to the public and those subject to periodic reporting requirements to indicate potential cyber risks, cyber incidents that have transpired, decisions to outsource material cyber functions and insurance coverage relevant to cyber events.[32] While the disclosure obligations are required, the *ex post* nature of the disclosure and the general cautionary language offers firms limited guidance regarding best practices for reporting and measuring potential concerns, and sharing and understanding industry-wide threats. The SEC disclosure obligations make no attempt to discuss addressing cyber threats against individual firms or the intermediaries that facilitate trading registered securities.

---

[29] *See, e.g.*, SCOTT J. SHACKLEFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS AND RELATIONS: IN SEARCH OF CYBER PEACE 306–11 (2014) (exploring an international framework for managing cyberattacks).

[30] FIN. INDUS. REGULATORY AUTH., *supra* note 17, at 16–26.

[31] Kristin N. Johnson, *Governing Financial Markets: Regulating Conflicts*, 88 WASH. L. REV. 185, 189, 209 (2013).

[32] DIV. OF CORP. FIN., SEC, CF DISCLOSURE GUIDANCE: TOPIC NO. 2, CYBERSECURITY (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguid ance-topic2.htm.

Finally, in response to Executive Order 13636 issued by President Barack Obama in February 2014, the National Institute of Standards and Technology (NIST) released the Framework for Improving Critical Infrastructure Cybersecurity to address cyber risks.[33] Similar to the FINRA guidelines, the NIST standards are voluntary.[34] While the NIST guidelines establish a standard of care in the industry, each firm may cherry pick which elements it implements and when to introduce relevant reforms. The NIST guidelines, however, begin to fill the gap by introducing cyber security best practices specifically designed to address shortcomings in the financial services sector.[35]

A coordinated effort across domestic regulators is required, but market participants must also collaborate and share information regarding successful and thwarted attacks. The creation of the Financial Services-Information Sharing Analysis Center (FS-ISAC) correctly supports cooperative efforts to mitigate industry-wide cyber risks.[36] Through such programs, financial institutions and third-party vendors, engaged in internal risk management processes such as development of redundant systems,[37] may share

---

[33] NAT'L INST. OF STANDARDS. & TECH., *Framework for Improving Critical Infrastructure Cybersecurity* (2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[34] *Id.* at 1.

[35] Press Release, Nat'l Inst. of Standards & Tech., NIST Seeks Comments on Guide to Help Financial Services Sector Manage IT Assets (Oct. 26, 2015), http://www.nist.gov/itl/acd/ncce/20151026nccoeguide.cfm.

[36] *See generally* Financial Services Information Sharing and Analysis Center, https://www.fsisac.com (last visited Dec. 2, 2015). FS-ISAC publishes guidance for addressing operational risk management concerns and promotes information sharing among financial institutions. *See, e.g.*, FINANCIAL SERVICES-INFORMATION SHARING AND ANALYSIS CENTER ET AL., BEST PRACTICES FOR U.S. FINANCIAL INSTITUTIONS: REDUCING RISKS ASSOCIATED WITH DESTRUCTIVE MALWARE (2015), *available at* https://www.fsisac.com/sites/default/files/news/Destructive%20Malware%20Paper%20TLP%20White%20VersionFINAL2.pdf (providing guidance related to destructive malware). To address anti-trust concerns related to information sharing among firms, the Federal Trade Commission and the Department of Justice issued a policy statement explaining that cyber risk and risk management information sharing are to be encouraged. Press Release, FTC, FTC, DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information (Apr. 10, 2014), https://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity.

[37] Redundancy refers to backing up data in multiple locations and being able to access that data in multiple ways to prevent catastrophic losses and to provide resiliency. *See* Derek Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 637 (2011). Redundancy applies both

information regarding trends, outcomes, and emerging technologies.

V. CONCLUSION

Cyberattacks pose a significant and alarming threat to financial markets, a deeply integrated network of exchanges, clearinghouses, and payment systems. In the increasingly interconnected universe of businesses that comprise financial markets, participants rely significantly on technology to execute trades, transfer cash and other assets, and facilitate payments. Cyber risks threaten to create systemic risks and engender negative externalities that spill over and impact governments, businesses, and communities around the world. Epistemological questions ensconce the theories of risk management and cyberspace and a fragmented body of domestic and international regulation leave chasm-sized gaps in existing cyberlaw. Exploring the questions surrounding these issues offers the best approach for beginning to outline a comprehensive domestic and international regulatory framework aimed at achieving cyberpeace.

---

to data storage (to guarantee that a company's data is safely kept in more than one place) and to Internet connection (to ensure continued access to the Internet in case someone disrupts either the company's Internet connection or the application service provider's connection). Risk assessments, redundancy, and information sharing can help these financial institutions identify and prioritize potential cyberattacks they could face and the steps they need to take to try and prevent these attacks, as well as measures for mitigation and containment for when a breach occurs.