

50 Ga. L. Rev. 547

Georgia Law Review

Winter, 2016

Essay

MANAGING CYBER RISKS

Kristin N. Johnson^{al}

Copyright (c) 2016 Georgia Law Review Association, Inc.; Kristin N. Johnson

Table of Contents

I.	Introduction	548
II.	Understanding, Managing , and Mitigating Systemic Risks	556
A.	IDENTIFYING RISKS	556
B.	WHY ARE SYSTEMIC RISKS SPECIAL?	559
1.	Understanding Systemic Risks	560
2.	A Brief Survey of RiskManagement Approaches	561
C.	SYSTEMIC RISK MITIGATION	565
III.	Emerging Systemic Risk Concerns: Cybersecurity Threats	568
A.	DEFINING CYBERSECURITY THREATS	569
B.	CYBER RISKS AND FINANCIAL INSTITUTIONS	571
IV.	Regulating Cyberspace	576
A.	TOWARD TRANSPARENCY AND INFORMATION SHARING	577
1.	The Cybersecurity Information Sharing Act of 2015	578
2.	Weaknesses of the CISA	580
B.	ALTERNATIVE INITIATIVES	583
V.	Conclusion	591

***548 I. INTRODUCTION**

Cybersecurity concerns are an ever-increasing threat.¹ The rising cost, frequency, and severity of data breaches² now dominate **riskmanagement** discussions.³ Over the last ten years, more than 4,000 known data breaches have shocked, debilitated, and even (temporarily) paralyzed markets.⁴ Commentators estimate that potentially billions of records containing confidential or sensitive data have been compromised.⁵ Experts suggest that data breaches cost the global economy more than \$400 billion dollars of losses annually.⁶ Heads of state around the world have committed to enhance **cybersecurity**, to protect intellectual property and confidential or sensitive data, and to aggressively ***549** prosecute cybercriminals.⁷ Private sector efforts to mitigate the effects of cyberattacks reflect similar goals.⁸ As cyberattacks multiply, governments, corporations, and citizens scramble to mount a successful defense against cyber-intrusions. The size, sophistication, and diversity of styles of the cyberattacks renders these activities among the most perilous of emerging **riskmanagement** concerns.

President Obama recently announced that **cybersecurity** is “one of the most serious economic and national security challenges we face as a nation.”⁹ By the admission of the President, however, the United States is woefully underprepared

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

to address the threat of cyberattacks.¹⁰ For the government and certain critical industries, **cybersecurityriskmanagement** concerns may have catastrophic consequences. By targeting these industries, hackers may disrupt business operations,¹¹ gain access to or manipulate sensitive or confidential data,¹² or simply steal intellectual property¹³ or tangible assets.¹⁴

***550** Cyberattacks capture national and international attention because of their pervasive effects. For example, in December 2013, Target announced that the discount retailer company had suffered a data breach.¹⁵ The hackers who orchestrated the crime obtained the confidential credit and debit card information of more than 40 million customers.¹⁶ As investigations ensued, Target continued to adjust its estimate of the number of records accessed, ultimately reporting that hackers captured the personal data of as many as 110 million customers.¹⁷ In 2014, in a data breach involving a similar method of deception, hackers invaded home improvement retailer Home Depot's records and acquired 56 million customers' ***551** credit and debit account information and 53 million customers' e-mail addresses.¹⁸

In both the Target and Home Depot data breaches, malicious software (malware) infected the business's cash register system enabling hackers to view, record, and alter data.¹⁹ One **risk** from such a breach of customers' credit and debit card information and personal data is that hackers may make counterfeit cards and commit fraud.²⁰ Research firm Aite estimates that the costs of counterfeit fraud reached \$1.35 billion in 2008 and accounted for 15.7% of the total \$8.6 billion in credit and debit card fraud in the same year.²¹

These large-scale data breaches are not unique to chain retailers. While cyberattacks against retailers are troubling, hackers' efforts to breach the firewalls of financial institutions and exchanges at the center of international commercial enterprise-financial institutions-could threaten to destabilize global economic systems.

The architecture of modern markets makes financial institutions critical to global commerce and to the operations of local, state, national, and foreign governments.²² The universe of ***552** financial institutions is broad. It includes conventional depository banks, as well as securities, commodities, and derivatives platforms or exchanges; investment banks, hedge, pension, and mutual funds; brokerage firms; and, in some cases, insurance companies. Pursuant to federal regulation and consistent with their business models, large financial institutions acquire, collect, and retain significant volumes of personal information. Possession of and control over this sensitive data makes financial institutions and retailers highly attractive targets for hackers.²³

Shocking examples of breaches at financial institutions underscore these concerns. In 2013, hackers penetrated network systems at both Citibank and JP Morgan Chase.²⁴ Consequently, hackers accessed the data related to tens of thousands of customer accounts. While the threat to individual financial institutions is alarming, 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.²⁵ If hackers successfully disrupt the sources of securities and commodities exchange platforms or the transaction network of the payment and banking system, the devastation and damage would trigger a chain of negative ***553** consequences for businesses, governments, and individuals around the world.

Cyber **risks** are evolving and this metamorphosis requires a prompt regulatory response. Unlike liquidity, credit, market, and other types of financial market **risks**, cyber **risks** threaten to trigger a series of losses far more debilitating than a run on any individual financial institution. Cyber **risks**, by their nature, reflect a sophisticated and complex concern. Cyber **risks** threaten disruptive attacks against interconnected and systemically important banking and non-banking

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

financial institutions. Even a temporary disruption in banking, payment, and financial instruments trading platforms may destabilize markets. The consequences of a well-targeted cyberattack cast a shadow that may reach institutions and individuals all over the country and possibly in many countries around the world.

It is possible that concerns regarding cyber threats and financial markets are overstated. While cyberattacks have yet to undermine the national economy, hackers continue to develop new methods of penetrating proprietary systems. The Carbanak cyberattack in 2013 evinces the imminent nature and high probability of this new front and establishes that we are on the edge of a new digital frontier.²⁶

In late 2013, the Carbanak cybergang unleashed a cyberattack on more than one hundred financial institutions across thirty different countries.²⁷ Over a period of several months, Chinese and European hackers remotely programmed automatic teller machines (ATMs) to dispense cash and transfer millions of dollars in funds from customers' accounts in Europe, the United States, and Japan.²⁸ Hackers gained control over the internal operational systems of the individual financial institutions by baiting bank employees with e-mails that appeared to be from colleagues, urging the employees to download malware.²⁹ For nearly two *554 years, the hackers used software to monitor employees' daily routines, captured videos and screenshots, and reviewed and recorded video feeds.³⁰ Hackers later used the intelligence they gathered to access the banking institutions' systems and impersonate employees while the malware remotely triggered ATMs to dispense cash and to transfer funds.³¹

Data breaches that result in fraud and theft create noteworthy risks for financial institutions and many scholars and commentators have explored these issues. This Essay suggests that the most significant cyber threats facing financial institutions loom under-explored and under-theorized. Cyber threats against financial intermediaries that link systemically important financial institutions create systemic risk concerns. Financial institutions are critically dependent on technology to conduct their business and their role in the domestic and international economy suggest that disastrous consequences may follow if the operations of these channels of commerce experience disruption.

In 2011, one of the largest international securities exchanges, NASDAQ, confirmed that its computer network was hacked and confidential documents were accessed.³² The brazen penetration of this venerable exchange, which provides a securities platform impacting market prices and economic stability around the world, shocked market participants. Theories regarding the hackers' motivations range from presumptions that the intruders were seeking nonpublic inside information to whispers of terrorism, theft, or wire fraud. The intentions that prompted the hackers to attack the exchange's network are far less troubling than the mere fact that their efforts were successful.

Adopting the perspective that cyber risks may engender catastrophic losses, Congress adopted the Cybersecurity Information Sharing Act of 2015 (CISA).³³ The Act designates a *555 method for federal and state governments, as well as private entities, to voluntarily exchange information regarding cybersecurity threats, seeks to prevent and mitigate cyberattacks, and establishes a process for real-time sharing and receipt of cybersecurity threat information.³⁴

This Essay approaches cyber risks as systemic risks. It presents an outline of principles governing the development of cyber risk regulation by normatively and descriptively examining the evolution of cyber regulation in financial markets and identifying promising opportunities to thwart hackers and others who seek to disrupt securities and commodities exchanges, banking institutions, and payment systems. Both endogenous and exogenous cyber threats reveal weak internal controls, crumbling firewalls, or failures to build redundant protective systems. Because these businesses are

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

publicly traded companies competing in capital markets to attract investors, it is unlikely that these institutions will be motivated to reveal **risk** exposures if the sole reward is protecting the public good.

This Essay examines these questions and proposed responses. Part II of this Essay examines the theory of **riskmanagement** concerns and argues that **cybersecurity** concerns constitute the newest **riskmanagement** frontier. Part III examines the contours and definitions of terms at the center of the **cybersecurityriskmanagement** crisis in the financial services industry and explains the **cybersecurity** concerns that plague financial institutions. Part III also surveys proposed solutions designed to address **cybersecurity** concerns at large, systemically important financial institutions. Part IV examines the contours of the CISA and argues that information sharing is a critical component to successfully defend against cyberattacks aimed at systemically important financial institutions and financial intermediaries. Information sharing alone, however, is an incomplete solution. This Essay evaluates the contributions of industry-initiated and *556 federal agency-proposed alternatives to the growing cyber **risks** that threaten domestic and international financial institutions.

II. UNDERSTANDING, **MANAGING**, AND MITIGATING SYSTEMIC **RISKS**

Financial market regulation and literature exploring regulation frequently implore market participants to take action to reduce the likelihood that “systemic **risks**” will materialize. The notion of systemic **risk** animates discussions regarding the causes of the recent financial crisis and justifications for the imposition of regulation designed to prevent future crises. Notwithstanding the use of this popular term, there is no widely accepted or uniform definition of systemic **risk**. Unable to define systemic **risk**, scholars, commentators, and regulators struggle to develop well-tailored regulation to **manage** and mitigate systemic **risk**. Part II.a identifies several commonly occurring **risks** in financial markets. Part II.b argues that the definition of systemic **risk** is evolving, creating challenges for regulators attempting to **manage** or mitigate systemic **risk**.

