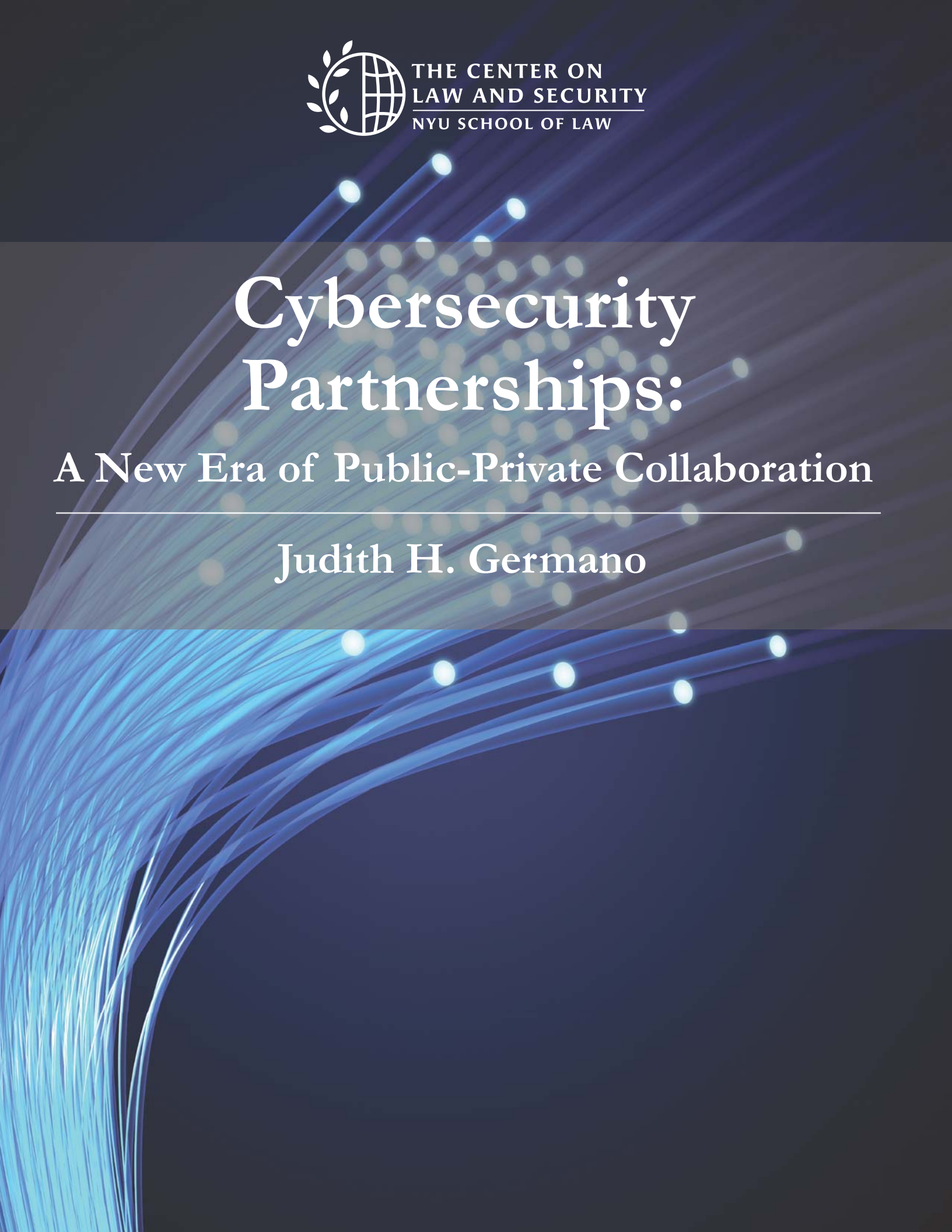

Cybersecurity Partnerships:

A New Era of Public-Private Collaboration

Judith H. Germano

Cybersecurity Partnerships:

A New Era of Public-Private Collaboration

Judith H. Germano

October 2014

The Center on Law and Security
New York University School of Law
139 MacDougal Street
New York, NY 10012
212.992.8854

CLS@exchange.law.nyu.edu
www.lawandsecurity.org

It is generally understood that the public and private sectors need to collaborate to address the nation's cybersecurity challenges, yet there remain significant questions regarding the circumstances, nature, and scope of those relationships. Legal, strategic, and pragmatic obstacles often impede effective public-private sector cooperation, which are compounded by regulatory and civil liability risks. Different government agencies have competing roles and interests, with the government serving dual roles as both partner and enforcer, influencing how companies facing cyberthreats view public authority. These domestic cybersecurity challenges are complicated further by cross-border issues, including inconsistent laws and perspectives regarding, in particular, privacy norms and restrictions, data transferability, and divergent political interests in combatting cyberthreats.

A welter of issues involving technology, business, law, and policy affect the strategic cybersecurity relationship between the government and the private sector. And many of those issues are evolving and unclear. Because cybersecurity's challenges are multi-faceted, traditional modalities of interaction between government and private sector—between regulators and regulated—do not always capture the nuanced ways in which the nature of the cybersecurity challenge has fundamentally altered these relationships.

In an effort to better understand and, hopefully, help address the challenges of institutionalizing effective cooperation, this paper will explore four key areas that should be clarified as a necessary step in adopting a strategic approach to cybersecurity:

1. Why is cybersecurity different from other threats, and why is public/private collaboration uniquely valuable to address cybersecurity challenges?

2. What barriers—including, for example, the evolving regulatory and civil litigation landscape, and cross-border challenges—impede effective cybersecurity collaboration, and themselves generate additional layers of uncertainty and cost for institutional victims of cyber attacks?

3. In light of those barriers, and available private-sector resources, should companies focus on self-help for addressing cybersecurity issues? When and to what extent can companies more effectively combat cyber threats without government assistance?

4. What methods of public-private sector collaboration have been more successful than the traditional models of governance, and what roles can, and should, different parts of the government play in a comprehensive cybersecurity strategy?

While the problems are difficult, the answers may, in some respects, be astounding in their simplicity—solutions grounded in basic principles of organizational communication, teamwork, trust and relationship building, accountability, and foresight to prepare for and invest in mitigating risk before disaster strikes. These approaches are critically important and readily attainable, for those within industry and government who are willing to invest time, thought, and resources proactively, to avoid the far greater costs of an ill-prepared cyber response strategy.

Yet, in other ways, the challenges to effective cybersecurity solutions are confounding. The technology is often complex and constantly evolving, the vulnerabilities are vast and elusive, and the laws are fragmented and unclear. Perhaps the greatest challenges emerge from the significant, sometimes competing, domestic and foreign policy consequences impacting both government and business that flow from any proposed policy or legal response. These issues emerge at the intersection of technology, risk management, business, law, and strategy; successfully navigating them requires a sophisticated understanding of each of those diverse areas.

Government and industry bring a diverse range of resources, priorities, and perspectives to these issues that can sometimes compete. But, at a strategic level, they often are fundamentally aligned in their shared desire to develop effective strategic solutions to cybersecurity challenges. The key is determining how best to maximize the collective resources of business and government at that point of alignment.

Ultimately, the short answer is that no single actor (or group of actors) can figure it out alone. A strategic cybersecurity solution mandates the combined resources and coordination of government and industry, within a practical framework that balances effectiveness with efficiency,

and security with privacy and innovation. To reach that solution, we first need to understand the benefits, barriers and alternatives to effective coordination, and why the nature of the problem demands new and innovative forms of collaboration. In doing so, we will come to realize that the government and private sector already are innovating in the forms of collaboration necessary to address the cybersecurity threat; next, the challenge will be to institutionalize and expand these means of working together.

