NEW AMERICA

CYBERSECURITY INITIATIVE

ELANA BROITMAN

SMART CYBER-LEGISLATION

What Congress Can Do to Foster America's Cybersecurity

OCTOBER 2015

About The Author

Elana Broitman is a shareholder in Greenbert Traurig, LLP.'s Government Law & Policy Practice and a New America Cybersecurity Fellow. Previously she served as the Deputy Assistant Secretary of Manufacturing & Industrial Base Policy in the Department of Defense and as a Senior Advisor to Sen. Kirsten Gillibrand (D-N.Y.), having spent time in a technology company, with prior service as Counsel to the House Foreign Affairs Committee. Elana's current work focuses on cybersecurity, the defense industrial base, and foreign affiars. She is a graduate of Trinity University and the University of Texas School of Law. She speaks both Russian and German.

Acknowledgements

This paper is the second in a series written by the 2015-16 New America Cybersecurity Fellows. The New America Cybersecurity Fellowship is a non-resident fellowship that brings together individuals from different backgrounds and provides a platform for Fellows to fine tune and promote their big ideas for the present and future of cybersecurity.

A number of experts in government, associations, and companies provided invaluable insights for this document. In particular, the author would like to thank Matthew Eggers of the Chamber of Commerce, Tom Finan of the Department of Homeland Security, and Larry Clinton of the Internet Security Alliance.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About the Cybersecurity Initiative

The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security Program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work—for the countries, for companies and for individuals.

Find out more at **newamerica.org/cybersecurity-initiative**.

Contents

EXECUTIVE SUMMARY

Security issues stemming from connectivity are not diminishing—estimates forecast rising costs from data breaches and cyber crime—but security spending in the private sector has not kept pace with the rising costs. At the same time, Congress has worked to pass bills that would increase the cybersecurity of Americans and American businesses but, despite some significant steps, has failed to pass a comprehensive bill with broad authorities or requirements that would strengthen private sector cybersecurity. The 114th Congress has an opportunity to change this record by passing bills to provide liability protection and open the door to more information sharing and defensive measures. While these bills would support greater private sector cybersecurity, more incentives are needed to move the needle.

The question, then, is: what will make a significant difference? Cybersecurity insurance has made a resurgence in the minds of some in Washington, D.C. as the solution for private sector cybersecurity problems. While insurance is unlikely to ever deliver a silver bullet, it does have the potential to catalyze better cybersecurity practices in the private sector through positive incentives. Traditional insurance is not adequate to address cybersecurity, and the cybersecurity insurance market needs to grow significantly. Congress can pursue a cyber-legislative agenda in order to inject more life into this marketplace by increasing the effectiveness of the database of risks and tools, supporting a cyber incident reporting database, expanding programs that certify safety measures, and capping insurance costs in catastrophic circumstances.

> **There is often a lack of clarity about how to prioritize [the] gravest cyber threats and what effective and cost-effective cybersecurity measures to take.**

CYBERSECURITY COSTS GROW

For years, Congress has contemplated passing bills that would increase the cybersecurity of Americans and American businesses. Yet, despite some significant steps such as the Electronic Communications Privacy Act (ECPA), the Stored Communications Act, and the Federal Computer Fraud and Abuse Statute, which are mostly framed as exceptions to prohibited behavior, in multiple sessions Congress has failed to pass a comprehensive bill with broad authorities or requirements that would strengthen private sector cybersecurity.

It's not that cybersecurity problems are diminishing. Estimates are difficult due to a lack of good data and vary greatly—but any published number is enormous: from a forecast of the cost of data breaches to reach $2.1 trillion globally by 2019,[1] to an estimate that cybrecrime robs between $300 billion and $1 trillion from businesses worldwide each year.[2] The costs of the attacks, their frequency, and the cost of mitigating them is growing year over year,[A] yet security spending has not increased by commensurate measure.[B]

WHAT DRIVES CYBER HYGIENE?

The corporate sectors where the breadth and depth of cybersecurity precautions have taken lead include the financial, health care and defense sectors—areas where a cyber breach has particularly costly consequences, enormous reputational risk, and regulators have built requirements and incentives for extra cybersecurity.[C] For example, the Securities and Exchange Commission Office of Compliance Inspections and Examinations has cybersecurity examinations among its 2015 priorities.[3] Healthcare organizations are beholden to Health Insurance Portability and Accountability Act (HIPAA)

requirements, mandating database security. Under HIPAA, covered entities must have a contingency plan to protect data in case of an emergency and must create and maintain retrievable exact copies of electronic Protected Health Information.[4] And for the defense sector, the Department of Defense has for some time had a Defense Industrial Base Initiative, the DOD-Defense Industrial Base Collaborative Information Sharing Environment, pursuant to which significant defense companies have been incentivized and expected to implement higher security and data sharing standards. It is clear that some industries' regulators have stepped up cybersecurity requirements such that the cost associated with higher risk is clearly attributable.

For the other sectors that are not under higher levels of regulatory scrutiny, the cost-benefit equation has been less clear for corporate decision makers.

Although data breaches have made front-page news, the impact is diluted. For smaller and even mid-size companies without the internal departments to focus on cybersecurity, there is often a lack of clarity about how to prioritize their gravest cyber threats and what effective and cost-effective cybersecurity measures to take. Yet, these companies—no matter how small—are inter-connected with significant market players and critical infrastructure so that their lack of security creates a potentially significant risk for all.