A. IDENTIFYING **RISKS**

The term **risk** is used colloquially to suggest that an action or decision may lead to a negative outcome.³⁵ In truth, **risk** taking may lead to either a positive or negative outcome.³⁶ **Risk** simply describes an element of uncertainty or the chance for a range of possible outcomes.³⁷

*557 Financial markets and financial institutions face various classes of **risk** including credit, liquidity, interest rate, and market **risk**.³⁸ Lending arrangements give rise to credit **risks** or concerns that a debtor may fail to repay an outstanding debt obligation. There are several types of contractual arrangements that create credit **risk**. When a creditor, such as a local community bank, extends a loan to a borrower to buy a home, the possibility that the borrower will not repay the outstanding principal or interest obligation creates a credit **risk**.³⁹ Credit **risks** are an immutable characteristic of lending arrangements and arise in contracts involving a diverse spectrum of borrowers.⁴⁰

Liquidity **risks** involve the potential that the debt obligations of an enterprise may exceed the assets of the business.⁴¹ Consider, for example, the activities of a conventional depository bank that maintains savings account deposits and issues home loans. The bank may face a liquidity crisis if all savings account holders run to the bank demanding return of their deposits at a time when the bank has issued their deposits to borrowers seeking home loans. The residential mortgages may have terms of ten, twenty, or thirty *558 years. In this situation, the bank could not return savers' deposits until borrowers repay residential mortgages. The business model of conventional depository banks creates an

asset-liability mismatch.⁴² If customers make a run on the bank and the bank must dispose of assets at fire sale prices, the bank may suffer substantial financial losses.⁴³

Another common type of financial **risk**-interest rate **risk**-is intimately related to liquidity **risk**.⁴⁴ Interest rates reflect the price at which banks agree to lend to borrowers, including other financial institutions.⁴⁵ Interest rates enable lenders to limit exposure when matching short-term assets and long-term liabilities.⁴⁶ Interest rates and asset trading prices comprise a broader category of **risks**-market **risks**. This category of **risk** arises from sudden changes in the prices of frequently traded assets or pricing benchmarks.⁴⁷ Firms engaged in the purchase and sale of securities, commodities, raw materials, and various manufacturing industries all navigate the challenges of market **risk**.⁴⁸ The active equity and debt securities or commodities *559 trading desks of financial institutions expose these businesses to significant market **risk**.⁴⁹

B. WHY ARE SYSTEMIC **RISKS** SPECIAL?

Recent turmoil in financial markets⁵⁰ casts a spotlight on the perils of **riskmanagement** failures in financial markets. Commentators, regulators, and financial market participants express concerns that a single shock or series of shocks may trigger a daisy chain of losses and lead to the insolvency of one or more systemically important financial institutions.⁵¹ Scholars and commentators describe the **risk** of a series of financial institution failures as systemic **risk**. Yet, systemic **risk** is not a term of art with a simple, precise, user-friendly definition. Interpretations differ regarding the types of threats that constitute systemic **risk**. Notwithstanding popular use of the term, the existing literature *560 leaves important questions regarding the specific details of systemic **risk** unresolved.

1. Understanding Systemic **Risks**. Interpreted literally, systemic **risk** refers to concerns that threaten the stability of an organizational system. In the context of financial markets, the “system” refers to the financial institutions, payment systems, and trading platforms and exchanges that comprise the foundation of the domestic and global economy. Clarifying the meaning of the “**risks**” that threaten financial market stability is, however, more complicated.

While there is no consensus on a definition of “systemic **risk**” and scholars and regulators' accounts of the events that engender systemic **risks** differ, descriptions of systemic **risk** possess some common elements. It is widely agreed that systemic **risk** refers to “a trigger event, such as an economic shock or institutional failure, [that] causes a chain of bad economic consequences-sometimes referred to as a domino effect.”⁵²

Yet, it is unclear how substantial volatility must be to register as systemically significant. Is the metric for volatility tied to whether fluctuating prices have significant adverse effects on the real economy? Or should the focus be on whether volatility may lead to a disruption and not a crisis? E. Gerald Corrigan, a former Federal Reserve President, proposes that focusing on the impact of **risks**-whether **risks** lead to a mere disruption and not a prolonged period of slow growth-helps us evaluate when **risks** ought to be classified as systemic.⁵³

This Essay adopts the perspective that one must evaluate the probability that a **risk** will materialize and the magnitude of the impact of **risk** that transforms the threat into a systemic **risk**. *561 This approach captures the elements of systemic **risk** that scholars commonly accept and goes further to encompass Frederic Mishkin's proposition that systemic **risk** is “the likelihood of a sudden, usually unexpected, event that disrupts information in financial markets, making them unable to channel funds to those parties with the most productive investment opportunities.”⁵⁴ As the Federal Reserve

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

has explained, systemic **risks** arise when important financial institutions, such as payment systems, experience disruptions that trigger a domino effect of consequences. According to the Federal Reserve,

[S]ystemic **risk** may occur if an institution participating on a private large-dollar payments network were unable or unwilling to settle its net debit position. If such a settlement failure occurred, the institution's creditors on that network might also be unable to settle their commitments. Serious repercussions could, as a result, spread to other participants in the private network, to other depository institutions not participating in the network, and to the nonfinancial economy generally. A Reserve Bank could be exposed to indirect **risk** if Federal Reserve policies did not address this systemic **risk**.⁵⁵

Exploring the methods of mitigating and **managing** systemic **risks** further clarifies the contours of systemic **risks**.

2. A Brief Survey of **RiskManagement** Approaches. **Riskmanagement** is a central pillar in financial market stability and a ***562** key element in financial market regulation.⁵⁶ Scholars describe efforts to identify, assess, or mitigate outcomes that could lead to losses as **riskmanagement** strategies.⁵⁷ Successful **riskmanagement** strategies may engender a multitude of benefits and are as diverse as the businesses and industries that adopt them. To **managerisks**, business may rely on a wealth of endogenous tools, such as enterprise **riskmanagement** (ERM) strategies⁵⁸ or corporate governance structures, and exogenous solutions, such as minimum capital ratios or living wills.⁵⁹ **Riskmanagement** thus “involves organizational processes that generally include **risk** identifying, measuring, and mitigating procedures.”⁶⁰ **Riskmanagement** is, “at its most fundamental level . . . about identifying bad outcomes that could occur in an uncertain future and taking deliberate action to shift the odds in a firm's favor.”⁶¹

Modern **riskmanagement** theory began at the turn of the twentieth century when Louis Bachelier pioneered a model of ***563** Brownian motion to analyze fluctuations in the prices of financial assets.⁶² In 1939, the American Finance Association met for the first time, and in 1942, they published their first journal, American Finance.⁶³ The decades that followed ushered in a period of innovation in **riskmanagement**.⁶⁴ Mathematicians and physicists embraced their celebrated role among financial institutions and developed asset pricing models such as the Black-Scholes options pricing formula and the Noble prize-winning Capital Asset Pricing Model.⁶⁵ Both models enjoyed tremendous popularity.

Beginning in the early 1970s with the collapse of the Bretton Woods system, financial product engineers began to design newly styled currency derivatives products.⁶⁶ Financial product engineers posited that these derivatives, currency futures, and options and interest rate swaps would reduce **risk** exposure and facilitate hedging.⁶⁷

During the 1980s and 1990s, market participants engineered and encouraged the development of hedging products including default and credit **riskmanagement** tools.⁶⁸ In the late 1980s, the Basel Committee on Banking Supervision initiated a series of discussions among the central banking authorities of the nations with the largest economies in the world; the discussions led several countries to implement the 1988 Basel Accord—a body of regulations designed to **managerisks** in the banking industry.⁶⁹ ***564** Depository banks subject to federal capital adequacy standards⁷⁰ adopted these **risk**-mitigating strategies because they reduced the appearance of the banks' **risk** exposure, enabling them to engage in a broader array of commercial activities.⁷¹

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

The 1980s and 1990s also saw American investment banks introduce formal **riskmanagement** departments.⁷² Two of the most widely celebrated internal **riskmanagement** models to emerge from this movement in the mid-1990s were RiskMetrics (a market **riskmanagement** tool) and CreditMetrics⁷³ (a credit **riskmanagement** tool).

Many financial institutions currently rely on value-at-**risk** (VAR) methodologies. VAR enables portfolio **managers** to avoid exceeding **risk** tolerance guidelines by estimating the worst expected loss over a given time period at a given confidence level under presumed market conditions.⁷⁴ VAR enables portfolio **managers** to assess the **risks** of loss associated with undertaking a certain **risk**.⁷⁵

Finally, stress testing offers another regularly cited **riskmanagement** strategy.⁷⁶ Financial institutions use stress tests to determine their capacity to **manage** certain types of **risks** or shocks.⁷⁷ A stress test enables financial market participants to evaluate how best to respond to “severe, yet plausible, stressed *565 market conditions such as low economic output, high unemployment, stock market crashes, liquidity shortages, high default rates, and failures of large counterparties.”⁷⁸ Employing stress tests reveals triggers and weak links that may cause extraordinary losses.⁷⁹

U.S. and foreign regulators increasingly emphasize the value of stress testing.⁸⁰ Regulators believe that stress tests will (1) facilitate efforts to promote **risk** oversight; (2) encourage quantitative skepticism within bank **riskmanagement** departments; and (3) align corporate governance practices among **management** in industries where externalities endanger significant populations such as, the nuclear power industry or the air traffic control industry.⁸¹

C. SYSTEMIC **RISK** MITIGATION

Examination of the commonly identified **risks** in financial markets and a comparison of these types of **risk** with systemic **risks** illustrate the rationale for treating systemic **risks** as unique and carefully regulating these concerns. Credit and capital markets serve as a critical infrastructure resource in international financial markets.⁸² Assets flow across territorial boundaries with *566 ease as market participants simultaneously transact with counterparties in any number of countries around the world.⁸³ An international network of exchanges and clearinghouses enable financial market participants to execute many of the world's most significant transactions, transferring cash, securities, commodities, and other assets across national borders in seconds.⁸⁴ Technological innovations in international banking, payment, and settlement systems increasingly facilitate cross-border transactions.⁸⁵ Advancing technology will increasingly ensure that financial market transactions are uninhibited by conventional boundaries.

The development of infrastructural resources, such as international banks, bank holding companies, securities and commodities exchanges, and clearinghouses facilitates the execution of cross-border transactions.⁸⁶ These institutions also provide critical benefits, enhance market efficiency, permit more accurate price discovery, and promote greater portfolio diversification.⁸⁷ The engineering of these critical market actors *567 and payment, trade, and settlement businesses, however, has also engendered endemic problems.

Regulatory efforts in the wake of the recent financial crisis reveal a fundamental concern growing in tandem with the burgeoning and deeply interconnected relationships among international financial market participants and financial institutions. No single international financial market regulator exercises the authority to address the lack of effective

regulation in international financial markets. While funds and assets flow across national borders with ease, jurisdictional limitations circumscribe the scope of national regulators' authority.⁸⁸

Conventional wisdom suggests that nations may regulate activities within their borders. But when transactions in one nation create market consequences in another nation, regulators, in limited cases, will impose restraints on the foreign actors engaging in the activity that affects their domestic markets.⁸⁹ Generally, however, each nation regulates the market participants domiciled, and the transactions executed, within its territorial boundaries.⁹⁰

From this background, one should note that a dearth of information regarding domestic or foreign market participants in any market or the failure of regulators to collect and share information in a timely manner stymies efforts to quell systemic *568 risks. Second, a revolution in riskmanagement practice and technology has characterized the most recent era in financial market innovation. Effective regulation of financial market participants or financial market intermediaries requires careful consideration of appropriate riskmanagement technology. Riskmanagement technology should occupy a central role in the development of any international regulatory approach.

When financial institutions (whether conventional depository banking institutions, investment banks, or some type of lending syndicate) act as creditors, each carefully screens borrowers to ascertain their creditworthiness.⁹¹ Portfolio diversification, or the strategic allocation of credit risks across the spectrum of borrowers, offers another risk mitigation strategy.⁹² Finally, lenders require the payment of interest in connection with most lending arrangements; higher interest rates offset increased credit risk.⁹³

These few examples of risks and risk mitigation strategies illustrate the challenges that financial institutions face in their efforts to execute business strategies. The list is not static. Financial institutions must continuously adapt to address emerging risks.

Efforts to regulate systemic risk pose indisputably unique 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.

III. EMERGING SYSTEMIC RISK CONCERNS: CYBERSECURITY THREATS

While a well-identified body of risks, including credit, market, interest rate, and liquidity risk, has long been the subject of riskmanagement experts, a new class of risk promises to test our most *569 valuable riskmanagement strategies. This Part examines the burgeoning universe of risks growing from our dependence on cyberspace. These underexplored cyber risks are indisputably the next frontier of riskmanagement concerns.