I. The Collaboration Imperative?

Does a private company need to cooperate with the government to adequately address its enterprise risk management concerns, or do the risks of government cooperation outweigh the benefits? When and why is that cooperation valuable and effective for a company? These questions often arise—sometimes directly, other times implicitly—when companies are creating a cybersecurity program or responding to a particular incident. Corporate decision-makers and advisors who have not previously dealt in a collaborative (and positive) way with the government generally are less willing to initiate contacts with the government after a cyber incident.

The private sector owns and controls many of the critical systems that need to be protected, and frequently has more resources than government for recruiting top technical and information security talent. Additionally, the private sector does not face many of the constitutional and statutory restrictions that regulate government's investigatory activities. Moreover, a host of private companies and consultants ready to assist the private sector with threat monitoring and detection, incident response, and active defense strategies have emerged in recent years. Thus, companies often not only fear the collateral consequences of involving the government in cyber incident response, but also feel confident they can handle the problems on their own.

Yet, even where critical systems are owned and operated by private companies, the government often still is expected to ensure that those systems are secure and to respond if they are damaged.

Moreover, while the private sector has crucial insight, expertise, and resources for combatting cyberthreats, the government is uniquely positioned to investigate, arrest, and prosecute cybercriminals; to collect foreign intelligence on cyberthreats; and, potentially, to provide certain statutory protections to companies that share information with the government.[1] The government also may be privy to threat information—from both domestic and foreign sources—in advance of that information being available to the private sector and can collect and disseminate information across companies and industries. In this way, the government can provide a more complete perspective on the threat and on effective mitigation techniques, while taking steps to protect individual victims. This can help assuage competitive and reputational concerns about revealing a particular company's vulnerabilities to its competitors, the marketplace, and cybercriminals.

Accordingly, because significant access, expertise, and perspective needed to address the cyberthreat reside in both the private and public sectors, and because the law in this area is unsettled, collaboration is essential to attain feasible and effective cybersecurity solutions. It is also important for the private sector be significantly involved in the development of the legal regime regarding cybersecurity or we risk ending up with laws that cannot be implemented as envisioned. Also, the private sector often needs the government's help to reach across borders and develop comprehensive international solutions to tracking, identifying, and mitigating cyberthreats.

II. Barriers To Effective Cooperation

Despite its importance and the potentially significant impact of a campaign to harmonize the efforts of the government and private sector in cybersecurity, there exist legal, pragmatic, cultural, and competitive hurdles to effective cooperation that need to be addressed. These hurdles mean that many companies may be inclined to refrain from extensive cooperation in addressing their cybersecurity challenges. And, despite the pervasive and persistent threat, a number of companies only consider working with the government once they are in crisis mode and responding to a cybersecurity incident, rather than on an ongoing and proactive basis. Major categories of obstacles

to effective cooperation between public and private actors combatting pervasive cyberthreats include: (1) issues surrounding trust and control of incident response; (2) questions about obligations regarding disclosure and exposure; (3) the evolving liability and regulatory landscape; (4) challenges faced in the cross-border investigation of cybercrime; and (5) cross-border data transfer restrictions that impede the ability of companies to respond nimbly to cyberthreats and incidents.

1. Trust & Control

The first major barrier to cooperation involves issues of trust, benefit, risk, and control. Can the organization's leaders trust the government not to unduly interfere with operations? What business benefits exist, weighed against the potential risks (including the perception of being too closely aligned with the U.S. government) to make this cooperation valuable? And how does one assess whether, and to what degree, cooperation makes sense in a particular scenario? Often, the issue turns on whether the company perceives itself to be able to better and more effectively address the problem on its own without government intervention, and whether there are legal duties to involve the government or otherwise disclose the threat or breach.

Some companies find it easier to address the problem on their own without government intervention and assistance. This generally occurs for several reasons. For example, a company may seek to retain control of the process and outcome of a breach investigation and response to avoid the risk of giving the government license to explore its systems or disclosing privileged or otherwise confidential information. Or a company may not be sure whether, and how, the government can assist it—or even whether it can or should share the information it has—and may not know whom in the government to ask for help. Another reason for reluctance is that a company may not know the scope of the breach and whether, by reaching out to the government, it could be triggering an unnecessary alarm or prematurely conceding the "materiality" of a breach and thereby subjecting it to disclosure obligations.

Some private companies also are reluctant to work with the government unless they are able to obtain adequate assurances that doing so does not mean they are granting unfettered access to, and possibly ceding control of, their private computer systems, proprietary information, and incident response strategy. Another barrier is timing—the government is not always as nimble as the private sector in responding to an incident due to bureaucratic and other constraints. And, if the government is leading the inquiry, the company may lose its ability to control the timing and process of the investigation, including how quickly it can terminate company insiders who may be implicated, notify those impacted, and change its controls to defend against a continuing attack. Companies also are understandably sensitive to maintaining independence and autonomy, protecting customers' privacy, and (particularly post-Snowden) avoiding any negative perception that they are working "too closely" with government. The sooner the government can identify and address those concerns, and explain the methods and safeguards it employs, the more effectively the government can establish productive relationships with impacted organizations. Whether any productive dialogue exists between a victim-company and the government is also often based on idiosyncrasies surrounding which particular officials are handling a matter. There remains a lack of clarity at the field level—both on the part of government and private sector actors—regarding the type and degree of information that can and should be shared and when.

There also is a significant concern that information sharing often is a one-way relationship: the government accepts information that companies share, but is not always capable of rendering tangible assistance in return. That relationship has improved dramatically in recent years regarding cybersecurity incidents, in particular through better communication and innovative approaches to cybersecurity collaboration (some of which are discussed below). The reality remains, however, that the government is constrained by secrecy obligations regarding national security, intelligence, grand jury information and Fourth Amendment issues that restrict how the government can interact with private employees' and customers' computer systems and data. Although there have been significant improvements in the balance of public-private sector information sharing, this is just one facet of a comprehensive response to a cybersecurity incident. Improvements in threat information sharing and remediation within and among industry

sectors, and the important role of industry consultants with prior government experience also are valuable.

2. Disclosure & Exposure

Yet another barrier to effective public-private sector cooperation is the matter of disclosure and exposure. Many companies remain reluctant to reveal security vulnerabilities, especially before they fully have assessed the scope of the problem. They are concerned that doing so will mean they could face negative press, regulatory scrutiny, and civil litigation. Yet, nationally and internationally, a patchwork of data breach notification laws require prompt disclosure of breaches, on the premise that such notice enables those affected to take protective action, including by changing passwords and more closely monitoring, or shutting down, compromised accounts. This fragmented landscape, however, is complicated by the wide range of government actors involved, each of which has a different role and focus. For example, the Federal Trade Commission (FTC) is primarily concerned with consumer rights; the Securities and Exchange Commission (SEC) focuses on regulated entities' behavior and disclosure requirements; and the Department of Justice (DOJ) deals primarily with preventing, investigating and prosecuting cyber crime and addressing domestic cyber threats. The National Security Agency and U.S. Cyber Command, meanwhile, are focused on intelligence matters and the use of cyber capabilities by the military.

Companies also are reluctant to contact the government for help addressing a cybersecurity incident out of fear they will be exposed in a government press release (or subject to a press leak), which may have negative repercussions for the company before the company has assessed the level of damage or implemented a fix for the security breach. This loss of control over the timing, content, and process of a disclosure makes some companies reluctant—or at least hesitant—to contact the government for help when a vulnerability or breach is discovered.