One may surmise that increased cybersecurity imperatives simply means passing more regulations, but this has proven politically very difficult. So Congress has attempted to pass more benign legislation that would provide tools both the private sector and cybersecurity experts agree will support enhanced cybersecurity, such as greater information sharing.

CONGRESSIONAL MOTIVATION

Many members of Congress are concerned about the cyber threat, yet like many other bills (other than appropriations, which have to pass annually for the government to run) cybersecurity bills have been stuck in political gridlock.

But what has most stalled cybersecurity legislation have been philosophical debates and the absence of a simple policy solution that overcomes criticisms. A few years ago strong opposition from the U.S. Chamber of Commerce to mandates on the private sector pitted pro-business senators against cybersecurity hawks aiming for tough regulations during the debate on the Lieberman-Collins bill, S. 2105, The Cybersecurity Act of 2012.[D]

More recently, privacy concerns have aligned members along philosophical, rather than partisan lines. Since Edward Snowden's revelations about National Security Agency practices, libertarian Republicans, such as Sen. Rand Paul (R-Ky.), and liberal Democrats, such as Sen. Ron Wyden (D-Ore.), and many in the House have staunchly opposed cybersecurity measures that could provide a back door to the intelligence community or risk exposing individuals' personally-identifying information. Witness the May

2015 Senate battle over extension of USA Patriot Act provisions such as Section 215, which provided broad authority for government to access records. There was even difficulty of getting to cloture on the House passed USA Freedom Act; even though with this bill, the House limited the broad government surveillance authorities in the Patriot Act. Privacy hawks continued to oppose the government's ability to view private communications. This demonstrated that in crafting broad rules of the road, it is simply very difficult to draw such nuanced lines in legislation.

Finally the 2016 presidential election has thrown the usual wild card into the privacy debate as hopefuls such as Sens. Marco Rubio (R-Fla.) and Paul have staked out their positions. Paul's filibuster of renewal of the Patriot Act, in fact, can be interpreted as a public stake in the ground to boost his visibility on an issue that appears to be sensitive for voters.

Without an identified class of victims or physical evidence or catastrophic sense of harm, cyber risk does not become the proverbial kitchen table issue for voters. The media coverage tends to niche reporting or episodic major cyber breach stories such as Sony or Target (which led to the resignation of the Chief Executive Officer and a dramatic decline in revenue). This lack of "kitchen table" attention from voters means there is an absence of a strong demand signal for legislative action in a busy and increasingly partisan Congress.

114TH SESSION

This year, once again Congress is poised to pass legislation designed to enhance cybersecurity measures in the private sector. The question of whether it can get a bill to the President lies in the Senate,[E] since the House has passed both the Intelligence and Homeland Security cybersecurity bills and sent them to the Senate as a merged bill.[F] A few factors in this 114th Session of Congress have improved the chances for passage of a measure.

One, President Obama has moved some of the prior legislative cybersecurity issues off the table by issuing Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity (2013 EO)), and Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience).[5] The 2013 EO mandated the government to work with "owners and operators of critical infrastructure" to share information about cyber threats and attacks, leading a year later to the National Institute for Standards and Technology (NIST) issuing the framework for improving cybersecurity. PPD-21 focused on clarifying the US government agencies' responsibilities for cybersecurity, supporting information sharing by defining government's baseline cybersecurity needs, and establishing an analysis imperative in the federal government to support greater cybersecurity.

Two, all three bills in Congress provide the business sector with clearer information sharing authorities, protections from liability for such sharing, and

authorities for certain defensive cybersecurity measures—all items that the U.S. Chamber of Commerce and other business groups have strongly supported. Importantly the bills have stayed away from mandates. The Senate is more hawkish than either House bill, given that the House members with their shorter election cycles and retail politics are more sensitive to post-Snowden privacy concerns.

The key to passage now depends on how privacy and intelligence sharing concerns are handled, as that could cleave both parties along security versus privacy lines. Many predict that if leadership allows a cybersecurity bill to come to the floor, the compromise would take more of the House Homeland Security approach because it is the narrowest authority.

The next question is whether this legislation will make a marked difference in promoting private sector-led cybersecurity. The three key components of all three bills are a positive step in this direction: (1) authorization of information sharing; (2) authorization of defensive measures; and (3) liability protection.

> **The new bill's greatest impact for ISPs and cybersecurity consultants is in their authorization to share customers' information.**

Information Sharing

The current cybersecurity bills' explicit authorization to share cyber threat information and provide safe harbor from liability for sharing in good faith should reduce legal uncertainty and promote useful cybersecurity sharing. Such sharing in turn ought to promote better knowledge among companies of the current risks, actionable cybersecurity indicators such as signatures of hackers or malware, and the prevalent measures to take.

The ideas behind these authorities are valid. Clear authority to share one's own as well as customer data, upon their consent, is expected to remove gray legal areas particularly for Internet Service Providers (ISPs) and cybersecurity consultants that deal with customer data. Today, they must operate via a negative "authority" existing in exemptions to ECPA, necessitating counsel review.[6] ECPA prohibits communications providers from voluntarily disclosing transiting communications content with the exception of emergency situations or to protect their own networks. ECPA allows ISPs to "intercept, disclose, or use that communications ... which is necessary to the protection of the rights or property" of the ISP.[6] Sharing is not directly authorized by law, but is permitted as an exception to a prohibition, which has created uncertainty around the legality of sharing cyber threat information.