A. DEFINING CYBERSECURITY THREATS

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 effort to access confidential or sensitive data.⁹⁴ A cybercrime is “any crime that is facilitated or committed using a computer, network, or hardware device,”⁹⁵ meaning cybercrimes are cyber-incidents involving acts prohibited by law. The cyber-activities that most trouble financial market riskmanagement experts are neither cyber-incidents nor cybercrimes. These categories of cyber-activities are over- and under-inclusive to describe the cyberthreats that plague financial markets.

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

Examining descriptions of cyberattacks provides a more useful point of departure. Identifying the activities that constitute cyberattacks, however, is more difficult and markedly more controversial.

Government and activist coalitions use the term cyberattack to describe undesirable cyber intrusions. The United States military, more specifically the Joint Chiefs of Staff, describes a cyberattack as:

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. *570 The intended effects of cyberattack 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 cyberattack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyberattack may be widely separated temporally and geographically from the delivery.⁹⁶

This approach limits references to cyberattacks to acts intended to harm cyber systems.

Some commentators base their characterization of cyber intrusions on the motivations of the actors who engage in a cyberattack. Authors of *The Law of Cyber-Attack* adopt a narrow definition, explaining that a cyberattack consists of “any action taken to undermine the functions of a computer network for a political or national security purpose.”⁹⁷ This approach encompasses hacking, bombing, cutting, and infecting, and states that “to be a cyber-attack [an action] must aim to undermine or disrupt the function of a computer network,” thereby defining cyberattack “according to its objective.”⁹⁸ The devices employed to undermine or compromise a computer network may include worms, viruses, or Trojan horses.⁹⁹ This definition is narrowly focused on the threats posed by cyber-technologies, which are motivated by political or national security rationales.¹⁰⁰

Five common depictions of cyberattacks clarify the methods and rationale for these intrusions.¹⁰¹ “Lone wolf” attacks are often *571 executed by “gifted teenagers” who want to compromise international networks for the rush of successfully intruding in a proprietary space (fun) or for bragging rights (fame).¹⁰² “Lone wolf” attacks are some of the most “difficult cyberattacks to detect and combat.”¹⁰³ Second are “hacktivists” attacks, which are conducted by individuals who are motivated to attack for political or moral reasons (furthering a cause).¹⁰⁴

A third type of cyberattack involves “fraud and criminal activity,” usually executed by someone who wishes to gain access to customer information for their own advantage (fraud).¹⁰⁵ These hackers tend to target banks and retailers due to the large amount of customer information they possess.¹⁰⁶ A fourth type of cyberattack, known as “industrial espionage,” usually involves a lone wolf targeting financial assets (funneling funds).¹⁰⁷ These attacks are often highly complex.¹⁰⁸ “Cyber warfare,” a fifth type of cyberattack, describes a cyberattack against a nation state (furthering a military or political campaign).¹⁰⁹ These are the least common of all cyberattacks, but could be the most destructive, even for the most developed countries.¹¹⁰

These definitional distinctions reflect different understandings of the elements of cyberattacks and the problems that these intrusions create.

B. CYBER RISKS AND FINANCIAL INSTITUTIONS

Who might initiate a cyberattack on a large, systemically important financial institution? Hackers (including activists who want to reveal weaknesses in **cybersecurityriskmanagement** practices or disrupt a firm's operations), foreigners engaged in ***572** corporate or traditional espionage, and terrorists¹¹¹ wreak havoc by penetrating firm firewalls, accessing confidential information, manipulating accounts,¹¹² and disrupting key platforms in the international financial monetary system.¹¹³ Historically, **cybersecurity** policies have aimed to protect “investor and firm information from compromise,” meaning loss of data confidentiality, integrity, or availability.¹¹⁴ While data protection continues to be an important area of cyber **risk** concern, cyberattacks that threaten the networks that link financial institutions, exchange and clearinghouse platforms, and payment systems comprise the new **cybersecurity** frontier.

Investment banks, broker-dealers, and securities and commodities exchange platforms strategically endeavor to anticipate and defend against cyberattacks. The Financial Industry Regulatory Authority (FINRA) reports that the “frequency and sophistication of these attacks is increasing and individual broker-dealers, and the industry as a whole, must make responding to these threats a high priority.”¹¹⁵

The **cybersecurity** concerns that financial institutions face threaten the stability of financial markets, the loss of billions of ***573** 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. As the New York State Department of Financial Services noted, “[c]yber hacking is a potentially existential threat to our financial markets”¹¹⁶ Regulators note that **cybersecurity** threats may “wreak serious havoc on the financial lives of consumers.”¹¹⁷

Financial and banking institutions are thus concerned about both internal and external cyber security threats, and both internal and external infiltration testing is needed to determine how secure a firm is against these potential threats.¹¹⁸ These institutions naturally vary in how they rank various threats due to the nature of the firm and their business model.¹¹⁹ “For example, online brokerage firms and retail brokerages are more likely to rank the **risk** of hackers as their top priority **risk**” whereas “[f]irms that engage in algorithmic trading were more likely to rank insider **risks** more highly.”¹²⁰ Similarly, large brokerage firms were more likely to rank “**risks** from nation states or hacktivist groups” higher than other firms.¹²¹

Technology plays a significant role in financial firms' ability to execute transactions, intensifying financial institutions' vulnerability to cyberattacks.¹²² Firms relying on the Internet to **manage** communications with clients; employees and clients' accessing information on firm websites using mobile devices; and firms' employees, clients, and regulators distributing information ***574** through e-mail communications, offer various opportunities for cyberattacks.¹²³

Regulators characterize the highest priority **cybersecurityrisks** as endogenous threats (concerns that insiders may compromise firm or client data),¹²⁴ exogenous threats (concerns that hackers will attack confidential firm data),¹²⁵ and operational **risks**.¹²⁶ Endogenous **risks** include employees' or other users' unauthorized access to firm systems and databases and their harvesting of sensitive or confidential data.¹²⁷ Exogenous **risks** include the threats posed by interfacing with vendors or other third-party systems.¹²⁸ While the three legs of this **riskmanagement** triangle are equally significant, the first two categories of **risk**- endogenous and exogenous **risks**-are the most pervasive.¹²⁹

These systemically important firms must understand the kinds of threats they face, what is most likely to be targeted for attack, who is likely to attack, what their vulnerabilities are, and how to best prepare for and protect against these threats. FINRA states that metrics are a “critical cyber security **management** tool,” and is concerned that some firms only use metrics minimally, thereby limiting their knowledge of how effective their cyber security procedures are.¹³⁰ In its survey of firm practices, FINRA noted that “over 80 percent of firms had established **cybersecurityrisk** assessment programs . . . a number of which draw on the COBIT 5 and ISO/IEC 27001 frameworks,” and others modeled their **risk** *575 domains on the Federal Financial Institutions Examination Council (FFIEC) handbook.¹³¹ However, FINRA is concerned that the remaining firms were either just starting to establish a **cybersecurityrisk** assessment program or had no program in place.¹³²

Firms have expressed additional concerns about information sharing, which must comply with regulatory requirements, including antitrust regulation.¹³³ The Federal Trade Commission and the Department of Justice, however, issued a policy statement explaining that sharing “cyber threat information is not likely to raise antitrust concerns and can help secure the nation's networks of information and resources.”¹³⁴ FINRA noted that firms use **cybersecurity** threat information and intelligence in many ways, including collecting and analyzing data related to threats and vulnerabilities that the firms can then “incorporate in their technical infrastructure, e.g., by adjusting firewall settings to block certain IP addresses, installing patches to fix vulnerabilities in software, or updating anti-virus and anti-malware software to capture newly identified instances of viruses or malware.”¹³⁵

According to FINRA, “[a] **riskmanagement**-based approach to **cybersecurity** permits firms to tailor their approach to the individual circumstances and the changing threats each firm faces” and can “inform firms' thinking at a programmatic as well as individual control level.”¹³⁶ While financial and banking institutions must be vigilant regarding **cybersecurity**, they can take some comfort in the fact that “most successful attacks take advantage of fairly basic control weaknesses.”¹³⁷ If the right policies are implemented and updated periodically, cyber criminals will have a much harder time accessing firms' confidential *576 information. Proper internal control policies, common wisdom argues, will disarm attackers seeking to access firms' confidential information. **Risk** assessments and information sharing can help these entities identify and prioritize the potential cyberattacks they could face and the steps they need to take to try to prevent these attacks,¹³⁸ as well as measures for mitigation and containment for when a breach occurs.¹³⁹

IV. REGULATING CYBERSPACE

Charting a course for appropriately addressing cyber **risks** requires exploring a number of solutions. Examining these solutions reveals critical opportunities to mitigate endogenous cyber **risks**. This Part reveals that reliance on conventional solutions is a passive defense to cyberattacks. This Part demonstrates the necessity of dynamic strategies and collaboration among businesses and government.

Cyberspace is governed by a patchwork of state, federal, and international regulations. Our fragmented regulatory framework, characterized by industry-specific legislation, leaves significant gaps in the oversight of cyberspace. No uniform international law currently exists to govern cyberspace and to specifically regulate cyberattacks, though entities including the United Nations, NATO, the Council of Europe, and the Shanghai Cooperation Organization have made some efforts to regulate cyberattacks.¹⁴⁰

***577 A. TOWARD TRANSPARENCY AND INFORMATION SHARING**

Congress has recently enacted or amended several significant **cybersecurity** regulations, including the Computer Fraud and Abuse Act,¹⁴¹ the E-Government Act of 2002,¹⁴² the **Cybersecurity** Research and Development Act of 2002,¹⁴³ the Federal Information Security **Management** Act of 2002,¹⁴⁴ the Cyber Security Enhancement Act of 2002,¹⁴⁵ the **Cybersecurity** Enhancement Act of 2014,¹⁴⁶ and the National **Cybersecurity** Protection Act of 2014.¹⁴⁷ These legislative steps are laudable for their efforts to introduce criminal laws that address fraud involving devices, computers, or e-mail; malicious interference with communications lines, stations, or systems; electronic communication interception; illicit access to electronic communications and records; and recording of dialing, routing, addressing, and signaling information. Currently, no single piece of federal legislation exists that addresses **cybersecurity** threats and issues.¹⁴⁸ The fragmented approach to addressing cyber **risks** creates opportunities for regulatory arbitrage. Moreover, none of these efforts effectively addresses mounting concerns that cyber **risks** ***578** may disrupt interconnected systems such as securities and commodities trading systems, banking systems, or payment systems. Leaving these systems vulnerable creates systemic **risk** concerns.

The most recently minted statute in the litany of cyber regulations—the **Cybersecurity** Information Sharing Act of 2015 (CISA)¹⁴⁹—demonstrates significant promise to address systemic cyber threats. Adopted on December 18, 2015, the CISA “[p]romotes and encourages the private sector and the United States government to rapidly and responsibly exchange cyber threat information.”¹⁵⁰ Notwithstanding the promise of the CISA, concerns regarding the absence of privacy protections raise important questions regarding the implementation of the Act.