As the aftermath of the recent Target breach demonstrated, CEOs, as well as other senior corporate executives and board members, increasingly are held personally accountable for cybersecurity incidents. Target had sophisticated cybersecurity systems in place (what it described as "among the best in class" in the retail industry) and was even certified as complying with industry standards for handling payment card information (PCI) in September 2013.[2] Yet, during the 2013 holiday season, Target suffered a high-profile breach affecting approximately 40 million customers' credit card numbers, as well as 70 million addresses, phone numbers, and other pieces of personal information.[3] According to reports, Target spent $61 million through February 1, 2014, responding to the breach[4] and saw declines in its holiday sales and stock prices.[5] And, by some accounts, Target ultimately will spend billions of dollars, in litigation, remediation and other costs, due to the breach.[6]

Target's Chairman, President, and Chief Executive Officer, Gregg Steinhafel, had been with the company for thirty-five years, spending the last six as CEO. Yet on May 5, 2014, Target's board of directors announced that Mr. Steinhafel would be stepping down.[7] The board's press release announcing the resignation stated: "Most recently, Gregg led the response to Target's 2013 data breach. He held himself *personally accountable* and pledged that Target would emerge a better company."[8] Target's directors were also under fire. The proxy advisory firm Institutional Shareholder Services (ISS) urged shareholders to oust seven of the company's ten board members for "not doing enough to ensure Target's systems were fortified against security threats."[9] ISS blamed the directors serving on Target's audit and corporate-responsibility committees for the issue, saying that "it appears that failure of the committees to ensure appropriate management of these risks set the stage for the data breach, which has resulted in significant losses to the company and its shareholders."[10]

Just as ambiguity may exist about what exactly companies need to do to ensure they are protected—both against breaches and against liability after cybersecurity incidents—regulators also are struggling to identify the exact role they will play. As SEC Commissioner Luis A. Aguilar aptly stated in March 2014: "There is no doubt that the SEC must play a role in this area. What is less clear is what that role should be."[11] That statement was two and a half years after the SEC's staff in the Division of Corporate Finance issued its October 13, 2011 guidance on issuers' disclosure obligations regarding cybersecurity harms and vulnerabilities.[12] The guidance recognized the goal of

eliciting disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision.[13] The SEC Guidance, specifically noting that it is "not a rule, regulation or statement," provides:

Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include:

- Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.[14]

Whether disclosure about these issues is sufficient to inform investors about the true costs and benefits of companies' cybersecurity practices is a matter of debate and discussion. Meanwhile, some have credited the SEC for not acting too quickly in a murky and developing area, while others have called for the SEC to take further regulatory action regarding issuers' disclosure requirements.[15] According to a Willis report on cyber disclosures in 10-Ks and Annual Reports that Fortune 1000 companies filed in 2012, a large number of cyber incidents were not deemed sufficiently "material" to trigger the requisite SEC disclosures, particularly for smaller companies.[16]

The Willis report noted:

- 21% of the Fortune 500 and 29% of the Fortune 501–1000 reported exposure to business interruption as a result of a cyber event;
- 21% of the Fortune 500 and 15% of the Fortune 501–1000 reported perceived exposure to cyber terrorism; and
- 13% of the Fortune 500 and 8% of the Fortune 501–1000 identified intellectual property risks.

Significantly, the report stated: "We note that the disclosure of actual cyber events remains at 1%, a seemingly low number given the number of attacks that appear in the press on a regular basis." Moreover, in disclosing risk protections (*i.e.*, insurance), the report noted that: "52% of the Fortune 500 and only 35% of the Fortune 501–1000 disclose the use of technical risk protections; 57% of the Fortune 501–1000, as opposed to 45% of the Fortune 500, make no reference to any risk protection."

Regarding cyber risk, the Willis report stated that the largest difference between the Fortune 500 and the Fortune 501–1000 was the percentage of each category that stayed silent on cyber risk: 12% of the Fortune 500 remained silent as opposed to 22% in the Fortune 501–1000.[17] According to the report: "The reason for this may be that, as companies get smaller, they may see themselves as less likely targets of an attack, or it may be that smaller companies needed more time to identify their cyber exposures."[18] Yet, the reality is that a large number of companies—due to lack of resources and knowledge—are just not dealing with cybersecurity risk and incidents. Companies that are grappling adequately with the challenge seem to be those who are forced to do so in response to a major breach; large companies with significant resources; and those that have executives, board members, or advisors who are particularly cyber-savvy. That leaves a large number of organizations still opting to keep their heads in the sand, or at least ducking the issue for another time. That divide, however, is changing as the dialogue increases on cybersecurity incidents, responses, and duties, and as the regulatory and civil liability landscape evolves, thereby highlighting the risk of failing to address cyber risk and incidents. With time and experience (and even more alarming news reports), more companies are becoming aware of, and realizing they need to address, cybersecurity concerns on a proactive basis.

3. *Cybersecurity's Evolving Regulatory & Liability Landscape*[19]

The evolving cybersecurity regulatory and liability landscape compounds the challenges that companies face from cyberattacks and further complicates the ability of corporate executives and their advisors to understand and effectively manage cyber risk. Companies must prepare for and respond to a potential cyberattack's direct damage, including financial and data loss, system and service interruptions, reputational harm, and compromised security. However, cyberattacks also expose companies to diverse and uncertain regulatory and civil liabilities. Although these risks generally become apparent post-breach, they must be contemplated and managed proactively before a breach occurs.

Theories of liability revolve around both the actual breach and the company's response to the breach, including regarding the content and timing of notice and disclosure. And exposure can be grounded in statutory, regulatory, and common law. Recent breaches have triggered a variety of claims based on inadequate security measures constituting unfair or deceptive practices, breach of contract, negligence, unjust enrichment, breach of fiduciary duty and duty of care, and negligent misrepresentation.

Ultimately, the divergent theories of liability against which companies might need to defend themselves derive from important differences in the goals and methods of diverse cyber actors, as well as the various institutions within the United States that have responsibility for cybersecurity. Different government agencies take different approaches to disclosure, with some encouraging enhanced cooperation, while others increasingly focus on holding companies accountable, civilly and possibly criminally, when their systems are breached. This challenge underscores why cybersecurity collaboration must be approached with an open mind and innovative approach to problem solving.

The SEC, FTC, and state attorneys general, for example, all have different mandates and focuses when guarding against different kinds of harms. When the perpetrator is an organized crime group, whose objective is to steal and then sell PCI or other personal data for a quick profit, there may be a large number of people affected, some of whom will subsequently turn into plaintiffs. The Department of Homeland Security, FBI, Secret Service, and other national security-focused government agencies, in turn, tend to seek different kinds of relationships with companies that have been the subject of a breach. They also tend to address different kinds of threats, namely state-sponsored advanced persistent threats seeking sensitive intellectual property and valuable trade secrets, which do not always lead to identifiable harms outside the company that will generate lawsuits.

The decision-making of companies that are facing systematic and strategic cyberthreats, therefore, is fraught with legal uncertainty about the implications of how they prepare for and respond to the threat. With piecemeal statutes and regulations, and emerging technologies, companies must navigate myriad potential sources of civil and criminal liability related to cyber incidents whose doctrinal contours are unsettled. Concerns include, for example, how to: institute and monitor security protections; implement cyber incident response policies and procedures; disclose threat, vulnerability, and incident information; and determine when, whether, and how best to inform, and potentially cooperate with, government agencies and industry counterparts. In addition to the inherent difficulties in determining how to address these concerns, companies must also evaluate how each of those decisions may impact litigation risk.

The regulatory duties and liability risks that companies now face take many forms and go far beyond requiring a determination of whether and when a breach is sufficiently material to trigger applicable SEC and state disclosure obligations. Companies might also face enforcement and private civil actions brought by, for example, the FTC, the SEC, state attorneys general, the DOJ, plaintiffs whose data is compromised (*e.g.*, customers, clients, corporate partners, vendors, unrelated third-parties like affected banks, etc.), and shareholders. Congress has also conducted inquires of varying levels of formality in response to data breaches and companies may be accountable to regulatory agencies, including the Consumer Financial Protection Bureau, Federal Communications Commission, and Department of Health and Human Services, among others.