The new bills' greatest impact for ISPs and cybersecurity consultants is in their authorization to share customers' information. Under current law, ISPs may access and divulge the contents of a stored communication "with the lawful [and appropriately broadly enough crafted] consent of the originator or addressee or intended recipient of such communication or the subscriber in the case of a remote computing service" or as otherwise allowed by ECPA.[7] Such consent is often unclear or does not go far enough to address a particular unanticipated situation. The clarity provided by the cybersecurity bills in the 114th Congress will allow companies to act more swiftly in more cases.

Both the Senate and House permit information sharing of "cyber threat indicators." These are defined to include information that is necessary to describe or identify malicious reconnaissance, methods of defeating a security control or exploiting a security vulnerability, methods of causing legitimate users to unwittingly enable the defeat of such controls or exploit of a security vulnerability, malicious cyber commands, actual or potential harms, and any other attribute of a cybersecurity threat not otherwise prohibited. The language allows for content of communications to be shared in order to, for example, analyze the content of a spear fishing email and determine the "methods of causing legitimate users ... to unwittingly enable the defeat such controls or exploit of a security vulnerability." While this broad definition raises

concern for privacy advocates, all of the bills require entities to strip out personally identifiable information (PII) prior to sharing information.

Where the difference comes in is that the Senate essentially exerts a more permissive requirement on companies to strip out private information. The House's "reasonable standard" for companies evaluating which information is personally identifying and thus must be stripped prior to sharing is judged by the Senate majority as leaving companies exposed to litigation and jury decisions about the "reasonableness" of their judgments. The Senate, instead, requires stripping of PII "known at the time," which privacy experts and the White House see as opening the door to companies' inadequate protection of customer data.

The House language is also interpreted as requiring a more deliberative approach than the Senate to stripping PII prior to sharing across the government, while the Senate immediately contemplates an automated information sharing mechanism across the government. The Cyber Information Sharing Act (CISA) allows fairly automatic transmission from the Department of Homeland Security (DHS), which has a portal to receive the data, to share it with other government entities.[H] The Senate bill charges the Attorney General with establishing a process of safeguarding the data, without proscribing future methodologies in order not to hamstring the government into specific, easily out of date technologies. Privacy groups worry that automated processes without a minimum standard of review developed by Congress will not allow for adequate privacy review, resulting in law enforcement or intelligence agencies receiving private, personal information, possibly otherwise protected, that they can leverage for law enforcement purposes.

But, while all three bills authorize information sharing by the private sector with government and among private entities, the Senate and the House Intelligence bills allow the government to use shared information for far broader purposes, including law enforcement and economic espionage, while the House Homeland Security bill sticks to cybersecurity. This broader purpose is more troubling for privacy advocates.

House bills specifically exclude the Department of Defense (DOD), including the National Security Agency, in the information sharing authorities. This is clearly motivated by political sensitivities, yet does not appear to undermine DOD's ability to maintain the cybersecurity measures in place with the defense industrial base (DIB) companies that have long taken a more cybersecurity conscious approach.

Liability Protection

The liability protection offered by the three cybersecurity bills is likewise positive for industry, though unlikely to move the needle in terms of incentives. A December 2014 multi-industry letter led by the U.S. Chamber of Commerce states that "Businesses need practical safeguards to increase their information-sharing capabilities. CISA's narrow protections—including limited liability, disclosure, and antitrust provisions—would constructively influence businesses' decisions to share cyber threat data and countermeasures more quickly and frequently." The liability protection appears to

The liability protection offered by the three cybersecurity bills is likewise positive for industry, though unlikely to move the needle in terms of incentives.

potentially eliminate the need for extra consultation of counsel. But it is unlikely to eliminate lawsuits, a slew of which has threatened businesses.

With regard to antitrust in April 2014, the Justice Department and Federal Trade Commission released guidelines outlining its interpretation of lawful cyber threat information sharing under existing electronic communications statutes.[8] While designed to be helpful, it was seen by some counsel as still requiring interpretation, which may slow down sharing. Thus these bills further facilitate an environment conducive to sharing cyber threat data.

Again, the two Chambers have taken discrete approaches, with the House extending liability protection even for non-action on the basis of threat information. The purpose is to insulate companies from liability when they are unable to act because they are inundated by threat indicators. The White House, however, opposes this inclusion, and the Senate did not include this protection for the same reason—in order not to discourage companies from acting when threats arise. The final bill is likely to exclude this "non-action protection."

Defensive Measures

All three bills take the same approach to defensive measures—new authority to operate defensive measures on the entity's own system, the system of another upon written consent and federal entity's information system upon consent. There is an explicit prohibition on counter-measures or defensive measures that "destroy, render unusable, or substantially harm an information system or data on an information system not belonging to: the acting entity or the entity authorized to grant approval, which had done so." Just as with information sharing provisions, the authority to take defensive measures that protect one's own as well as customers' data can be important and allow companies to act more expeditiously than they would under current authorities "by exception."[I]

There continues to be a great reluctance to deputize the private sector in protecting itself to such an extent that it can become "offensive" and damage the systems of innocent actors, when for example, their systems are used simply for transit for a hack. Thus the bills do not provide liability protection for defensive measures. This is apparently a red line for the administration out of concern that companies could over-reach at a cost to customers' data.