1. The **Cybersecurity** Information Sharing Act of 2015. The CISA aims to protect “information systems or information that is stored on, processed by, or transiting an information system The statute expressly declares its intent to protect information systems and information warehoused in these systems from **cybersecurity** threat attacks.”¹⁵¹ To this end, the statute creates a voluntary **cybersecurity** information sharing exchange designed to encourage public and private sector actors to share cyber threat information.¹⁵²

The CISA invites private entities to gather and share relevant **cybersecurity** threat information with federal agencies or private entities without concerns that such acts violate antitrust regulations or create liability.¹⁵³ **Cybersecurity** threats are defined in the statute as actions “that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.”¹⁵⁴ Title I—“**Cybersecurity** Information Sharing”—permits private entities to ***579** monitor their networks and engage in defensive measures¹⁵⁵ to protect their own information systems and networks from **cybersecurity** attacks.¹⁵⁶ Upon identifying **cybersecurity** threats, private entities may share information regarding cyber threat indicators, which include:

- (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a **cybersecurity** threat or security vulnerability;
- (B) a method of defeating a security control or exploitation of a security vulnerability;
- (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- (E) malicious cyber command and control;
- (F) the actual or potential

harm caused by an incident, including a description of the information exfiltrated as a result of a particular **cybersecurity** threat; (G) any other attribute of a **cybersecurity** threat, if disclosure of such attribute is not otherwise prohibited by law; or (H) any combination thereof.¹⁵⁷

The CISA includes a number of privacy protections. For example, upon identifying a cyber threat indicator or a defensive measure, private entities must remove any “personal information of a specific individual or information that identifies a specific individual” from the data before sharing that information.¹⁵⁸ In ***580** addition to implementing screening and redacting policies, participants can only use the information obtained through this information sharing process for the limited purposes identified in the statute, which include: identifying cyber threats or their sources; identifying potential security vulnerabilities; and responding to, preventing, or mitigating specific threats such as serious bodily harm, or a serious economic harm, including a terrorist act or a use of a weapon of mass destruction.¹⁵⁹

Titles II, III, and IV of the CISA create a number of new **cybersecurity**-related requirements, including a reporting requirement for government agencies, in order to promote internal defenses against cyberattacks and improve federal network security;¹⁶⁰ inviting federal efforts to coordinate with industry and other stakeholders to develop capabilities that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber threat indicators and defensive measures;¹⁶¹ promoting the development of best practices for **cybersecurity**;¹⁶² requiring a government study on mobile device security;¹⁶³ and allowing apprehension and prosecution of international cyber criminals, even if they do not have any assets within the United States' jurisdiction.¹⁶⁴

2. Weaknesses of the CISA. Critics of the **Cybersecurity** Information Sharing Act contend that the statute grants broad powers of surveillance and fails to incorporate appropriate privacy protections. Market participants express concern regarding the government's ability to safeguard proprietary and confidential ***581** information.¹⁶⁵ Government warehousing of shared data is only as safe as the government's capacity to prevent cyber intrusions. After recent cyberattacks breaching government agency defenses, many express concerns that shared information may be more vulnerable in the hands of government agencies.

Privacy advocates' concerns regarding secondary transfer of data may be one of the most hotly debated issues. Once information is shared with one agency of the federal government, the agency may transfer the shared information to the National Security Agency or the Federal Bureau of Investigation.¹⁶⁶ With great alarm, critics of the bill proclaim that the bill allows extensive monitoring of web-based activities, empowers government officials and agencies to occupy a central role in gathering confidential and proprietary information, and creates too few limitations on law enforcement's subsequent use of the information.¹⁶⁷

These critics argue that the expansive definitions of “cyber threat indicator” and “**cybersecurity** threat” and the surveillance and liability protections afforded in the CISA give the government and private companies too much latitude in what types of information they gather and how they gather it.¹⁶⁸ Others say the law is redundant of other information-sharing practices like ***582** Information Sharing and Analysis Centers (ISACs) and the Department of Homeland Security's Enhanced **Cybersecurity** Services.¹⁶⁹ These critics argue that Congress and the Obama administration have not addressed if or why these other information-sharing practices are deficient.¹⁷⁰ A few have even compared the CISA to the USA Patriot Act, stating that both laws are expensive that reflect legislative approaches with ideas that had previously been rejected by Congress and then quickly passed in a subsequent session before many would have had a chance to read through the entire bill.¹⁷¹ Important technology firms, including Google, Facebook, and Yahoo

oppose various elements of the legislation and have expressed their intent not to participate in the information sharing program.¹⁷²

Still others argue that the statute expands the power of the federal government in undesirable ways. For example, under Title I of the CISA, the Director of National Intelligence will lead the charge in developing “procedures to facilitate and promote . . . timely sharing of classified cyber threat indicators and defensive measures . . . and information relating to **cybersecurity** *583 threats”¹⁷³ with relevant federal entities,¹⁷⁴ non-federal entities,¹⁷⁵ or the public if appropriate.¹⁷⁶ As critics have indicated, existing legislation grants the President broad powers in times of national emergency, which include the threat of a major **cybersecurity** incident.¹⁷⁷

After the September 11th terrorist attacks, public concerns over executive power escalated with regard to the President's authority to conduct surveillance within the United States,¹⁷⁸ including President Bush's controversial authorization enabling the NSA “to intercept international electronic communications between persons in the United States”¹⁷⁹ The continuing expansion of executive and federal authority should be subject, these critics argue, to appropriate limitations.

Finally, the defensive measures authorization provision in the CISA does not address measures that adversely impact third-party networks or data. Consistent with the congressional establishment of a voluntary sharing framework, the legislation disclaims any intention of creating a duty to share cyber threat indicators or defensive measures or a duty to warn or act based on the receipt of such indicators or measures.¹⁸⁰ Congressional critics have already introduced a bill to repeal the CISA.¹⁸¹

B. ALTERNATIVE INITIATIVES

While the CISA may mitigate certain cyber threats, voluntary information sharing alone will not overcome the possibility of *584 systemic cyber **risks**. Fortunately, regulatory efforts by FINRA, the Securities Exchange Commission, and the National Institute of Science and Technology (NIST) supplement the CISA's efforts and introduce important best practices and mandatory **cybersecurity** guidelines. Twice in recent years, FINRA surveyed over two hundred financial firms to gain insight into the contours of financial market participants' **cybersecurity** practices.¹⁸² The surveys revealed three critical cyber security threats for financial firms, including: hackers penetrating firm systems; insiders compromising firm or client data; and operational **risks** materializing.¹⁸³ To counter these concerns, FINRA outlined a body of best practices.

Some of the FINRA's proposed best practices are trite and non-controversial. For example, to combat **cybersecurity** attacks created when an insider such as an employee downloads malware,¹⁸⁴ FINRA proposes that effective employee training on **cybersecurity** issues is vital to a firm's **cybersecurity** program.¹⁸⁵ Other best practices techniques introduce more aggressive efforts and acknowledge that third-party relationships create significant **risk** for cyberattacks. The FINRA guidelines propose (1) development of a defense-in-depth strategy by layering several independent security controls throughout their IT system; (2) limiting users' and employees' access to the firm's data and systems; (3) encrypting data to protect data confidentiality and information integrity; (4) having third-parties attempt to penetrate the firm's system to test any potential **cybersecurity** weaknesses; and (5) increasing surveillance of third-party vendors whose security standards might not meet those of the firm.¹⁸⁶

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

While these practices may be helpful in overcoming weaknesses in cyber security **risk** mitigation, FINRA's guidelines are completely voluntary and simply amount to helpful suggestions for ***585** firms to develop or improve their **cybersecurity** procedures.¹⁸⁷ While it may be true that “there is no one-size-fits-all solution to address cyber threats,”¹⁸⁸ FINRA acknowledges that “[a] sound governance framework with strong leadership is essential” to **managing** and mitigating cyberattacks.¹⁸⁹ In other words, internal governance structures cannot wait for industry-led or government-proposed initiatives. Board members and senior-level **managers** must seek out and implement **cybersecurityrisk** mitigation measures.

Taking an approach consistent with the Commission's reliance on disclosure-based regulation,¹⁹⁰ the SEC's Division of Corporation Finance recently published guidance providing that companies registering securities for sale to the public and those subject to periodic reporting requirements should indicate potential cyber **risks** they face, any cyber incidents that have transpired, and whether they outsource material cyber-functions and any relevant insurance coverage.¹⁹¹ The SEC posits that disclosure of **cybersecurityrisks** “must adequately describe the nature of the material **risks** and specify how each **risk** affects the registrant.”¹⁹² Registrants should tailor their disclosure to their particular circumstances, detailed enough that investors know the nature of the cyber **risks** that the company faces.¹⁹³

Registered company **managers** should also discuss and analyze **cybersecurityrisks** and incidents that are part of an event or trend that is “reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.”¹⁹⁴ ***586** Registrants should discuss possible outcomes and expected costs of potential cyber threats.¹⁹⁵ If a cyber incident occurs, registrants must provide disclosure of losses that are reasonably possible and should aim to mitigate losses.¹⁹⁶ Additionally, registrants are required to disclose their assessments of the effectiveness of their disclosures, controls and internal oversight procedures.¹⁹⁷

The SEC's reliance on transparency fails to offer a valuable tool for **risk** mitigation.¹⁹⁸ Disclosure is an ex post declaration of events that have already transpired and offers limited guidance for firms seeking to prevent losses.¹⁹⁹ Creating disclosure obligations may serve to alert the investing public to cyber **risks**.²⁰⁰ This approach also creates, however, challenges for registered companies seeking to raise capital from the investing public. Registered companies must determine when a cyber threat is sufficiently material to require disclosure.²⁰¹ Certainly, the disclosure of every cyber **risk** is not useful to investors and simply serves to inundate markets with information.²⁰² Determining the magnitude of the impact of evolving cyber threats, however, will prove challenging for firms. Evaluating disclosure regarding firms' preparedness for cyberattacks will initially pose an industry-wide conundrum: ***587** Disclosing too little information creates liability **risks** but disclosing too much damages capital raising efforts.²⁰³

Finally, a public-private initiative may represent the most valuable path toward cyber **risk** mitigation.²⁰⁴ In February 2013, President Barack Obama signed an Executive Order authorizing NIST to develop a Framework for Improving Critical Infrastructure **Cybersecurity** to address cyber **risks**.²⁰⁵ Similar to FINRA's best practices, the NIST framework is not mandatory, though, many have enthusiastically embraced the guidelines as the appropriate standard for financial markets. The framework is designed specifically to protect critical infrastructure, or resources that provide vital national, physical, or virtual systems and assets whose destruction “would have a debilitating impact on **cybersecurity**, national economic security, national public health or safety, or any combination of those matters.”²⁰⁶ The framework consists of three parts—the Framework Core, the Framework ***588** Profile, and the Framework Implementation Tiers—and “focuses

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

on using business drivers to guide **cybersecurity** activities and considering **cybersecurityrisks** as part of the organization's **riskmanagement** processes.”²⁰⁷ Similar to FINRA's guidelines,²⁰⁸ this framework is not a one-size-fits-all approach for **managing** cyber threats.²⁰⁹ Firms will vary in implementing the framework depending on their unique threats and vulnerabilities.²¹⁰

The Framework Core provides industry standards, guidelines, and practices for **cybersecurity** activities and desired outcomes for all levels within a company by using five key functions: identify, protect, detect, respond, and recover.²¹¹ Identify refers to developing a procedure to identify and **manage** cyber threats.²¹² Protect refers to ensuring delivery of critical infrastructure services.²¹³ Detect refers to promptly identifying that a **cybersecurity** incident has occurred.²¹⁴ Respond refers to taking action after detecting a **cybersecurity** incident.²¹⁵ Recover refers to resilience and restoring capabilities or services that were harmed because of a **cybersecurity** incident.²¹⁶

The NIST framework Profile applies the Framework Core to a particular scenario in order to reach outcomes based on business needs that a company has selected from the framework categories and subcategories.²¹⁷ Companies should have a Current Profile (showing the **cybersecurity** outcomes the company is currently achieving) and a Target Profile (showing the desired **cybersecurityriskmanagement** goals and outcomes).²¹⁸ Comparing these two profiles can help identify gaps in a company's **cybersecurityriskmanagement** procedures and thus help the company to close those *589 gaps.²¹⁹ The NIST Framework Implementation Tiers describe how a company views **cybersecurityrisks** and what measures the company has implemented to **manage** and combat those **risks**.²²⁰ There are four tiers within this section of the framework: (1) Partial; (2) **Risk** Informed; (3) Repeatable; and (4) Adaptive.²²¹ Companies are encouraged to progress to higher tiers “when such a change would reduce **cybersecurityrisk** and be cost effective.”²²²