Litigation concerns are compounded by the fragmentary condition of state and federal laws governing cybersecurity obligations. The mixture includes statutes and regulations and evolving common law standards that pose an obstacle to formulating stable expectations about cybersecurity behavior. Despite legislative efforts and extensive discussions, there is currently no federal data breach notification law. Instead, there exists a patchwork of, sometimes contradictory, state data breach notification laws.

With the addition of Kentucky on April 10, 2014, forty-seven states, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have enacted legislation requiring private or government entities to notify individuals of security breaches of personally identifiable information.[20] In the context of this uncertainty, government enforcement has become more aggressive and the plaintiffs bar is also increasingly more active in this area.

What is the proper way to reconcile—or at least balance—the desire to assure companies that cooperation is beneficial and not an undue risk, while also holding them accountable for deficient security measures or for failing to provide timely and adequate disclosures of cyber vulnerabilities and attacks? The public and private sectors are struggling with that question and legislative efforts have thus far fallen short of providing an adequate answer.

Several noteworthy cases highlighting some of the various theories of liability (and diverse actors employing them) are addressed in a separate article.[21]

4. International Investigations and Prosecutorial Challenges

The international nature of cyberthreats also creates significant challenges, and presents unique opportunities, for cross-border collaboration on cybersecurity. While technological capabilities (and cyber vulnerabilities) often know no borders, there are vast differences in law and policy across countries that meaningfully shape and constrain action. Some of the most important factors include the role, reach, duties, and capabilities of government; perceptions and parameters of privacy; legal and policy limits on self-help by private companies; laws governing how evidence is gathered and used; and the legal and diplomatic relationship between countries, at times refracted through mutual legal assistance treaties. Those factors significantly impact how both government and companies respond, unilaterally or collaboratively, to cyberthreats. There is no clear roadmap for when companies should seek government assistance when facing international cyberthreats, or when they might have greater success if they were to proceed unilaterally to detect, prevent, and address cyber harms. In either approach, there exist stringent, though inconsistent, cross-border data transfer restrictions that create an extra layer of challenge in responding to cyberthreats.

In the traditional model of cross-border criminal investigation, law enforcement agencies often work with victim companies to identify perpetrators, collaborate with local host governments to collect evidence that ultimately can be introduced in American judicial proceedings, and, if the stars align, then begin often protracted extradition proceedings, or lure a perpetrator to a jurisdiction in which an arrest can be affected (and then begin the protracted extradition process). Yet, for a variety of reasons, including non-cooperative jurisdictions from which a large number of cybercriminals operate, and difficult evidentiary questions, the traditional model alone often is insufficient to systematically dismantle networks of cybercriminals.

There is a significant lack of clarity regarding the parameters of public-private sector cooperation domestically, which becomes compounded when addressing cross-border investigations and incident-response. Testifying before a joint House Homeland Security Subcommittee meeting on May 21, 2014, Larry Zelvin, then-Director of the National Cybersecurity and Communications Integration Center (NCCIC) within the Department of Homeland Security (DHS), reported that legal hurdles were hindering the government's response to the Heartbleed vulnerability, which compromised hundreds of thousands of websites in April 2014. Zelvin stated: "While there was rapid and coordinated federal government response to Heartbleed, the lack of clear and updated laws reflecting the roles and responsibilities of civilian network security caused unnecessary delays in the incident response."[22]

Challenges also arise when targets are lodged in countries that will not extradite to, or cooperate with, the

United States, particularly when the perpetrators are themselves state actors. On May 19, 2014, the same day as the Blackshades takedown, the United States brought the first-ever criminal cyber-espionage case against state actors, charging five Chinese military officials with hacking into major U.S. companies to steal trade secrets.[23] While it is highly unlikely those defendants will ever appear in a U.S. court, the government sent both perpetrators and victims a global message that it is resolute in exposing cybercriminals, even those who are state actors. The domestic response to this action was mixed: on one hand, companies commended the government for taking a strong stance against cybercrime and undertaking potentially risky action to defend U.S. companies; on the other hand, there were complaints that the indictment was an ineffective "public relations ploy" with the potential to do more harm than good.[24]

As for the response in China, media reports note that Chinese officials have ramped up political and economic pressure on the U.S. government and large technology companies, and renewed their push to promote domestic technology.[25] A senior Chinese general, Sun Jianguo, spoke out at an international security forum, saying that the United States is the "world's biggest cyberthief" and alleged that it filed the indictment to draw attention away from itself.[26] From either perspective, this indictment shows that policy and strategy decisions often are integral components of a coordinated international cybersecurity response.

Recent successes show that one of the most important roles of government is to address cyberthreats by leveraging its international network of law enforcement partners, counterparts, and industry experts, buttressed by diplomatic and other channels and relationships in new and sometimes unconventional ways—a unique role that only the government is able to play. Effective responses to cyberattacks often must be swift and nimble.

International relationships built on informal information sharing and supported by formal procedures for gathering and preserving admissible evidence are extremely valuable. These efforts can be resource intensive and there are often barriers to trust, inconsistent goals and priorities, and legal hurdles. Successful collaboration therefore requires effective cross-border—and cross-barrier—communication and cooperation among government and private industry actors, preferably by establishing relationships and, if possible, information sharing procedures before a crisis arises. These measures must be thoughtful, reasonable, and undertaken with sufficient transparency so as not to further undermine trust in government and the public-private relationships that do exist, and must not overstep constitutional rights or norms and expectations of privacy.[27] While creating helpful international (and even domestic) laws that foster information sharing may be too far over the horizon to address today's pressing cybersecurity needs, current successful operations that test international coordination and strengthen those cooperative relationships are a large step forward in useful cross-border relationships to help combat cyberthreats.

5. Cross-Border Data Transfer Challenges

Efforts to enhance cross-border law enforcement cooperation have been hindered, however, by conflicting laws and policies. In particular, cross-border data transfer restrictions greatly limit international efforts to detect and thwart cyberattacks because international companies must comply with multiple and sometimes conflicting local, national, or supranational data protection laws. The European Court of Justice's landmark decision on May 13, 2014, involving Google and the Spanish Data Protection Authority underscores international companies' broad exposure and highlights the significant potential consequences of the extra-territorial application of European Union data protection laws.[28] In that ruling, the court interpreted Google's responsibility under European Union data protection laws regarding its online search engine broadly, finding that Google: (1) was subject to Spanish data protection law; (2) was obligated to delete web search results that link to web pages containing accurate but outdated information regarding a person; and (3) upon an individual's request invoking her "right to be forgotten," also must delete search results linking to even truthful information about a person that is prejudicial or that she wishes to be "forgotten" over time. Likewise, in February 2014, the Higher Court of Berlin ruled that Facebook was required to comply with German data protection laws even though Facebook processes German user data at its European headquarters in Ireland.[29]

These cases show the wide-reaching jurisdictional scope of different data privacy laws and the serious consequences if companies do not sufficiently understand their legal obligations. For companies seeking to gather information to identify perpetrators of hacks or to review their systems to assess harm, they also have to mind the welter of data protection laws and ensure they handle information and systems consistent with those laws. Companies and the U.S. government are required to exert significant effort to navigate potentially inconsistent cross-border obligations. These challenges can limit the flow of robust international cooperation and information sharing on cybersecurity matters, thereby impeding our collective ability to detect, prevent, and mitigate international cyberattacks.

Given this environment, the extant legal regime does not provide clear guidance to companies that are looking to effectively manage not only cyber incidents themselves, but also the attendant liabilities. Moreover, in light of the uncertainty and broad range of potential exposure, a victim-company may understandably be reluctant to disclose threat and incident information voluntarily to the government or may delay disclosure out of concern that the statements might be used against it in subsequent legal proceedings.