Does current legislation go far enough to incentivize stronger cybersecurity protection?

Good cybersecurity practices have been driven by market pressures—when the cost of inaction is high, good cybersecurity attracts customers and business opportunities, or shields companies from losses. Such market dynamics have been hobbled by several challenges: (a) corporate leaders do not always know how to prioritize their cyber risks and thus determine which measures make the most sense; (b) legal uncertainty; and (c) the unpredictable cost of a potential attack weighed against the current and predictable cost of cyber hygiene.[J] The current bills, along with measures instituted by the DHS, the NIST Cybersecurity Framework, the DOD, and others pursuant to the President's EOs and Directives, provide industry with some of tools in response to the first two challenges.

But a number of industry experts contend these measures still may not move the needle far for non-critical sector, non-Fortune 500 enterprises, all of which nevertheless affect critical supply chains. And even for those that have taken precautions, the pace of change and innovation among hackers outpaces and raises costs of cyber hygiene.

The question becomes what could move the needle in fostering more companies to adopt good cyber hygiene. The White House had acknowledged in the past what we have observed over the last few years of attempts at cybersecurity legislation and executive orders—building market-based incentives is one of the most effective ways to promote cybersecurity. The challenge for Congress is how to use legislative measures, which are not nimble, to incentivize market forces. Insurance is one such an answer.

WHAT'S NEXT: INSURANCE

White House Cybersecurity Czar Michael Daniels explained that the 2013 EO was intended to support the insurance market, "to build underwriting practices that promote the adoption of cyber risk-reducing measures and risk-based pricing and foster a competitive cyber insurance market."[9]

Insurance has historically served as a lever of safety measures in many industries, from as early as shipping to the airline industry. Insurance makes firms more proactive about instituting safety measures, better protected, and more resilient to attacks. It rewards safety measures by offering lower insurance premiums and/or higher awards. Moreover, insurance is based on actuarial data demonstrating the effectiveness of cybersecurity measures and the likelihood that certain risks will occur, thus providing companies with an evidence-based way to prioritize their investment in cyber hygiene.[K] Insurance companies, handling a number of cyber incidents, develop a response protocol that supports companies' ability to respond to cyber attacks. Finally, insurance ought to protect the private sector from devastating harm.

Traditional insurance is not adequate to address cybersecurity. Sony's attempt to collect insurance payouts under its commercial general liability insurance after the cyber breach was denied, and finally settled out of court, has highlighted the need for specific cybersecurity insurance. In Sony's lawsuit against its insurer for coverage under its commercial general liability (CGL) policy, Justice Jeffrey K. Oing of the Supreme Court of the State of New York ruled that acts by third-party hackers do not constitute "oral or written publication in any manner of the material that violates a person's right of privacy" in the Coverage B (personal and advertising injury coverage) under the CGL policy issued by Zurich.[10]

> **Insurance makes firms more proactive about instituting safety measures, better protected, and more resilient to attacks**

Today many major commercial insurance companies offer some type of cybersecurity insurance in the United States. Nationally, businesses are expected to spend $2 billion on cyber-insurance premiums this year, a 67 percent increase from the $1.2 billion they spent in 2013, and just $600,000 in 2010, according to Betterley Risk Consultants.[11] But this is still a fraction of the $247 billion of direct premiums written for the total U.S. commercial lines insurance market in 2012.[12]

Even companies purchasing cybersecurity insurance may not obtain full protection. Cybersecurity insurance policies tend to cover the event response, liability protection, extortion and network interruption.[13] But in this relatively

immature market, insurance carriers are still refining their offerings and policies appear to differ greatly, making insurance decisions difficult for the companies' risk managers. Most policies remain far short of the full costs that can befall victim companies, including intellectual property theft, reputational damage, or the physical damage resulting from cyber incidents.

The picture is even less mature internationally. PWC's Insurance Banana Skins 2015 noted that cyber risk has for the first time entered the top ten list of concerns in a survey of the insurance industry covering 54 countries. Yet, cyber risk rises to top three in only a handful of active markets—the United States, Canada, United Kingdom and Ireland. Although the need for cybersecurity insurance is beginning to be recognized in Europe, the U.S. market is far ahead because demand is driven by the various states' data breach reporting requirements. While a few British cybersecurity insurance carriers appear to be extending the type of loss they cover, a recent report co-authored by the Marsh Insurance Company and the U.K. government, "UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk," "focuses on how insurance can help make UK companies more resilient to the cyber threat."[14] As the European Union works on the next version of data protection regulation, requirements for data breach notification are likely to drive the European insurance market just as similar state regulations in the United States have.

One obstacle is building of demand. While the risk of a cyber event is universal, less than half of the Fortune 500, and less than that in the middle/large companies buy any type of cybersecurity insurance.[15] This means the majority of U.S. businesses are not focusing on the costs of the cyber eventuality. Media coverage will drive public awareness. Congress can do its part with more hearings and speeches by members.

In supporting expansion of the cybersecurity insurance market, Congress can help by increasing the effectiveness of the database of tools and risks, supporting a cyber incident reporting database, expanding programs that certify safety measures, and capping insurance costs in catastrophic circumstances.