These three parts work together to facilitate **riskmanagement** and information sharing. The framework describes **riskmanagement** as “the ongoing process of identifying, assessing, and responding to **risk**,”²²³ specifically **cybersecurityrisks**.²²⁴ The framework should start and end at the executive level. Executives should communicate the priorities, available resources, and the overall **risk** tolerance of the entire business. At the most senior business level, decisions should reflect a general **riskmanagement** process and collaboration across operations to communicate business needs and create a Profile. The operations division of the business must then perform an impact assessment based on the information received. This information should be reported up to the executive level. Finally, the executive level must discuss what changes to make regarding **riskmanagement** and how to make those changes based on that outcome.²²⁵

Companies can implement the NIST framework by following seven easy-to-follow steps to establish or improve their **cybersecurity** programs.²²⁶ Step one-“Prioritize and Scope”-requires identifying business objectives and priorities to make strategic decisions about implementing or improving a **cybersecurity** program.²²⁷ Step two-“Orient”-invites businesses to identify systems, assets, regulatory requirements and an overall *590 approach to **risk** based on the scope of the **cybersecurity** program determined in step one.²²⁸ Step three-“Create a Current Profile”-means showing which Category and Subcategory outcomes from the Framework Core are already being achieved.²²⁹ Step four-“Conduct a **Risk** Assessment”-means determining the likelihood of a **cybersecurity** incident occurring and the potential impact that incident could have on the company.²³⁰ Step five-“Create a Target Profile”-means focusing on the Framework Categories and Subcategories that fit the company's desired **cybersecurity** outcomes.²³¹ Step six-“Determine, Analyze, and Prioritize Gaps”-means comparing the Current and Target Profiles to determine any gaps and create a plan to

address those gaps.²³² Step seven-“Implement Action Plan”-means taking action in response to the gaps identified in Step six and monitoring current **cybersecurity** practices against the Target Profile.²³³

The NIST framework, however, does have some shortcomings. While it “offers worthwhile standards for improving **cybersecurity**, it does not fully address several critical areas.”²³⁴ For example, it does not address data privacy issues or standards; it does not address the need to implement measures to identify a company's unique threats, motivations, and capabilities; and it does not discuss a company's statutory, contractual, or regulatory **cybersecurity** requirements.²³⁵

*591 V. CONCLUSION

Cyberattacks are a central, pervasive, and endemic threat, which will grow exponentially in coming years.²³⁶ As President Obama observed, cyberattacks threaten to “sabotage our power grid, our financial institutions, and our air traffic control systems.”²³⁷ These information structures “serve as the backbone of our national economy.”²³⁸ Simply stated, we must acknowledge the critical natures of cyber **risks** and the threat such **risks** impose on “economic value creation, exchange, and transfer.”²³⁹

This Essay questions the existing emphasis on **riskmanagement** solutions that focus on information and agency failures. Over the last four decades, parallel to the development and increasing sophistication of regulation and financial market engineering, **riskmanagement** strategies have evolved. Traditional **riskmanagement** solutions have relied on independently developed, implemented, and enforced **riskmanagement** practices. This Essay dismisses the conventional approaches to **riskmanagement** in international financial markets. Rather than focusing on solutions applicable to individual **riskmanagement** issues, this Essay surveys solutions to identify strengths and limitations of existing regulatory options *592 and emphasizes developing a comprehensive understanding of cyber **risks** and cyber **riskmanagement**.

Footnotes

a1 Professor of Law, Director of the Regulation, Governance, and **RiskManagement** Program, Seton Hall University Law School; B.S., Edmund A. Walsh School of Foreign Service, Georgetown University; J.D., University of Michigan Law School. For his careful review of earlier drafts, I thank Carlos Lopez. I am indebted to Tom Lin and Scott Shackelford for their generous responses to my earliest musings on the subject of this Essay. For significant research assistance, I thank my research assistant Sarah Wilbur.

1 See Tom C.W. Lin, *Financial Weapons of War*, 100 *Minn. L. Rev.* 1377, 1381 (2016) (discussing financial infrastructure as a “new theater of war”); Matthew Goldstein, *Brokerage Firms Worry About Breaches by Hackers, Not Terrorists*, Dealbook, N.Y. Times (Feb. 3, 2015, 11:54 AM), http://dealbook.nytimes.com/2015/02/03/brokerage-firms-most-worried-about-hackers-and-rogue-employees-finra-report-says/?_r=0 (discussing the threat of hacking faced by financial firms); Sam Jones, *Cyber Security: Business Is in the Front Line*, Fin. Times (Apr. 29, 2014, 10:35 AM), <http://www.ft.com/intl/cms/s/0/11b41ac4-c3cb-11e3-a8e0-00144feabdc0.html#axzz3hFamiepE> (noting an increase of data breaches by 63% in 2013); see also David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of U.S. Workers*, N.Y. Times (June 4, 2015), <http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html> (reporting that a large breach of federal employees' data originated in China).

2 Data breaches occur when cybercriminals hack into businesses or corporations to steal confidential information such as credit and debit card numbers, e-mail addresses, and phone numbers. E.g., Rachael M. Peters, *So You've Been Notified, Now*

What? The Problem with Current Data-Breach Notification Laws, 56 Ariz. L. Rev. 1171, 1173 (2014) (discussing sizable data breaches at Target, Home Depot, and JPMorgan Chase).

3 See *infra* Part II.b.2.

4 Protecting Consumer Information: Can Data Breaches Be Prevented? Hearing Before the H. Subcomm. on Commerce, Mfg., and Trade, 113th Cong. 1-2 (2014) (statement of Lisa Madigan, Att'y Gen. of Illinois), <http://energycommerce.house.gov/hearing/protecting-consumer-information-can-data-breaches-be-prevented>.

5 See Ctr. for Strategic & Int'l Studies, Net Losses: Estimating the Global Cost of Cybercrime 3 (2014), <http://mcafee.com/US/resources/reports/np-economic-impact-cybercrime2.pdf> (“The cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen-incidents in the last year include more than 40 million people in the US, 54 million in Turkey, 20 million in Korea, 16 million in Germany, and more than 20 million in China. One estimate puts the total at more than 800 million individual records in 2013.”).

6 *Id.* at 2.

7 See Press Release, Office of the Press Sec'y, The White House, Excerpts of the President's State of the Union Address (Jan. 20, 2015), <http://www.whitehouse.gov/the-press-office/2015/01/20/excerpts-president-s-state-union-address> (providing President Obama's statement that “[n]o foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets or invade the privacy of American families, especially our kids” (internal quotations omitted)); Nicholas Watt et al., David Cameron Pledges Anti-Terror Law for Internet After Paris Attacks, *The Guardian* (Jan. 12, 2015, 5:04 PM), <http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg> (“The Prime Minister said a future Conservative government would aim to deny terrorists ‘safe space’ to communicate online”); Mark Rutte, Prime Minister of N.Z., Speech at the Hague Global Conference on Cyber Space (Apr. 16, 2015), <https://www.government.nl/topics/cybercrime/documents/speeches/2015/04/16/speech-by-prime-minister-mark-rutte-at-the-opening-of-the-gccs-2015> (“We need to invest in security so that legitimate [Internet] users will benefit and criminals will think twice.”).

8 See *infra* Part II.b.

9 Barack Obama, President of the U.S., Remarks by the President at the **Cybersecurity** and Consumer Protection Summit (Feb. 13, 2015), <https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit>.

10 *Id.*

11 See, e.g., Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 *Harv. J.L. & Tech.* 429, 445-46 (2012) (“Cyberattacks' indirect effects are generally larger than their direct effects because the attackers focus on causing disruption after the attacks”).

12 See, e.g., Matthew Goldstein & Nicole Perlroth, Authorities Closing in on Hackers Who Stole Data from JPMorgan Chase, *Dealbook*, N.Y. Times (Mar. 15, 2015), <http://www.nytimes.com/2015/03/16/business/dealbook/authorities-closing-in-on-hackers-who-stole-data-from-jpmorgan-chase.html> (“[H]ackers gain[ed] access to email addresses and phone numbers for 83 million households and small businesses”); Jones, *supra* note 1 (“[C]riminally-motivated cyber breaches are not just related to cyber theft, but can increasingly involve market manipulation. One international lawyer says he is aware of attacks that targeted his and other similar law firms to mine information on merger and acquisition activity in London and New York.”).

13 See, e.g., Fighting China's Hackers: Is It Time to Retaliate Against Cyber-Thieves?, *Economist* (May 25, 2013), <http://www.economist.com/news/united-states/21578405-it-time-retaliate-against-cyber-thieves-fighting-chinas-hackers> (“American officials . . . report that intellectual property (IP) is being stolen on an unprecedented scale, and that passive defenses no longer work.”).

- 14 See, e.g., David E. Sanger & Nicole Perloth, Bank Hackers Steal Millions via Malware, N.Y. Times (Feb. 14, 2015), <http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html> (describing how hackers forced an ATM to dispense cash); Ian Wylie, Danger in the Digital Age: The Internet of Vulnerable Things, Fin. Times (Apr. 26, 2015, 11:59 PM), <http://www.ft.com/cms/s/0/fc2570f0-cef4-11e4-b761-00144feab7de.html#axzz3r0dmZUId> (“Less well understood are the growing cyber threats to physical assets, as the online world merges with the real one.”).
- 15 See Rachel Abrams, Target Puts Data Breach Costs at \$148 Million, and Forecasts Profit Drop, N.Y. Times (Aug. 5, 2014), <http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html> (discussing how hackers stole Target customers' credit card and other personal information in a data breach).
- 16 Elizabeth A. Harris & Nicole Perloth, For Target, the Breach Numbers Grow, N.Y. Times (Jan. 10, 2014), <http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html>.
- 17 Harris & Perloth, *supra* note 16; see also Nicole Perloth, Target Stuck in the Cat-and-Mouse Game of Credit Theft, N.Y. Times (Dec. 19, 2013), <http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html> (“Target said that from Nov. 27 to Dec. 5 hackers stole customer names, credit or debit card numbers, expiration dates and three-digit security codes . . .”).
- 18 Shelly Banjo, Home Depot Hackers Exposed 53 Million Email Addresses, Wall St. J. (Nov. 6, 2014, 8:03 PM), <http://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282>; see also Maggie McGrath, Home Depot Confirms Data Breach, Investigating Transactions from April Onward, Forbes (Sept. 8, 2014, 5:32 PM), <http://www.forbes.com/sites/maggiemcgrath/2014/09/08/home-depot-confirms-data-breach-investigating-transactions-from-april-onward/> (discussing Home Depot's payment data systems breach).
- 19 See Banjo, *supra* note 18 (“The hackers evaded detection in part because they moved around Home Depot's systems during regular daytime business hours and designed the malware to collect data, take steps to transmit it to an outside system and erase its traces.”); Andrea Peterson, Secret Service Estimates Type of Malware that Led to Target Breach Is Affecting Over 1,000 U.S. Businesses, Wash. Post (Aug. 22, 2014), <https://www.washingtonpost.com/news/the-switch/wp/2014/08/22/secret-service-estimates-type-of-malware-that-led-to-target-breach-is-affecting-over-1000-u-s-businesses/> (“The malware remotely exploits businesses' administrator accounts and steals consumer's [sic] payment data, such as their credit and debit card numbers.”).
- 20 For a general discussion of the concept of **risk**, see *infra* Part II.a.
- 21 Fed. Reserve Sys., The 2013 Federal Reserve Payments Study: Recent and Long-Term Payment Trends in the United States: 2003-2012, at 41 tbl.3.3.1, 42 tbl.3.3.2 (2013), https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf.
- 22 See *infra* Part III.a.
- 23 See Doug Carroll, Banks Admit Growing Cyberattack **Risks**, USA Today (Aug. 28, 2014, 4:06 PM), <http://www.usatoday.com/story/money/business/2014/08/28/banks-growing-cyber-security-risks/14741653/> (highlighting financial firms' responses to cybercrime **risks**); Jones, *supra* note 1 (“As many of the world's largest companies are beginning to realise, the threat to their margins, their brands and even their continued existence from cyberattacks is no longer an abstract **risk** they can ignore.”); R. Andrew Patty II, Credit Card Issuers' Claims Arising From Large-Scale Data Breaches, 28 J. Tax'n Fin. Inst. 5, 5 (2015) (“[L]arge collections and streams of information in the possession or control of major retailers and other merchants associated with specific financial accounts held at card-issuing financial institutions have proven to be tempting targets for bad actors who are seeking pecuniary gain or striving to sabotage infrastructure for political or ideological reasons.”).
- 24 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/SB10001424052702304259304576374713184158>; 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>.