III. Go It Alone? Corporate Self-Help

In light of the obstacles to effective public-private cooperation to address cybersecurity challenges, companies often ask how far and in what manner they, as private actors, can proceed unilaterally and without government assistance to defend against cyberattacks. There may be certain circumstances where private actors, who may not be bound by domestic and international conventions, can be more effective in detecting and mitigating cyber harms than if they collaborate with government. And, at times, private companies and their advisors (many of whom have prior government experience) may be able to forge their own strategic relationships to such a degree that partnering with the U.S. government might hinder, rather than help, their efforts to address cyberattacks.

Companies are increasingly frustrated that, while they are under constant attack and facing debilitating harm, they also are themselves legally hindered in what measures they can take to defend themselves. Bolstering perimeter defenses, hardening application security, monitoring network traffic and scanning for malware are important and valuable. But a number of companies want to take more proactive, innovative, and bold action that may or may not be legal in the United States or elsewhere.

Companies are seeking more guidance from the U.S. government on how far they can go without the government's aid to identify perpetrators, halt attacks, and protect their systems and information. Companies, and their legal and strategic advisors, also often seek more information regarding the permissible potency of those measures. In addition to direct hack-backs—hacking into an intruder's computer to identify who she is and what she stole, an activity that is illegal in many countries—companies seek to use methods like the deployment of:

- Web beacons, to monitor behavior and pass along information such as the IP address and browser type of the computer perpetrating an infiltration;
- Honey pots, which are traps set to detect, deflect, or counter unauthorized users by luring them to a controlled environment where their behavior can be observed;
- Honey nets, which are two or more honeypots on a network; and
- Honey tokens, which are digital data created and monitored as indicators of digital theft, often distributed to ensure the perpetrator is likely to obtain it, enabling tracking of the perpetrator.[30]

Some companies also seek to use honey tokens with fake executables or with links embedded in data—if data is stolen and executed, the honey tokens "dial home" and send attribution information about the hacker.[31] But hacking a hacker is illegal in the United States and many other countries; besides, sophisticated hackers know to protect against such tactics.

What is particularly unclear is whether, and to what degree, a company's cybersecurity strategy should be regulated and by whom. For example, if a U.S.-based private company employs an overseas security firm to protect its

networks in countries where affirmative defense techniques contrary to American law are permitted, how much leeway would the security firm have and how closely would the company need to supervise its activities? Many of these questions lack clear answers.

The Computer Fraud and Abuse Act has two pertinent subsections that limit, or prohibit, active defense techniques:

> (a)(2)(C) whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer; [and]
> (a)(5) whoever
>
> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss [violates the law].[32]

Because the current version of the statute turns on access to a computer and not access to the information itself, defensive techniques must be structured accordingly.[33] There is an ongoing debate regarding how far companies can and should be permitted to go to protect their systems and respond to attempted and actual intrusions.[34] As technology advances, there will be an ongoing need to address the applicable laws and policies that govern this sphere and to provide clarity and direction on permissible actions and limitations.

Clarifying the laws regarding what unilateral action companies can take to defend themselves against cyberattacks would help to define the parameters of legitimate, private-sector responses to those attacks. But that, alone, is not a comprehensive solution to cyber threats. We also need to continue to develop innovative methods of working together across government and industry to collectively address cybersecurity issues.

IV. New Models: New Forms of Collaboration

To better define the collaborative landscape, and surmount the obstacles to effective cooperation on cybersecurity issues, there needs to be an ongoing dialogue among stakeholders regarding respective expectations and solutions. This dialogue should occur internally at both companies and the government, as well as between—and among—companies and the government.

We also need to clarify what companies and the government seek to obtain through a collaborative cyberdefense effort, beyond the obvious results of preventing and thwarting attacks and mitigating harm. One potential outcome is apprehending and prosecuting domestic and international cybercriminals, which can be valuable in deterring and preventing further attacks. If the goal is not only to stop the harm and to detect and deflect attacks as swiftly as possible, but also to use the evidence gathered to prosecute the wrongdoers, then evidence would need to be collected in a way that it would be admissible in court proceedings.

There are, however, other available tools, beyond prosecution, that can be considered, but they must be weighed against the financial and political consequences impacting companies and government. Those include, for example, sanctions and indictments of foreign officials, provided those steps are seen to reap sufficient benefits toward combatting international cyberthreats rather than potentially doing more harm than good and hindering international business opportunities.

In many cases, the answer to questions regarding the best means and method for detecting and preventing cyberattacks is a resounding: "It depends." Although the analysis of an appropriate response will vary depending on the circumstances, it is important to understand the issues, risks, benefits, options, and procedures impacting that response before an incident occurs. Indeed, there are many variables that affect how companies and the government approach cybersecurity issues, and the platform on which these issues are addressed is still evolving.

There have been, however, a number of innovative models of public/private cooperation that recently have emerged in response to the barriers to effective cooperation identified above. Strategic success in addressing the cybersecurity problem depends in large measure on continued innovation not only on technical cybersecurity measures, but also on models of collaboration between relevant actors.

For collaboration to exist and succeed, there must be safeguards in place to encourage parties on all sides to share information in a way that, to the greatest extent possible, protects confidentiality and competitive concerns. Improved and meaningful communication around the parameters of effective collaboration will help address the issues of trust and control that currently impede a coordinated cybersecurity analysis and defense.

The existing measures to improve information sharing between the government and private sector should also be examined, better defined, and potentially expanded. Those methods include granting limited security clearances to key corporate actors and embedding private sector actors in government-operated cybersecurity centers beyond those that already exist in the DHS. And it is important for companies to understand what information they can share, when, and how. Existing victim rights can also be buttressed or clarified to protect companies that may be reluctant to disclose a breach to the government (if they are not otherwise obligated by data breach notification or other laws), including by promoting collaboration on when and under what circumstances the government can or should disclose a breach or name a particular victim in the press.

But more still is needed. Fundamentally, changes must take place that institutionalize the processes by which the public and private sectors can cooperate to address the cyberthreat. These institutional forms of cooperation must be tailor-made to the nature of the cyberthreat, rather than mere adaptations of structures that were created to mitigate different kinds of problems.

1. Leveraging Resources & Expertise in Innovative Response Structures

Given the significant and evolving nature of cyberthreats, it is necessary to pool as many resources and informed perspectives as possible to address the problem comprehensively and effectively. And given the myriad extant barriers to effective cooperation, there needs to be innovation and creativity in the ways in which companies and the government do so.

An example of an innovative model of public-private cooperation to mitigate the new cybersecurity threat landscape can be found in the combined response to the crippling distributed denial of service (DDoS) attacks on American banks in 2012.[35] This was one of the largest DDoS campaigns ever launched, orchestrated by a group calling itself the Izz ad-Din al-Qassam Cyber Fighters, which disrupted service to the online banking portals of a number of major U.S. financial institutions.[36] At the peak of those DDoS attacks, U.S. banks were grappling with electronic traffic of up to 120 gigabytes per second—at least three times the volume of traffic most large bank websites were equipped to handle at the time—and banks were spending tens of millions of dollars to mitigate the problem.[37]

A. Financial Sector Coordination

To address this new type of threat, the government, together with industry implemented, on a global level, a new kind of response. Media reports in April 2014 revealed that, two years earlier, when major U.S. banks were besieged by the DDoS attacks, the U.S. government took the unprecedented step of appealing—both diplomatically and technologically—to 120 countries to help cut off the computer traffic at nodes around the world, thereby mitigating the threat. The two-pronged international appeal to counterparts overseas was made diplomatically by State Department officials and technologically by DHS cyber technicians.[38] While reports noted it was not a "silver bullet" to cease the attacks entirely, it did help to significantly ease the barrage of traffic that was crippling banks.[39]

In addressing this DDoS threat, private industry was also involved in sharing valuable threat and other infor-

mation, including recommended solutions. Much of the information sharing was coordinated through the Financial Services Information Sharing and Analysis Center (FS-ISAC), which interfaces with NCCIC.[40] This was highly effective in enabling financial institutions to thwart the 2012 DDoS attacks and to mitigate harm.[41] Since then, to further enhance its capabilities, the FS-ISAC has completed a Critical Infrastructure Notification System to allow it to send security alerts rapidly and simultaneously to multiple recipients worldwide, while authenticating users and confirming delivery.[42]

This and other examples of cyber cooperation illustrate the different roles that the U.S. government can play in a comprehensive cybersecurity strategy, which go beyond traditional approaches like law enforcement investigations and prosecutions, or intelligence activities of which victim companies remain unaware. Involvement can include intelligence gathering and, to the extent permitted, sharing; technological assistance and coordination; investigatory and prosecutorial efforts and assistance; and domestic and international outreach and coordination. But more important than any individual effort, a hybrid approach has evolved that makes use of various informal links within diplomatic, law enforcement, network defense, and other government agencies, as well as the private sector. The primary focus of this approach is usually to mitigate the cyber harm itself, though it also has proven valuable in helping apprehend and incapacitate perpetrators.