Effective Cybersecurity Databases

Congress can help ensure that public information about cyber risks and tools is detailed, supported by evidence and that companies' use of cybersecurity tools is appropriately incentivized.

Congress can help by increasing the effectiveness of the database of tools and risks, supporting a cyber incident reporting database, expanding programs that certify safety measures, and capping insurance costs in catastrophic circumstances

The NIST published the Cybersecurity Framework—a set of practices, standards, and guidelines that are common across critical infrastructure sectors, providing guidance for developing individual company cybersecurity measures.[16] The Framework, produced in collaboration with insurance and other industries, was a positive step. But it has not gone far enough to jump-start more comprehensive cybersecurity insurance coverage or even help most companies rate risks and cybersecurity tools, thus enabling better decision-making.

It is a menu of cybersecurity choices that does not provide data to allow measure of risk in different business sectors or anticipate the magnitude of the losses, particularly third party customer losses, reputational harm, and the potential aggregate cost of a single malware attack that impacts an entire sector. Insurers do not have enough actuarial data to adjust premiums based on effectiveness of security controls and products, according to Andrew Braunberg, research director at NSS Labs.[17] The Framework can certainly be leveraged to develop a robust set of cybersecurity guidelines, but doing so requires concerted effort as exhibited in the American Water Works Association's development of the Process Control System Security Guidance for the Water Sector utilizing the Cybersecurity Framework.[18]

Other less organized or proactive business sectors would benefit from a database measuring the effectiveness of cybersecurity tools: the costs of implementing them, analysis of risks based on sector-by-sector vulnerability, frequency of breach, and alignment of risks and the cybersecurity tools that work best to minimize them.[L] Greater awareness and ability to analyze risk would drive demand for cybersecurity coverage, which in turn would bring more insurance carriers and types of policies into the market.

Such information will come, for one thing, from increased cyber threat indicator sharing pursuant to the new legislation. DHS should publish the aggregate data and cross-reference it to the NIST Cybersecurity Framework in order to provide the empirical data that helps the private sector choose and invest. But we can and should go further—by beta testing the cybersecurity tools identified by the NIST Cybersecurity Framework, investing in research and development of cybersecurity measures, and testing the tools identified by companies sharing their information. Publishing this evidence of efficacy and cost-effectiveness will provide the data insurance providers need to build actuarial models that are fundamental to underwriting policies.

This is a role that government is best situated to play, as predicated in the 2013 EO:

> (b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations.
>
> To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.[19]

In addition to a robust cybersecurity database of tools, DHS has been leading an effort in collaboration with the insurance industry and other private sector actors to investigate the

benefits of a cyber threat indicator database, the Cyber Incident Data and Analysis Working Group (CIDAWG). The group has identified a number of benefits to the development of a robust cybersecurity insurance industry from anonymized sharing of cyber incidents, particularly if such a database can segregate reporting by sector, geography, association with certain annual events, and other factors that would help the insurance industry create strong and specific actuarial information and allow companies to judge their own cybersecurity in view of their peers.[20]

Congress has a clear role: ensuring that there are appropriate and sufficient resources for the research and development, testing, and aggregating and publishing of data. New appropriations, while welcome, are difficult to pass. Re-prioritizing and focusing available resources must also be considered.

Not only will this data enable insurance providers to broaden and deepen policy coverage, it will also guide companies that do not have the resources to research, develop, test, and analyze products themselves. Mandates are not acceptable to the private sector, but measurable indicators of efficacy provide a legitimate standard and help businesses understand which cybersecurity tools are cost effective and warrant investment.

Where cost of cybersecurity tools do not make sense under normal market conditions, Congress can create incentives. They can be tax breaks, procurement requirements or incentives, or regulatory and licensing advantages. For example, DOD issued a Defense Federal Acquisition Regulation to protect unclassified controlled technical information.[21] Other federal procurement models can similarly prioritize companies that implement cybersecurity tools, and a tested NIST Cybersecurity Framework would provide a generally accepted set of such cybersecurity tools among others. The insurance industry, in turn, can use this information to require or prioritize the cybersecurity practices rewarded by cheaper premiums or more comprehensive coverage. There is a long history of incentivizing business activity for the public good. Cybersecurity, with its lack of borders, distributed points of vulnerability and potential to infect many in the inter-connected marketplace, is a good candidate.

SAFETY Act Amendments

To further help the insurance industry develop the set of acceptable cybersecurity tools to require or promote through its policies, Congress can look to a post-9/11 law designed to foster development of anti-terrorism technology. The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) limits liability for a "qualified anti-terrorism technology'' used in an "act of terrorism.''[22] Congress passed the SAFETY Act in 2002 after learning that the threat of tort litigation was inhibiting the development and continued deployment of security products. Congress incentivized the deployment of effective and reliable security products and services through a liability management program under DHS. Importantly, customers of a SAFETY Act certified product are shielded from claims that the company's products failed to prevent an act of terrorism if an attack were to happen. And an applicant is required by the SAFETY Act to obtain liability insurance in the amount of the specified liability cap certified by the Secretary, thus spurring development of relevant insurance policies. The vast majority of the over 700 SAFETY Act awards have related to physical security products and systems.