- 25 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).
- 26 Sanger & Perlroth, *supra* note 14 (“[T]he ‘Carbanak cybergang,’ named for the malware it deployed, represents an increase in the sophistication of cyberattacks on financial firms.”).
- 27 See *id.* (“[T]he scope of the attack . . . could make it one of the largest bank thefts ever.”).
- 28 *Id.*
- 29 *Id.*
- 30 *Id.*
- 31 *Id.*
- 32 Devlin Barrett et al., *Nasdaq Confirms Breach in Network*, *Wall St. J.* (Feb. 7, 2011, 12:01 AM), <http://www.wsj.com/articles/SB10000142405274870398950457612863256880>.
- 33 H.R. 2029, 114th Cong., div. N., tit. I §§ 101-111 (enacted). See also Orin Kerr, *Op.*, *How Does the Cybersecurity Act of 2015 Change the Internet Surveillance Laws?*, *Volokh Conspiracy*, *Wash. Post* (Dec. 24, 2015), <https://www.washingtonpost.com/news/volokhconspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/> (describing the recently adopted provision of the Omnibus Appropriations Act aimed at cybersecurity surveillance-the Cybersecurity Act of 2015).
- 34 See *infra* Part IV.a.
- 35 Cf. Geoffrey Parsons Miller, *The Law of Governance, RiskManagement, and Compliance* 535 (2014) (“The traditional notion conceives of risk as the chance of something bad happening The more modern approach, however, sees the chance of something bad happening as only one aspect of risk. A more general understanding would also include the chance of something good happening. Risk in this sense is measured by the dispersal of outcomes rather than simply the chance of a bad one.”).
- 36 *Id.*
- 37 See Roger Miller & Donald Lessard, *Evolving Strategy: RiskManagement and the Shaping of Large Engineering Projects* 4 (MIT Sloan Sch. of Mgmt., Working Paper No. 4639-07, 2007), <http://ssrn.com/abstract=96260> (“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.”).
- 38 Anthony Saunders & Marcia Millon Cornett, *Financial Markets and Institutions* 576 tbl.19-1 (5th ed. 2012). 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.* Financial institutions face these and several other risks. See, e.g., *id.* (defining risks in financial institution). Because the attributes of the business models of financial institutions vary, the risks described here may present differently for each type of financial institution.
- 39 See Heath Price Tarbert, *Comment*, [Are International Capital Adequacy Rules Adequate? The Basel Accord and Beyond](#), 148 *U. Pa. L. Rev.* 1771, 1775 (2000) (“The bank’s role as a financial intermediary involves many specific risks, of which the most predominant is credit risk—that a borrower will default on a loan.”); Kristin N. Johnson, [Governing Financial Markets: Regulating Conflicts](#), 88 *Wash. L. Rev.* 185, 206 (2013).

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

- 40 See Kristin N. Johnson, [Addressing Gaps in the Dodd-Frank Act: Directors' RiskManagement Oversight Obligations](#), 45 U. Mich. J.L. Reform 55, 64 (2011) (“Large, complex financial institutions originate loans to many types of borrowers including corporations with operations around the world; other banks, thrifts, and more sophisticated financial institutions; hedge funds; and private equity firms.”).
- 41 FDIC RMS Manual of Examination Policies, Liquidity and Funds Management § 6.1-2 (2015).
- 42 When a financial institution does not possess the necessary cash to satisfy a withdrawer request, the institution “may have to sell some of their less liquid assets to meet the [demands].” Saunders & Cornett, supra note 38, at 579.
- 43 See id. (providing examples of financial institutions that experienced severe distress after a “run” by depositors on cash deposits).
- 44 Interest rate risk can occur when financial institutions “mismatch[] the maturities of its assets and liabilities as part of its asset transformation function.” Id. at 580. Longer maturity assets pose increased risk for financial institutions because interest rates can change from year to year. Office of Investor Educ. & Advocacy, Sec. & Exch. Comm'n, SEC Pub. No. 151, Investor Bull.: 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. Interest rate risk encompasses the following: refinancing risk, a type of interest rate risk where the “the cost of refinancing can be more than the return earned on asset investments”; reinvestment risk, “[t]he risk that the returns on funds to be reinvested will fall below the cost of funds”; and price risk, “the risk that the price of the security will change when interest rates change.” Saunders & Cornett, supra note 38, at 581-82.
- 45 Lending Rates, Bank of Can. (Oct. 2011), http://www.bankofcanada.ca/wp-content/uploads/2010111/lending_rates.pdf (explaining how banks set interest rates).
- 46 Saunders & Cornett, supra note 38, at 580.
- 47 Id. 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).
- 48 Johnson, supra note 40, at 63-64.
- 49 Saunders & Cornett, supra note 38, at 583. The named examples of risks are generally self-explanatory. For a careful and valuable examination of reputational risk and the theory of misconduct risk, see Christina Parajon Skinner, [Misconduct Risk](#), 84 Fordham L. Rev. 1559 (2016). It bears mentioning, however, that the sovereign risk described here refers to “[t]he risk that repayments from foreign borrowers may be interrupted because of interference from foreign governments.” Saunders & Cornett, supra note 38, at 588. Unlike loans to domestic corporations, where there are available remedies for default, loans to foreign subsidiaries may not be paid back because “the government of the country in which the corporation is headquartered may prohibit or limit debt repayments due to foreign currency shortages and adverse political events.” Id. If a foreign country is unable or unwilling to repay their debt, the loaning financial institution “has little if any recourse to local bankruptcy courts or to an international civil claims court.” Id. at 589. Insolvency can result in the failure of a significant financial institution, which could disrupt the domestic and global economy and even trigger a domino effect of global losses. See, e.g., id. (describing the failure of two major financial institutions, Washington Mutual and Citigroup, due to insolvency).
- 50 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), 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.”).
- 51 See, e.g., Steven L. Schwarcz, [Systemic Risk](#), 97 Geo. L.J. 193, 204 (2008) (defining systemic risk).

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

- 52 *Id.* at 198. Professor Steven Schwarcz instructs that “[t]hese consequences could include (a chain of) financial institution and/or market failures . . . [or] [l]ess dramatically . . . (a chain of) significant losses to financial institutions . . . [and] can deprive society of capital and increase its cost . . . or decrease[] its availability.” *Id.*
- 53 Hedge Funds and Systemic **Risks** in the Financial Markets: Hearing Before the H. Comm. on Fin. Servs., 110th Cong. 8 (2007) (statement of E. Gerald Corrigan, **Managing Dir.**, Goldman Sachs & Co.) (“[S]ystemic **risk** of a financial nature is . . . a financial shock that brings with it the reality or the clear and present danger of inflicting significant damage of the financial system and the real economy.”).
- 54 Frederic S. Mishkin, Comment on Systemic **Risk**, 7 Res. Fin. Svcs. Priv. & Pub. Pol’y 31, 32 (1995) (“Systemic **risk** is the likelihood of a sudden, usually unexpected, event that disrupts information in financial markets, making them unable to effectively channel funds to those parties with the most productive investment opportunities.”).
- 55 **Policy Statement on Payments System Risk**, 66 Fed. Reg. 30,199, 30,200 (Bd. of Governors of the Fed. Reserve Sys., 2001).
- 56 See generally Pierre Duguay, Dep’y Governor, Bank of Can., Remarks to the **RiskManagement** Association, Toronto Chapter, Toronto, Ontario (Jan. 8, 2009) (explaining the importance of **riskmanagement** strategies to achieve financial stability).
- 57 E.g., Nizan G. Packin, It’s (Not) All About the Money: Using Behavioral Economics to Improve Regulation of **RiskManagement** Financial Institutions, 1 U. Pa. J. Bus. L. 419, 434 (2012) (“**Riskmanagers** . . . attempt to reduce the likelihood of negative outcomes.”); Johnson, *supra* note 40, at 61 (“[M]ethods developed to measure, mitigate, or **managerisk** generally focus on estimating the probability and magnitude of **risks** that lead to losses.”); Miller & Lessard, *supra* note 37, at 8 (describing several **riskmanagement** techniques).
- 58 See Kristin N. Johnson, **Macroprudential Regulation: A Sustainable Approach to Regulating Financial Markets**, 2013 U. Ill. L. Rev. 881, 899 (describing the complexity of the **riskmanagement** strategies businesses adopt, including ERMs, which “attempt to comprehensively measure **risks**”).
- 59 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/article/fed-proposes-extra-capital-requirement-for-8-biggest-u-s-banks-1481507> (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-us-banks-refile-living-wills-after-regulatory-rebuke-1436212747> (reporting that, among others, JP Morgan Chase & Co. re-submitted plans for reorganization to help mitigate damage in the event of financial failure). See generally Rene Stulz, **RiskManagement** and Derivatives (2003) (providing insight into the way businesses can maximize corporate value through various **riskmanagement** techniques).
- 60 Johnson, *supra* note 40, at 63.
- 61 Robert Weber, **A Theory for Deliberation-Oriented Stress Testing Regulation**, 98 Minn. L. Rev. 2236, 2251 (2014) (citing Dan Borge, *The Book of Risk* 4 (2001)).
- 62 Georges Dionne, **RiskManagement**: History, Definition and Critique 6 (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2231635.
- 63 *Id.*; see also About the Association, Am. Fin. Ass’n, <http://www.afajof.org/details/page/3710241/About-the-Association.html> (last visited Sept. 20, 2015).
- 64 Dionne, *supra* note 62, at 7.
- 65 Press Release, Royal Swedish Acad. of Scis., The Prize in Economics 1990 (Oct. 16, 1990), http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/1990/press.html; Phillipe Jorion, Value at **Risk** 417-18 (3d ed. 2007) (describing CAPM).