In the last several months, there has been a growing public discussion of a number of additional instances of novel forms of collaboration between the U.S. and other governments, as well as private industry experts, to combat cybercrime.

For example, on May 19, 2014, the FBI announced what it described as "unprecedented cooperation" in "the largest global cyber operation to date" involving Blackshades creepware.[43] According to prosecutors, Blackshades affected hundreds of thousands of users globally, allowing users of the malicious software to secretly and remotely control victims' computers. To accomplish this takedown, which involved more than ninety arrests and more than three hundred executed searches, the DOJ coordinated with nineteen cooperating countries.[44] While the DOJ has coordinated major international efforts in the past—including prosecuting large international child exploitation and narcotics trafficking rings—this type of effort in the cybercrime context is an unprecedented development. It is especially groundbreaking in the size of the operation, the varying level of cybercrime experience among partners in each of those countries, and the importance of operating in a swift and cross-border way to obtain significant results.

Just two weeks later, on June 2, 2014, the DOJ announced successful global operations resulting in the disruption of two massive and sophisticated cybercrime schemes related to the "Gameover Zeus" botnet and "Cryptolocker" ransomware, which also affected hundreds of thousands of computer users.[45] Through this effort, U.S. law enforcement coordinated with counterparts in more than ten countries and with numerous private sector industry experts in the United States. The DOJ described Gameover Zeus, which targets banking credentials and other personal information, as "the most sophisticated botnet" that the government and its allies "ha[d] ever attempted to disrupt;" the botnet employed an estimated 500,000 to one million compromised computers and diverted more than $100 million dollars from victim companies' bank accounts. Cryptolocker was a pernicious and complex scheme that secretly encrypted more than 234,000 hard drives and then demanded ransom payments for giving users access to their own files and data; the DOJ cited one estimate indicating that Cryptolocker garnered more than $27 million in ransom payments in just two months. Showing its willingness to reach outside its borders, the U.S. government brought federal charges in courts in Pittsburgh, Pennsylvania and Omaha, Nebraska against Evgeniy Mikhailovich Bogachev, the alleged administrator of the Gameover Zeus botnet, who lives in Anapa, Russia. Bogachev is described in court documents as the alleged leader of a gang of cybercriminals based in Russia and Ukraine who were behind the Gameover Zeus and Cryptolocker schemes.[46]

Then, on July 23, 2014, the Manhattan District Attorney's Office announced that seven individuals were arrested in the United States, Canada, and Europe for participating

in an international cyber ring that targeted 1,600 accounts of Stub-Hub, the online ticket selling website.[47] The purported head of the ring was a Russian national arrested while vacationing in Spain; he is now pending extradition to the United States.[48]

B. Numerous Cooperative Options Exist

Beyond these innovative approaches to specific cybersecurity problems, the government has created many task forces and inter-agency groups to facilitate robust information sharing within the government and between the government and private sector on an ongoing basis. For an example of intra-public sector coordination, the National Cyber Investigative Joint Task Force, led by the FBI, is comprised of nineteen members from the United States Intelligence Community and law enforcement agencies; it serves as the lead multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to domestic cyberthreat information and national security investigations.[49]

And there are several examples in the area of public-private sector coordination. The Department of Defense's Defense Cyber Crime Center, an Army initiative, is a national center focusing on addressing forensics, investigative training, research, and analytics impacting government agencies and private companies operating in the defense sector.[50] The DHS's U.S. Computer Emergency Readiness Team, the operational arm of the NCCIC, also plays a leading role in international information sharing.[51] And the DOJ's Computer Crime and Intellectual Property Section works with prosecutors and agents nationally and overseas, as well as with companies and governments, to investigate and prosecute cybercrime.[52]

The InfraGuard, ISAC and Electronic Crimes Task Force (ECTF) groups also have provided, for more than a decade, significant advances in public-private information sharing.[53] For example, the ECTFs at the U.S. Secret Service (USSS), which focus on identifying and locating international cybercriminals connected to cyber intrusions, bank fraud, data breaches, and other cybercrimes, have achieved significant success in detecting and apprehending numerous international cybercriminals.[54] Additionally, the USSS Cyber Intelligence Section has worked with law enforcement partners worldwide to secure the arrest of cybercriminals responsible for the thefts of hundreds of millions of credit card numbers and losses exceeding $600 million to financial and retail institutions.[55] These investigations are often most effective when there is robust information sharing and cooperation between the government and the private sector. While that phenomenon is not unique to cybersecurity cases, the information sharing is particularly valuable in combatting cybercrime because of the differences in the nature, type, and access to pertinent information and capabilities that reside in the private and public sectors. This includes, for example, instances where: victim-companies that have been hacked promptly report the breach and allow the government to access their systems to identify the point of entry and other vulnerabilities; victim-banks who issue credit cards help identify and track the compromised data and provide credit card numbers that are active but not tied to actual identities (so the bank, not a consumer, incurs the harm), which can be used in undercover operations; and credit card payment processors help identify and track activity of compromised cards and illicit payments.

For example, in the largest credit card breach to date, when Albert Gonzalez stole more than 130 million credit card numbers, the government compiled and analyzed breach information from several different victim-companies and determined similarities that showed the attacks were connected and likely from the same source.[56] Specifically, the government determined that the same code appeared in the SQL injection strings that were used to employ backdoors allowing access to the victims' systems and that the infiltration IP address (for injecting malicious code into those systems) and exfiltration IP address (for receiving the credit card data that was removed from the systems) were the same for each incident.[57]

As Congress continues to explore—as it has for years now without success—potential legislation to encourage cyber intelligence sharing and provide certain safe harbor protections to companies, cyberthreats continue to increase and new attacks occur on a daily basis. This conversation would be greatly enhanced by clarifying (through legislative or other means) what information companies and the government can properly share and what clearances,

protections, and controls exist to protect that information and those who provide or otherwise use it. Cybersecurity coordination too often is episodic or bureaucratic; this needs to be transformed into a workable culture of information sharing and coordination. Appropriate institutions must be created to effectuate the implementation of these cultural shifts, as many private actors still do not know whether, when, or how it would be beneficial (or detrimental) to engage with the government on these issues.

Because the legal landscape is evolving, it is important that the government and private sector communicate regarding the appropriate roles, capabilities, and authorities of law enforcement agencies (including the FBI, DHS, and USSS) and regulators (like the SEC and FTC), as well as regarding sources of potential civil liability. Public-private sector communication is essential to ensure a fair and practical legal framework that balances security, responsibility, accountability, information sharing, and common sense. That balance is best attained only after understanding the appropriate scope and framework of the public-private relationship regarding cybersecurity.