In the 113th Congress, the House Homeland Security Committee reported out H.R. 3696, Rep. Michael McCaul's (R-Texas) bill that clarified that "act of terrorism'' as defined in the SAFETY Act includes "cybersecurity technology'' used in a "qualifying cyber incident.'' The intent of this clarification was to provide an incentive for companies to be innovative in developing methods and technologies for defending against, responding to, recovering from, mitigating, or otherwise combating cyber attacks, as well as to help ensure the widespread deployment of such items.

In May 2015 after thirteen years of the SAFETY

Act's existence, the DHS finally certified the first cybersecurity products: FireEye's Multi-Vector Virtual Execution engine and Dynamic Threat Intelligence cloud platform. While several SAFETY Act awards have previously gone to some cybersecurity- related products and services, the highest level of protection, a Certification, had not gone to a product designed purely for cybersecurity purposes until this year. The technology will be placed on an "approved products list" for Homeland Security.[23] This certification was a watershed moment as it is reportedly spurring the cybersecurity industry to seek SAFETY Act coverage. This in itself should spur innovation. Moreover given the SAFETY Act's requirement that certified products must be insured up to the level of the liability cap, greater use of the SAFETY Act should foster the insurance market.

> **Simply using the current law or amending it may not be enough. Congress can institutionalize the step taken by DHS this year by passing a version of the SAFETY Act that is tailored to cybersecurity.**

But simply using the current law or amending it may not be enough. Congress can institutionalize the step taken by DHS this year by passing a version of the SAFETY Act that is tailored to cybersecurity. Given the difficulty of attribution, such a cyber SAFETY Act version should not be based on a terrorism finding by the Secretary of Homeland Security, but rather on a federal certification based on the nature of the attack and the scale and type of damage. As currently required under the law the DHS Secretary must analyze several factors in finding a terrorist incident, including "to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions."[24] Cyber incidents' "instrumentalities" do not differ between criminal and terrorist or nation-state activities, however. In a SAFETY Cyber Act, it is more applicable if the Secretary simply certifies that certain sophisticated, large-scale attacks that cause mass destruction, injury or loss are covered, on the highly plausible theory that they are likely to be the result of governments or organizations motivated by geopolitical considerations, rather than only or simply crimes. The definitions will be difficult to negotiate, but such legislation will be more appropriate to the reality of cybersecurity than the policy crafted to address the issues faced almost fifteen years ago.

Cyber TRIA

Even as insurance providers need more information to measure risk and evaluate cyber safety measures—as a floor on which to build policies, the insurance industry is concerned that cyber attacks by nation-states or terrorist groups can cause catastrophic risk and damage that they cannot sustain. The catastrophic damage of 9/11 drove passage of The Terrorism Risk Insurance Act of 2002 (TRIA), which was re-authorized in January 2015.[M] Passing a Cyber TRIA offers an opportunity for Congress to take a similar step in the case of a catastrophic cyber event that could bring down a critical infrastructure sector, regardless of the origin of the attack.

According to the American Insurance Association, "TRIA is one of the nation's most effective public-private partnerships. Since it was first enacted a dozen years ago, the program has provided insurers the confidence they need to write terrorism risk insurance."[25] The law's legislative history explains that:

> TRIA… was enacted to address disruptions in the market for terrorism risk insurance, to help ensure the continued widespread availability and affordability of commercial property and casualty insurance for terrorism risk, and to allow for the private markets to stabilize and build insurance capacity to absorb any future losses for terrorism events.[N]

Typical cybersecurity insurance policies do not cover state sponsored or terrorism attacks. Most policies specifically exclude state-sponsored or terrorist cyberattacks.

> TRIA… requires insurers to "make available" terrorism risk insurance for commercial property and casualty losses resulting from certified acts of terrorism and provides for shared public and private compensation for such insured losses.[26]

When TRIA was being reauthorized, insurance industry representatives argued for an amendment to clarify that cyber terrorism would apply. An insurance industry representative participating in the President's Working Group on Financial Markets reasoned that clarity is needed regarding the application of TRIA to losses from cyber attacks.[27]

Typical cybersecurity insurance policies do not cover state sponsored or terrorism attacks. Most policies specifically exclude state-sponsored or terrorist cyberattacks.

> 'The damage is potentially so virulent and disruptive that these attacks amount to cyber warfare,' observed Eric Cernak, vice president and cyber product manager with The Hartford Steam Boiler Inspection and Insurance Co., a subsidiary of Munich Re. 'The insurance industry historically has seen war exposures as uninsurable because they create accumulation risks that are unlike anything else.' Accumulation refers to a combination of risks from a single event.

> 'No cyber policy has TRIA designation,' explained Heather A. Steinmiller, senior vice president and general counsel of insurance brokerage Conner Strong & Buckelew, noting 'TRIA provides backstop for reinsurance but requires insurance carriers to endorse certain policies.'[28]

As with the SAFETY Act, simply applying TRIA to a cyberattack may not be adequate. As previously stated, attribution is notoriously difficult, and often the hackers themselves are private individuals, whose direction by a government or affiliation with a terrorist group may be hard to prove. Certain types of targets, sophistication of attack and magnitude of damage are likely related to geopolitical considerations rather than simple crime. In these cases—if damage can be devastating enough—the insurance industry will be reluctant to repay without a federal backstop.