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

- 66 Shinhua Liu, Currency Derivatives and Exchange Rate Forecastability, 63 *Fin. Analyst J.* 72, 72 (2007).
- 67 See Arthur E. Wilmarth, Jr., [The Transformation of the U.S. Financial Services Industry, 1975-2000: Competition, Consolidation, and Increased Risks](#), 2002 *U. Ill. L. Rev.* 215, 332-33 (noting how the availability of new financial “tools” such as derivatives led to increased hedging by financial institutions).
- 68 Dionne, *supra* note 62, at 8.
- 69 *Id.*
- 70 See [Uniform Financial Institutions Rating System](#), 62 *Fed. Reg.* 752, 752 (notice of adoption of policy statement Jan. 6, 1997) (providing a rating system by which to monitor the financial soundness and risk-taking of depository institutions using six key composite rating factors: Capital adequacy; asset quality management capability; earnings level and quality; liquidity adequacy; and market risk sensitivity).
- 71 See Allen C. Puwalski, Derivatives Risk in Commercial Banking, posting in [An Update on Emerging Issues in Banking](#), FDIC (Mar. 26, 2003), <http://www.fdic.gov/bank/analytical/fyi/2003/02603fyi.html> (“The ability of participants in the financial markets to adjust specific risk exposures enhances the efficiency of capital flows by allowing companies to conduct business activities without amassing certain risks that would otherwise attend that business.”).
- 72 Dionne, *supra* note 62, at 8.
- 73 *Id.*
- 74 Miller, *supra* note 35, at 563 (defining VAR as an estimate of “the maximum expected loss a firm will face within a specified probability level (known as the ‘confidence level’) over a particular time period (known as the ‘time horizon’)”).
- 75 Weber, *supra* note 61, at 2254.
- 76 See *id.* at 2238-39 (explaining how financial systems could benefit from stress testing).
- 77 *Id.* at 2238.
- 78 *Id.* at 2238-39.
- 79 *Id.* at 2239.
- 80 See *id.* (“What is new, however, is the zeal with which lawmakers and regulators have looked to stress testing as a regulatory technique.”).
- 81 See *id.* at 2301-02 (noting three themes regulators should focus on when dealing with regulated firms and the implementation of stress tests).
- 82 See John C. Coffee, Jr., [Extraterritorial Financial Regulation: Why E.T. Can't Come Home](#), 99 *Cornell L. Rev.* 1259, 1269-70, 1269 n.33 (2014) (noting the relevance of “commons” literature to the regulation of financial institutions (citing Kristin N. Johnson, [Things Fall Apart: Regulating the Credit Default Swap Commons](#), 82 *U. Colo. L. Rev.* 167, 174 (2011))). Coffee, Johnson, and Steven Schwarcz 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 scarce resources in a tragedy of the commons to the exploitation of scarce resources in a financial system). The innovative application of the tragedy of the commons parable to financial markets offers alternative

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

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.

- 83 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).
- 84 See 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).
- 85 Manyika et al., *supra* note 83, at 37 (“[W]e see huge growth in the digital portions of flows of goods and services—a process we call digitization.”).
- 86 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”).
- 87 See Jeremy C. Kress, *Credit Default Swaps, Clearinghouses, and Systemic Risk: Why Centralized Counterparties Must Have Access to Central Bank Liquidity*, 48 Harv. J. on 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”); Johnson, *supra* note 39, at 189, 209 (noting that self-regulatory organizations, including financial institutions such as the British Banker's 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).
- 88 See Pierre-Hugues Verdier, *Transnational Regulatory Networks and Their Limits*, 34 Yale J. Int'l L. 113, 114 (2009) (finding that although numerous institutions began regulating international economic interactions, “economic regulation in crucial areas such as competition, securities, and banking remains first and foremost a domestic phenomenon”).
- 89 E.g., Robert W. Staiger & Alan O. Sykes, *International Trade and Domestic Regulation* 44 (Stan. U. Pub. L. & Legal Theory Research Paper Series, Paper No. 1504913, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1504913 (illustrating how a country can regulate foreign actors who impose negative externalities on international markets by banning the importation of the foreign actor's harmful product and shifting the foreign producer's externalities from the domestic market).
- 90 See Gary B. Born, *A Reappraisal of the Extraterritorial Reach of U.S. Law*, 24 L. & Pol'y Int'l Bus. 1, 10-16 (1992) (discussing traditional notions of the extraterritorial application of national law, particularly in the context of the American notion of extraterritoriality).
- 91 Saunders & Cornett, *supra* note 38, at 579.
- 92 *Id.*
- 93 *Id.* at 578.
- 94 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).
- 95 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), <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”).
- 96 Memorandum from Gen. James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, U.S. Marine Corps., for the Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories 5 (2010).

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

- 97 Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 Cal. L. Rev. 817, 826 (2012).
- 98 *Id.* at 826-27.
- 99 *Id.* at 828 (quoting Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 Naval L. Rev. 132, 139 (2005)).
- 100 Hathaway et al., *supra* note 97, at 826.
- 101 Jones, *supra* note 1.
- 102 *Id.*
- 103 *Id.*
- 104 *Id.*
- 105 *Id.*
- 106 *Id.*
- 107 *Id.*
- 108 *Id.*
- 109 *Id.*
- 110 *Id.*
- 111 Fin. Indus. Regulatory Auth., Report on **Cybersecurity** Practices 1 (2015), http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.
- 112 See *id.* (discussing the threat of “hackers penetrating systems for the purpose of account manipulation”).
- 113 See Katherine T. Smith et al., *Case Studies of Cybercrime and Its Impact on Marketing Activity and Shareholder Value*, 2011 Acad. Mktg. Stud. J. (forthcoming), <http://ssrn.com/abstract=1724815> (“A challenge facing e-business or cyber-business is that it is vulnerable to e-crime, also called cybercrime. Cybercrime can totally disrupt a company's marketing activities. Cybercrime costs publicly traded companies billions of dollars annually in stolen assets, lost business, and damaged reputations. Cybercrime costs the U.S. economy over \$100 billion per year. Cash can be stolen, literally with the push of a button. If a company website goes down, customers will take their business elsewhere. In addition to the direct losses associated with cybercrime, a company that falls prey to cyber criminals may lose the confidence of customers who worry about the security of their business transactions. As a result, a company can lose future business if it is perceived to be vulnerable to cybercrime. Such vulnerability may even lead to a decrease in the market value of the company, due to legitimate concerns of financial analysts, investors, and creditors.” (internal citations omitted)).
- 114 Fin. Indus. Regulatory Auth., *supra* note 111, at 3.
- 115 *Id.*
- 116 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>.
- 117 *Id.*
- 118 Fin. Indus. Regulatory Auth., *supra* note 111, at 14, 22.

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

- 119 Id. at 5.
- 120 Id.
- 121 Id.
- 122 Id. at 1.
- 123 Id.
- 124 Id. at 4.
- 125 Id.
- 126 Id.
- 127 Id. at 4, 17. Other endogenous **cybersecurity** concerns include firms inadvertently granting new hires inappropriate access, employees accruing privileges by being promoted to a higher position with potentially greater access to information, and misuse of credentials when a thief steals an employee's credentials. Id. at 17.
- 128 Id. at 26.
- 129 Id. at 4; see also Justin Baer, Morgan Stanley Fires Employee Over Client-Data Leak, Wall St. J. (Jan. 5, 2015, 10:03 PM), <http://www.wsj.com/articles/morgan-stanley-terminates-employee-for-stealing-data-1420474557> (discussing how Morgan Stanley fired one of its financial advisers accused of “stealing account data on about 350,000 clients and posting some of that information for sale online in potentially the largest data theft at a wealth-**management** firm”).
- 130 Fin. Indus. Regulatory Auth., supra note 111, at 11.
- 131 Id. at 14.
- 132 Id.
- 133 Id. at 36.
- 134 Press Release, Fed. Trade Comm'n, FTC, DOJ Issue Antitrust Policy Statement on Sharing **Cybersecurity** Information (Apr. 10, 2014), <https://www.ftc.gov/news-events/press-releases/2014/08/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity>.
- 135 Fin. Indus. Regulatory Auth., supra note 111, at 36.
- 136 Id.
- 137 Id.
- 138 Id.
- 139 Id. at 24.
- 140 Hathaway et al., supra note 97, at 860 (“There has been only limited U.N. action on the issue of cyber-security. The U.N. General Assembly has passed several related resolutions. These resolutions, however, are vague and have not required any specific action by U.N. members.” (footnotes omitted)); id. at 861-62 (“NATO recently began to address the threat of cyber-attacks. NATO did little in response to the 2007 cyber-attack on Estonia, laying bare that it ‘lacked both coherent cyber doctrine and comprehensive cyber strategy.’ On the heels of that attack, NATO held its first meeting—the 2008 Bucharest Summit—to formally address cyber-attacks. This summit prompted the creation of two new NATO divisions focused on cyber-attacks: the Cyber Defence **Management** Authority and the Cooperative Cyber Defence Centre of Excellence.” (footnotes

omitted)); id. at 862-63 (“The Council of Europe has taken the most direct and concrete approach to regulating a subset of the cyber-security problem-in particular, cyber-crime-of any international organization to date. As the first international treaty on crimes committed using the Internet and other computer networks, the 2001 Council of Europe Convention on Cybercrime (‘Cybercrime Convention’) promulgated ‘a common criminal policy aimed at the protection of society against cybercrime,’ primarily through legislation and international cooperation. The United States ratified the Convention in 2006.” (footnotes omitted)); id. at 865 (“The Shanghai Cooperation Organization, an intergovernmental mutual security organization founded in 2001 by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan, has taken significant preliminary steps toward cooperation in the cyber-security area. In its Yekaterinburg Declaration of June 16, 2009, ‘[t]he SCO member states stress[ed] the significance of the issue of ensuring international information security as one of the key elements of the common system of international security.’ The Organization presents a possible center of gravity in international legal action on cyber-attacks.” (alteration in original) (footnotes omitted)).

- 141 [18 U.S.C. § 1030 \(2012\)](#).
- 142 [Pub. L. No. 107-347, 116 Stat. 2899](#).
- 143 [Cyber Security Research and Development Act, Pub. L. No. 107-305, 116 Stat. 2367](#).
- 144 [Pub. L. No. 107-347, § 301-05, 116 Stat. 2946, 2946-61](#).
- 145 [Pub. L. No. 107-296, § 225, 116 Stat. 2156](#).
- 146 [Pub. L. No. 113-274, 128 Stat. 2971](#).
- 147 [Pub. L. No. 113-282, 128 Stat. 3066](#).
- 148 See Hathaway et al., *supra* note 97, at 877 (“U.S. domestic law, though potentially a powerful tool for battling cyber-attacks, has not yet addressed the challenge directly, and what remedies exist are in many cases restricted by jurisdictional limits.”).
- 149 [H.R. 2029, 114th Cong., div. N, tit. I §§ 101-111 \(2015\) \(enacted\)](#).
- 150 [Cybersecurity Legislation Watch, ISACA, <http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx> \(last visited Feb. 10, 2016\)](#).
- 151 [H.R. 2029, div. N, tit. I, § 102\(4\)](#).
- 152 See generally id. tit. I (describing the new information sharing exchange).
- 153 See id. (setting up regulations to encourage information sharing).
- 154 Id. § 102(5)(A).
- 155 The statute defines a defensive measure as “an action, device, procedure, signature, technique, or other measure . . . that detects, prevents, or mitigates a known or suspected [cybersecurity](#) threat or security vulnerability.” Id. § 102(7)(A).
- 156 Id.
- 157 Id. § 102(6)(A)-(H).
- 158 Id. § 104(d)(2)(A)-(B).
- 159 Id. § 105(d)(5)(A).
- 160 Id. div. N, tits. I-III. Title III is called “Federal [Cybersecurity](#) Workforce Assessment,” and states that the federal government must evaluate the current state of its [cybersecurity](#) workforce and identify critical needs for information technology,