C. Making the Business Case for Collaboration

To better combat cyberthreats with a swift and coordinated response, the government and private sectors must promote awareness, at senior management and operational levels, of the benefits of public-private cooperation under particular defined circumstances and the risks or disadvantages if that sharing does not exist. In other words, we need to make "the business case" for public-private cooperation. To effectively do so while managing the shifting technological, legal, and political landscape requires executives, including at the board and senior leadership level, not only to make sure that adequate technological defenses are in place, but also to think strategically regarding how to create and implement corporate governance, communication, and response structures to manage cyber risk. This means ensuring that the organization can effectively identify and address emerging regulatory and liability issues on both a proactive and responsive basis. Moreover, because systems can be compromised at any level, it also involves communicating (through training and protocols) the significance and means of properly managing cybersecurity risk.

Accordingly, companies need to develop, implement, and test effective corporate governance structures for balancing those concerns while making and executing effective and timely decisions regarding cybersecurity cooperation and response. Much of this comes down to effective internal corporate communication and requires getting the right people in the room speaking a common language in a cybersecurity-focused discussion facilitated by internal, and sometimes external, experts. Some companies are doing that more effectively than others.

Given the backdrop of legal vulnerabilities and international hurdles, companies and the government need to think proactively regarding how to encourage a coherent, strategic approach to managing cybersecurity risk. This includes both traditional investigative and law enforcement measures, as well as more innovative diplomatic and strategic techniques that include effective cross-border and multi-agency collaboration and coordination, in a nimble framework that directly responds to the nature of the cyber threat on technological, strategic, business and policy levels. Success in this area mandates that key individuals within the private and public sectors cultivate and maintain open communication lines and cooperative relationships to be poised to respond quickly as challenges arise.

Although there is no "silver bullet" to address the diverse and persistent nature of cyber threats, and the problem is and will remain pervasive, enhanced public-private sector collaboration in recent years has yielded success. As stakeholders in business and government become increasingly aware of the significance and breadth of the threat, and the opportunities to engage in meaningful efforts to prevent, prepare for and respond to cyber attacks, including through effective relationships and collaboration between the government and private sector, we become better able to create a more effective and cohesive cybersecurity strategy.

ACKNOWLEDGMENTS

As part of the research culminating in this paper, and in addition to other innovative cybersecurity programming in the 2013–2014 academic year, NYU School of Law's Center on Law and Security hosted a series of roundtable discussions in early and mid-2014. We brought together key leaders, including high-ranking government officials, senior corporate executives from leading U.S. companies, and legal advisors from both the public and private sectors to explore critical cybersecurity issues impacting industry and government. We wish to thank those esteemed roundtable participants for giving generously of their time and valuable insights. In addition, I had numerous informal, individual conversations with leading stakeholders, experts and advisors in this area. I am particularly impressed and grateful that people who are so incredibly busy battling a virtual Typhon would agree to share their precious time to discuss these important issues. Their insight and willingness to share their thoughts, concerns and solutions provides greater hope for success as we, collectively, work toward more effective cybersecurity strategies and a collaborative framework for addressing cyber threats.

Judith H. Germano is a Senior Fellow at the Center on Law and Security, and Adjunct Professor of Law, at NYU School of Law. She is also the founding member of GermanoLawLLC. Judith specializes in cybersecurity, privacy, securities and other financial fraud, and regulatory compliance matters, and is the former Chief of Economic Crimes at the U.S. Attorney's Office, District of New Jersey.

The Center on Law and Security is a non-partisan multidisciplinary research institute at NYU School of Law focused on promoting informed dialogue and conducting groundbreaking research on the most important national security, legal, and strategic questions of the post-9/11 era. The Center is led by its Faculty Director, Professor Samuel Rascoff, and its Executive Director, Zachary Goldman.

The Center on Law and Security wishes to thank the Verizon Foundation for its generous support. The Center also wishes to thank Ernst & Young for its support.

[1] For examples of legislative efforts to promote public-private sharing of cybersecurity information, *see*, *e.g.*, Homeland Security Act of 2002, Pub. L. 108–275, tit. II, subtit. B, sec. 211, 116 Stat. 2135, 2150 (codified at 6 U.S.C. § 131–134 (2002)) (limiting the disclosure of cyber threat information shared with the Department of Homeland Security); H.R. 624, 113th Cong., *available at* https://beta.congress.gov/bill/113th-congress/house-bill/624 (allowing for the sharing of internet traffic information between the government and technology companies); S. 2588, 113th Cong., *available at* https://beta.congress.gov/bill/113th-congress/senate-bill/2588 (same).

[2] Bruce Carton, *ISS Recommends Ouster of Several Target Directors*, Compliance Week (May 29, 2014), http://www.complianceweek.com/blogs/enforcement-action/iss-recommends-ouster-of-seven-target-directors-for-data-breach-failures#.U91FChYePwJ (quoting statement of Target as "among best in class"); John P. Mello, Jr., *Target Breach Lesson: PCI Compliance Isn't Enough*, Tech News World (Mar. 18, 2014, 12:09 PM), http://www.technewsworld.com/story/80160.html (regarding PCI compliance).

[3] Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Cards: How Target Blew It*, Bloomberg Businessweek (Mar. 13, 2014), http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

[4] Amrita Jayakumar, *Data Breach Hits Target's Profits, But That's Only the Tip of the Iceberg*, Wash. Post, Feb. 26, 2014, *available at* http://www.washingtonpost.com/business/economy/data-breach-hits-targets-profits-but-thats-only-the-tip-of-the-iceberg/2014/02/26/159f6846-9d60-11e3-9ba6-800d1192d08b_story.html.

[5] Target's profit for the holiday shopping period fell 46 percent from the same quarter the year before; the number of transactions suffered its biggest decline since the retailer began reporting the statistic in 2008. *See* Elizabeth A. Harris, *Data Breach Hurts Profits at Target*, N.Y. Times, Feb. 26, 2014, *available at* http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html.

[6] Riley et. al, *supra* note 3.

[7] Statement from Target's Board of Directors (May 5, 2014), *available at* http://pressroom.target.com/news/statement-from-targets-board-of-directors.

[8] *Id.* (emphasis added).

[9] Carton, *supra* note 2.

[10] *Id.*

[11] Statement of Luis A. Aguilar, Comm'r, Sec. & Exch. Comm'n, "The Commission's Role in Addressing the Growing Cyber-Threat" (Mar. 26, 2014), http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184#.U-DhyRYePwI.

[12] SEC Div. of Corp. Fin., *CF Disclosure Guidance: Topic No. 2—Cybersecurity*, (Oct. 31, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[13] *Id.*

[14] *Id.*

[15] *See* Letter from Sen. John D. Rockefeller IV to Mary Jo White, Chair, Sec. & Exch. Comm'n (Apr. 9, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51 (urging SEC to take further action).

[16] *Willis Fortune 1000 Cyber Disclosure Report*, Willis N. Am. (Aug. 2014), *available at* http://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf.

[17] *Id.*

[18] *Id.*

[19] This is addressed in greater detail in a separate article published by the Center on Law & Security at New York University School of Law. Judith H. Germano & Zachary K. Goldman, After the Breach: Cybersecurity Liability Risk (2014), *available at* http://www.lawandsecurity.org/Portals/0/Documents/CLS%20After%20the%20Breach%20Final.pdf. This section is a condensed version of that article.

[20] Kentucky's law went into effect on July 14, 2014; the only states still without data breach notification laws are Alabama, New Mexico and South Dakota. *See, e.g.*, National Conference of State Legislatures, digest of security breach notification laws, April 4, 2014, *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[21] *See* Germano, Goldman, After the Breach: Cybersecurity Liability Risk, for specific examples and further discussion.

[22] *Hearing on Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland Before the Joint. Subcomm. of the H. Comm. on Homeland Security*, 113th Cong. (May 21, 2014) (prepared statement of Larry Zelvin, Director, National Cybersecurity Communications Integration Center), *available at* http://www.dhs.gov/news/2014/05/21/written-testimony-nppd-house-committee-homeland-security-joint-subcommittee-hearing.