Thus Congress should consider modeling new legislation on the TRIA program, basing TRIA coverage on the particular characteristics of a cyber attacks rather than solely attribution. For example, where the damage is financially devastating, impacts a major segment of the nation's critical infrastructure, or the Director of National Intelligence identifies the attack as one by a state or terrorist group, the federal government would share in the cost alleviation with the insurance industry. Like TRIA, insurance providers would be compelled to include such coverage in its offering.

CONCLUSION

In the 114th session of Congress, we see an environment more conducive to passing cybersecurity legislation than ever before: the Office of Personnel and Management breach has magnified the significant costs of lax cybersecurity,[29] the recent Third Circuit decision that FTC can come after a company for lax cyber hygiene should drive proactive measures,[30] the president's executive orders have taken some of the previously divergent issues off the table, and both the House and Senate have passed similar companion bills. The information sharing, liability protection, and other sections of the bills are positive steps for incentivizing good cyber hygiene.

Fostering a strong and comprehensive cybersecurity insurance market would build on these measures to support market driven cyber hygiene.

Notes

A. According to PWC's The Global State of Cybersecurity Survey 2015, "the more than 9,700 security, IT, and business executives found that the total number of security incidents detected by respondents climbed to 42.8 million this year, an increase of 48 percent over 2013. That's the equivalent of 117,339 incoming attacks per day, every day." (See: "Managing cyber risks in an interconnected world." PWC. September 30, 2014. www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf) The data-breach firm Experian estimates the average costs for a breached company to total $9.4 million over a 24-month period.

B. The same PWC survey reports that "Despite elevated concerns, ...global [Internet Security] budgets actually decreased 4 percent compared with 2013. In fact, security spending as a percentage of IT budget has remained stalled at 4 percent or less for the past five years." According to the Internet Security Alliance, the manufacturing sector has been slow to take up cybersecurity investments. (See: John Wiegand, "Concerns over cyber security reach corporate boardrooms of Michigan manufacturers," MiBiz, June 21, 2015. mibiz.com/item/22630-concerns-over-cyber-security-reach-corporate-boardrooms-of-michigan-manufacturers). Moreover, cyber-insurance take up has not moved to the broader medium size market.

C. Cyber hygiene has been defined as "making sure we are protecting and maintaining systems and devices appropriately and using cyber security best practices for anything and everything that connects to the web. It includes organizing security in hardware, software and IT infrastructure, continuous network monitoring, and employee awareness and training. " See: "The Importance of Cyber Hygiene in Cyberspace," InfoSec Institute, April 30, 2015. resources.infosecinstitute.com/the-importance-of-cyber-hygiene-in-cyberspace

D. The initial version of the Lieberman-Collins bill mandated minimum security standards for critical infrastructure computer systems. Despite these being watered down to optional measures, the bill was defeated based on objections that it was too onerous for industry.

E. As of this publication, the Senate Select Intelligence Committee had passed S.754, the which has passed the Cybersecurity Information Sharing Act.

F. The bills–The Protecting Cyber Networks Act and the National Cybersecurity Protection Advancement Act—were merged as H.R. 1560 and passed the House as a single bill.

G. 18 USC 2702: ISP may not disclose customer content except with customer consent, necessary to protect ISP rights/property or to provide service, or to law enforcement if inadvertent to protecting against crime.

H. Both Chambers of Congress limit how this information should be shared—through a portal CISA charges DHS to create. This ought to limit inadvertent inappropriate transmission of privacy information, as well as help ensure coordination within the government.

I. "The issue of liability limitations has been discussed at length during the pendency of the cyber-security legislation. It obviously is an important issue for companies, and it needs to be resolved appropriately in order to encourage information sharing. With that said, having clearly defined limitations may help companies even more than having a 'notwithstanding any other law' blanket exception." Written Statement of Mary Ellen Callahan, Partner and Chair, Privacy and Information Governance Practice, Jenner & Block Former Chief Privacy Officer, U.S. Department of Homeland Security Before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, March 4, 2015.

J. A forthcoming New America report will focus on how these costs can be better predicted and quantified.

K. "A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of

self-protection." (See: "Cybersecurity Insurance," Department of Homeland Security, 2015 www.dhs.gov/cybersecurity-insurance

L. The Insurance Industry Working Group convened by DHS in July 2014 noted that "in the absence of more cyber risk actuarial data, carriers have struggled to estimate the probable first, second, and third-order effects of a cyber attack on critical infrastructure—key information they need in order to better determine the extent of first-party coverage they should offer and how to price it. Several participants suggested that developing and exercising new cyber incident models and simulations, with insurance industry input, would help carriers better understand the value of critical infrastructure and who might pay a premium to restore it. Specifically, they stated that such tools would help them understand: what cyber risks will implicate which infrastructure components; which components present the greatest concern from a business interruption perspective; what economic and other consequences might ensue without appropriate cyber risk controls in place; and which controls would likely have the greatest mitigation effect. While the participants stated that this information would be immediately helpful from an underwriting perspective, they emphasized that the development of parallel tools that help determine both the likelihood and the probable consequences of a cyber incident to a particular organization would resonate most with that organization's leadership. Such tools, they explained, would likely have the most success in driving more informed risk mitigation and risk transfer investments." See: "Insurance Industry Working Session Resdout Report—Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues," Department of Homeland Security, July 2014. www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf

M. Pre-TRIA, Congress had created other catastrophic insurance policies, including a "war damage" insurance program during World War II, insurance against aviation war risk, and federal riot reinsurance following large scale urban riots in the late 1960s. The government agreed to cover some percentage of an insurance company's losses above a certain deductible in exchange for a premium paid by that insurance company. See: Baird Webel, "Terrorism Risk Insurance: Issue Analysis and Overview of Current Program," Congressional Research Service, February 2013.