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

- cybersecurity**, or other cyber-related workforce. Id. tit. III, § 304(a)(1). The government must submit progress reports in compliance with this section. Id. § 304(a)(2).
- 161 Id. tit. I, § 105; see id. § 102(7)(a) (defining a defensive measure as “an action, device, procedure, signature, technique, or other measure . . . that detects, prevents, or mitigates a known or suspected **cybersecurity** threat or security vulnerability”).
- 162 Id. § 404(c), § 206(c)(2).
- 163 Id. § 401.
- 164 Id. div. N, tit. IV, § 403.
- 165 John D. McKinnon, Congress Poised to Pass **Cybersecurity** Measure, Wall St. J. (Dec. 16, 2015), <http://www.wsj.com/articles/congress-poised-to-pass-cybersecurity-measure-1450284622>; see also Press Release, Open Tech. Inst., Omnibus Funding Bill is a Privacy and **Cybersecurity** Failure (Dec. 16, 2015), <https://www.newamerica.org/oti/omnibus-funding-bill-is-a-privacy-and-cybersecurity-failure/> (quoting Robyn Greene, Policy Counsel at New America's Open Technology Institute, who said, “[t]he new, renamed version of CISA sets up a near free-for-all for the NSA and FBI to ramp up surveillance and investigation of Americans, and could seriously undermine data security and **cybersecurity** in general. If the excess of personal information that may be shared under this bill is targeted by malicious and nation state hackers-and there's no reason to think it won't be-this may well turn out to be the Intelligence Community's next major boondoggle.”).
- 166 Press Release, Open Tech. Inst., *supra* note 165.
- 167 Letter from Civil Soc'y Orgs., to Member of Congress (Dec. 17, 2015), <http://www.constitutionproject.org/wp-content/uploads/2015/12/Coalition-Letter-Opposing-Cybersecurity-in-Omnibus.pdf>.
- 168 Jessica Beyer, The **Cybersecurity** Information Sharing Act (CISA), Henry M. Jackson Sch. Int'l Stud., U. Wash. (Oct. 30, 2015), <https://jsis.washington.edu/news/the-cybersecurity-information-sharing-act-cisa/>.
- 169 Mark Jaycox & Lee Tien, Obama's Computer Security Solution is a Mishmash of Old, Outdated Policy Solutions, Electronic Frontier Found. (Jan. 16, 2015), <https://www.eff.org/deeplinks/2015/01/obamas-computer-security-solution-mish-mash-old-outdated-policy-solutions>. See, e.g., Dep't of Homeland Sec., Enhanced **Cybersecurity** Services, <http://www.dhs.gov/sites/default/files/publications/ECS%20Fact%20Sheet%2007.30.15.pdf> (last visited Feb. 22, 2016).
- 170 Jaycox & Tien, *supra* note 169.
- 171 Jenna McLaughlin, Hasty, Fearful Passage of **Cybersecurity** Bill Recalls Patriot Act, The Intercept (Dec. 19, 2015, 11:05 AM), <https://theintercept.com/2015/12/19/hasty-fearful-passage-of-cybersecurity-bill-recalls-patriot-act/>.
- 172 John D. McKinnon, Lawmakers, White House Near **Cybersecurity** Agreement, Wall St. J. (Dec. 15, 2015, 5:39 PM), <http://www.wsj.com/articles/lawmakers-white-house-near-cybersecurity-agreement-1450219168?cb=logged0.01276299450546503>; see also Damian Paletta & Daisuke Wakabayashi, Apple Piles On as Senate Debates Cyber Bill, Wall St. J. (Oct. 21, 2015, 11:46 AM), <http://www.wsj.com/articles/apple-piles-on-as-senate-debates-cyber-bill-1445442387> (reporting that Apple did not support the **Cybersecurity** Information Sharing Act and Apple's statement, “[t]he trust of our customers means everything to us and we don't believe security should come at the expense of their privacy”); Cory Bennett, Major Tech Group Comes Out Against Cyber Bill, The Hill (Oct. 15, 2015, 12:34 PM), <http://thehill.com/policy/cybersecurity/257029-major-tech-group-opposes-cyber-bill> (listing Sprint, T-Mobile, Amazon, eBay, Netflix, Microsoft, Facebook, Google, Apple and Yahoo as opponents of the CISA).
- 173 **Cybersecurity** Information Sharing Act of 2015, H.R. 2029, 114th Cong., div. N, tit. I, § 103(a)(1)-(2) (enacted).
- 174 See id. § 102(8) (defining Federal entity as “a department or agency of the United States or any component of such department or agency”).

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

- 175 See id. § 102(14)(A) (defining non-Federal entity as “any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof”).
- 176 Id. § 103(a).
- 177 David W. Opderbeck, **Cybersecurity** and Executive Power, 89 Wash. U. L. Rev. 795, 813 (2012).
- 178 Id. at 822.
- 179 Id. at 826.
- 180 H.R. 2029, 114th Cong., div. N, tit. I, § 106(c)(1)(B).
- 181 H.R. 4350, 114th Cong. § 1 (2016).
- 182 Fin. Indus. Regulatory Auth., supra note 111, at 3.
- 183 Id. at 4.
- 184 Id. at 31.
- 185 Id.
- 186 Id. at 16-27.
- 187 Id. at 2.
- 188 Id. at 38.
- 189 Id. at 1.
- 190 Michael D. Guttentag, An Argument for Imposing Disclosure Requirements on Public Companies, 124 Fla. St. U. L. Rev. 123, 124-25 (2004) (“Disclosure requirements are the primary tool the federal government uses to regulate public companies.”).
- 191 Div. of Corp. Fin., Sec. & Exch. Comm'n, CF Disclosure Guidance: Topic No. 2, **Cybersecurity** (2011), <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.
- 192 Id.
- 193 Id.
- 194 Id.
- 195 Id.
- 196 Id.
- 197 Id.
- 198 Cf. Joel Bronstein, The Balance Between Informing Investors and Protecting Companies: A Look at the Division of Corporate Finance's Recent Guidelines on **Cybersecurity** Disclosure Requirements, 13 N.C. J.L. & Tech. Online 257, 259 (2012) (noting that the guidelines force companies into a catch-22; they either expose themselves to further cyberattacks or **risk** failing to meet disclosure requirements).
- 199 See Black's Law Dictionary 497 (8th ed. 2004) (defining disclosure as “[t]he act or process of making known something that was previously unknown; a revaluation of facts”).

MANAGING CYBER RISKS, 50 Ga. L. Rev. 547

- 200 See Sam Young, Note, *Contemplating Corporate Disclosure Obligations Arising From Cybersecurity Breaches*, 38 J. Corp. L. 659, 663-64 (2013) (noting the potential impact that a cyberattack would “have on investors or potential investors in a public company”).
- 201 See Deloitte, *CISOs Welcome SEC Cyber Security Disclosure Guidance But Struggle to Respond*, C10 Journal, Wall St. J. (Aug. 29, 2012, 12:01 AM), <http://deloitte.wsj.com/cio/2012/08/29/cisos-welcome-sec-cyber-security-disclosure-guidance-but-struggle-to-respond/> (“[C]ompanies are wondering what cyber risks they need to disclose and how they can disclose them without exposing their vulnerabilities and inviting cyber criminals to attack them.”).
- 202 See *TSC Indus. v. Northway, Inc.*, 426 U.S. 438, 448-49 (1976) (noting that disclosure of too much information could, if “trivial information,” “bury” investors and prevent informed decisionmaking).
- 203 See Roland L. Trope & Sara Jane Hughes, *The SEC Staff’s “Cybersecurity Disclosure” Guidance: Will It Help Investors or Cyber-thieves More?*, Bus. L. Today, Dec. 2011, at 4, <http://www.americanbar.org/content/dam/aba/publications/blt/2011/12/sec-cybersecurity-201112.authcheckdam.pdf> (explaining the Hobbesian choice created by the SEC’s guidance; businesses will either discuss too little or too much).
- 204 See Intelligence & Nat’l Sec. Alliance, *Addressing Cyber-Security Through Public Private Partnership: An Analysis of Existing Models 3* (2009) (“Since the nation’s cyber infrastructure is not government owned, a partnership of government, corporate and private stakeholders is required to secure the internet.”).
- 205 See Sari Greene, *Cybersecurity is an Executive Responsibility: Preparing for Upcoming Cybersecurity Examinations*, Maine Banker, Mar.-Apr. 2015, at 5, <http://learn.sagedatasecurity.com/hubfs/docs/cybersecurity-is-an-executive-responsibility.pdf?t=1443532531801> (“While not mandatory, there is an expectation that financial institutions will adopt the NIST Cybersecurity Framework as a way to measure cybersecurity readiness and resilience, as well as to create a cybersecurity roadmap.”); Paul A. Ferrillo, *Understanding and Implementing the NIST Cybersecurity Framework*, Harv. L. Sch. F. on Corp. Governance & Fin. Regulation (Aug. 25, 2014), <http://corpgov.law.harvard.edu/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/> (quoting Graham Scott, Interview: Greg Touhill, DHS, USA on Cybersecurity, Global Gov’t Forum (July 28, 2014), <http://www.globalgovernmentforum.com/brigadier-general-greg-touhill-cybersecurity-department-of-homeland-security-interview/> (“Though ‘voluntary,’ it cannot be overstated that the [NIST] Framework is ‘a National Standard’ developed with input from industry experts, collaborators and businesses with years of cyber experience.”)).
- 206 Nat’l Inst. of Sci. and Tech., *Framework for Improving Critical Infrastructure Cybersecurity* 37 (2014), <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.
- 207 Id. at 1.
- 208 See supra notes 186-89 and accompanying text.
- 209 Nat’l Inst. of Sci. and Tech., supra note 206, at 2.
- 210 Id.
- 211 Id. at 4.
- 212 Id. at 8.
- 213 Id.
- 214 Id.
- 215 Id. at 8-9.
- 216 Id. at 9.

- 217 Id. at 5.
- 218 Id. at 11.
- 219 Id.
- 220 Id. at 5.
- 221 Id. at 10-11.
- 222 Id. at 9.
- 223 Id. at 5.
- 224 Id.
- 225 Id. at 12.
- 226 Id. at 13-14.
- 227 Id. at 14.
- 228 Id.
- 229 Id.
- 230 Id.
- 231 Id.
- 232 Id.
- 233 Id.
- 234 PricewaterhouseCoopers LLP, Why You Should Adopt the NIST **Cybersecurity** Framework 6 (2014), <https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf>.
- 235 Id.
- 236 Martin Giles, Defending the Digital Frontier, *Economist* (July 12, 2014), <http://www.economist.com/news/special-report/21606416-companies-markets-andcountires-are-increasinglyunderattack-cyber-criminals> (“Data breaches are becoming ever bigger and more common. Last year over 800 [million] records were lost, mainly through such attacks Among the most prominent recent victims has been Target, whose chief executive, Gregg Steinhafel, stood down from his job in May, a few months after the giant American retailer revealed that online intruders had stolen millions of digital records about its customers, including credit- and debit- card details. Other well-known firms such as Adobe, a tech company, and eBay, an online marketplace, have also been hit.”); see also Fin. Indus. Regulatory Auth., *supra* note 111, at 38 (encouraging businesses to recognize and combat growing **cybersecurity** threats).
- 237 Barack Obama, President of the United States, Remarks by the President in the State of the Union Address (Feb. 12, 2013).
- 238 Yogesh Malhotra, **Risk**, Uncertainty, and, Profit for the Cyber Era: Model **RiskManagement** of Cyber Insurance Models Using Quantitative Finance and Advanced Analytics 12 (Jan. 2015) (unpublished thesis, State University of New York), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553547.
- 239 Id. at 1-12.

End of Document

© 2017 Thomson Reuters. No claim to original U.S. Government Works.