[23] Indictment, *United States v. Dong et al.*, No. 14-CR-118 (W.D. Pa. May 1, 2014).

[24] *See generally*, Mark Landler & David E. Sanger, *Hacking Charges threaten Further Damage to Chinese-American Relations*, N.Y. Times (May 21, 2014), *available at* http://www.nytimes.com/2014/05/22/world/asia/hacking-charges-threaten-further-damage-to-chinese-american-relations.html.

[25] *US Is World's Leading Cyber Thief – Chinese Military*, BRICS Post (May 28, 2014, 11:35 AM), http://thebricspost.com/us-is-worlds-leading-cyber-thief-chinese-military/.

[26] *Id.*

[27] *See generally, The Surveillance Transparency Act of 2013: Hearing Before the S. Subcomm. on Privacy, Tech. and the Law of the S. Comm. on the Judiciary*, 113th Cong. (2013) (written testimony of Richard Salgado, Director, Law Enforcement and Information Security, Google, Inc.), http://www.judiciary.senate.gov/meetings/the-surveillance-transparency-act-of-2013 (highlighting the current distrust between the public, companies, and the government, and encouraging greater transparency).

[28] *See* Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos* (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?docid=152065& mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=116349.

[29] *See* Loek Essers, *Facebook Must Comply with German Data Protection Law, Court Rules*, P.C. World (Feb. 18, 2014, 4:05 AM), http://www.pcworld.com/article/2098720/facebook-must-comply-with-german-data-protection-law-court-rules.html.

[30] *See, e.g.*, Jerome Radcliffe, CyberLaw 101: A Primer on US Laws Related to Honeypot Deployments, SANS Inst., *available at* http://www.sans.org/reading-room/whitepapers/legal/cyberlaw-101-primer-laws-related-honeypot-deployments-1746.

[31] *See, e.g.*, Roger A. Grimes, *Beyond Honeypots: It Takes a Honeytoken to Catch A Thief*," InfoWorld (April 16, 2013), *available at* http://www.infoworld.com/d/security/beyond-honeypots-it-takes-honeytoken-catch-thief-216467?page=0,0.

[32] 18 U.S.C. § 1030.

[33] The legal analysis and arguments for and against affirmative defense (hacking-back techniques) are articulated in an enlightening online debate between Orin Kerr and Stewart Baker, set forth in a series of posts on The Volokh Conspiracy blog between October 13-17, 2012, the last two of which are available at http://www.volokh.com/2012/10/16/the-legality-of-counterhacking-bakers-last-post/, and http://www.volokh.com/2012/10/17/a-final-post-on-hacking-back/.

[34] *See id. See also, e.g., Alexei Alexis, Debate Brewing Over Whether Companies Should Strike Back at Their Cyber Attackers*, Bloomberg BNA (April 9, 2013), http://www.bna.com/debate-brewing-whether-n17179873246/.

[35] Nicole Perlroth, *In Cyberattacks on Banks, Evidence of a New Weapon*, N.Y. Times (Oct. 5, 2012, 8:30 PM), http://bits.blogs.nytimes.com/2012/10/05/in-cyberattacks-on-banks-evidence-of-a-new-weapon/.

[36] Joseph Menn, *Cyber Attacks Against Banks More Severe than Most Realize*, Reuters, May 18, 2013, *available at*

http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518.

[37] Ellen Nakashima, *U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks*, Wash. Post, April 11, 2014, *available at* http://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html.

[38] *Id*.

[39] *Id*.

[40] *See About the National Cybersecurity and Communications Integration Center*, U.S. Dep't of Homeland Sec., http://www.dhs.gov/about-national-cybersecurity-communications-integration-center (discussing NCCIC's role in coordinating information sharing between the public and private sectors).

[41] Fred Donovan, *FS-ISAC Threat Information Sharing Helped Thwart DDos Attacks Against US Banks*, FierceIT-Security (Nov. 14, 2013), *available at* http://www.fierceitsecurity.com/story/fs-isac-threat-information-sharing-helped-thwart-ddos-attacks-against-us-ba/2013-11-14.

[42] *About FS-ISAC*, Fin. Servs. Info. Sharing & Analysis Ctr., https://www.fsisac.com/about (last visited Aug. 26, 2014).

[43] Fran Berkman, *Nearly 100 Hackers Arrested in Global Blackshades Malware Sting*, The Daily Dot (May 19, 2014), http://www.dailydot.com/news/blackshades-malware-hackers-arrested-global-sting/; Aaron Katerksy, *Dozens of Arrests in 'Blackshades' Hacking Around the World*, ABC News (May 19, 2014), http://abcnews.go.com/ Blotter/dozens-arrests-blackshades-hacking-world/story?id=23778246.

[44] Evan Perez et al., *More than 90 People Nabbed in Global Hacker Crackdown*, CNN (May 19, 2014, 8:56 PM), http://www.cnn.com/2014/05/19/justice/us-global-hacker-crackdown/.

[45] Press Release, Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), *available at* http://www.justice.gov/usao/paw/news/2014/2014_june/2014_06_02_01.html.

[46] *Id*.

[47] Yamiche Alcindor, *Arrests Made in Global, $1.6M StubHub Cybertheft Case*, USA Today, July 23, 2014, *available at* http://www.usatoday.com/story/tech/2014/07/23/cyberthieves-stubhub-fraud/13036243/.

[48] Karen Freifeld, *Seven Arrests Made in $1.6 Million StubHub Cyberfraud Case*, Reuters, July 23, 2014, *available at* http://www.reuters.com/article/2014/07/23/us-usa-cybercrime-idUSKBN0FS09Q20140723.

[49] *National Cyber Investigative Joint Task Force*, FBI, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (last visited Aug. 25, 2014).

[50] *About DC3*, Def. Cyber Crime Ctr., http://www.dc3.mil/index/about-dc3 (last visited Aug. 24, 2014).

[51] *About Us*, U.S. Computer Emergency Readiness Team, http://www.us-cert.gov/about-us (last visited Aug. 25, 2014).

[52] *About the Computer Crime & Intellectual Property Section*, DOJ, http://www.justice.gov/criminal/cybercrime/ (last visited Aug. 25, 2014).

[53] *See, e.g.*, Mary Kathleen Flynn, *ISACs, Infragard, and ECTF: Safety in Numbers*, CSO Online, *available at* http://www.csoonline.com/article/2113264/security-leadership/isacs--infragard--and-ectf--safety-in-numbers.html.

[54] U.S. Dept. of Homeland Security, *Defending Against Cybercriminals* (Sept. 18, 2012), http://www.dhs.gov/defending-against-cybercriminals.

[55] *Id*.

[56] *See* Indictment, *United States v. Gonzalez* (D.N.J. Aug. 17, 2009) [hereinafter New Jersey Indictment], 2009 WL 2499004 (charges involving cyberattacks on Heartland Payment Systems, Inc.; 7-11, Inc.; and Hannaford Brothers Co.); Indictment, *United States v. Gonzalez* (D. Mass. Aug. 5, 2008), 2008 WL 2975802 (charges involving cyberattacks on BJ's Wholesale Club, DSW, OfficeMax,

Boston Market, Barnes & Noble, Sports Authority, and several TJX companies); Superseding Indictment, *United States v. Gonzalez* (E.D.N.Y. May 14, 2008), 2008 WL 3199939 (charges involving cyberattacks on Dave & Buster's, Inc.); *see also, e.g.*, James Verini, T*he Great Cyberheist*, N.Y. Times Mag., Nov. 10, 2010, http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html.

[57] *See* New Jersey Indictment, *supra* note 52, at ¶ 18 (describing the overt acts taken in furtherance of the cyberattack conspiracy).