N. A Congressional Research Report states that "Since TRIA's passage, the private industry's willingness and ability to cover terrorism risk have increased. Prices for terrorism coverage have generally trended downward, and approximately 60 percent of commercial policyholders have purchased coverage over the past few years." See: Webel, Baird. 2013. See: Baird Webel, "Terrorism Risk Insurance: Issue Analysis and Overview of Current Program," Congressional Research Service, February 2013.

O. Insurance Workgroup participants discussed possible options to incentivize private carriers to extend cybersecurity insurance coverage to "cyber hurricanes" including by:

> Establishing a federal reinsurance entity – like the entity established under the Terrorism Risk Insurance Act (TRIA)
>
> Promoting the development of actuarial data that carriers will need to create new insurance products
>
> Passing a "Cyber Safety Act" – modeled on the SAFETY Act – to promote the development of (1) new cybersecurity- enhancing technologies and services; (2) insurance requirements for purchasers of those offerings; and (3) corresponding liability caps.

See: "Insurance Industry Working Session Resdout Report—Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues," Department of Homeland Security, July 2014. www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf

Sources

1 James Moar, "The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation," Juniper, May 12, 2015. www.juniperresearch.com/researchstore/strategy-competition/cybercrime-security/financial-corporate-threats-mitigation

2 Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of Cybercrime II," McAfee, June 2014. www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

3 U.S. Securities and Exchange Commission, "Priorities Focus on Protecting Retail Investors, Assessing Market-Wide Risks and Using Data Analytics," January 13, 2015. www.sec.gov/news/pressrelease/2015-3.html

4 Linda Saches, "The HIPPA Security Rule and the NIST Cybersecurity Framework." U.S. Department of Health and Human Services, September 23, 2014. csrc.nist.gov/news_events/hipaa-2014/presentations_day1/stine_hipaa_2014_day1.pdf

5 Office of the Press Secretary, "Executive Order—Improving Critical Infrastructure Cybersecurity," The White House, February 12, 2013. www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

6 18 USC 2511

7 18 USC 2702

8 Department of Justice and Federal Trade Commission, "Antitrust Policy Statement on Sharing of Cybersecurity Information," U.S. Department of Justice, April 10, 2014. www.justice.gov/atr/public/guidelines/305027.pdf

9 Michael Daniel, "Incentives to Support Adoption of the Cybersecurity Framework," The White House, August 6, 2013. www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework

10 Young Ha, "Sony, Zurich Reach Settlement in PlayStation Data Breach Case in New York," Insurance Journal, May 1, 2015. www.insurancejournal.com/news/east/2015/05/01/366600.htm

11 Abha Bhattarai, "Cyber-insurance becomes popular among smaller, mid-size businesses," The Washington Post, October 12, 2014 www.washingtonpost.com/business/capitalbusiness/cyber-insurance-becomes-popular-among-smaller-mid-size-businesses/2014/10/11/257e0d28-4e48-11e4-aa5e-7153e466a02d_story.html

12 President's Working Group On Financial Markets, "The Long-Term Availability and Affordability of Insurance for Terrorism Risk 2014," Coalition to Insure Against Terrorism, April 2014. www.insureagainstterrorism.org/PWGTRIAReport2014_FINAL.pdf

13 Vijay Basani, "Cybersecurity insurance – weighing the costs and the risks," MarketWatch, March 25, 2015.www.marketwatch.com/story/cybersecurity-insurance-weighing-the-costs-and-the-risks-2015-03-25

14 "The Role of Insurance in Managing and Mitigating the Risk," Marsh, March 23, 2015. www.marsh.com/content/dam/marsh/Documents/PDF/US-en/UK%20Cyber%20Security%20The%20Role%20of%20Insurance%20in%20Managing%20and%20Mitigating%20the%20Risk-03-2015.pdf

15 Mark Hollmer, "Treasury Troubled by Smaller Firms Not Buying Cyber Insurance," Insurance Journal, February 18, 2015. www.insurancejournal.com/news/national/2015/02/18/357713.htm

16 "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, February 12, 2014. www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

17 Lucian Constantin, "5 Things You Need to Know About Cybersecurity Insurance," CIO, April 25, 2014. www.cio.com/article/2376802/security0/5-things-you-need-to-know-about-cybersecurity-insurance.html

18 "Process Control System Security Guidance for the Water Sector." American Water Works

Association, 2014. www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf

19 Office of the Press Secretary, "Executive Order —Improving Critical Infrastructure Cybersecurity," The White House, February 12, 2013. www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

20 "Enhancing Resilience Through Cyber Incident data Sharing and Analysis," Department of Homeland Security, June 2015. www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015.pdf

21 4 C.F.R. 204, 212, and 252.

22 Subtitle G of the Homeland Security Act of 2002, Pub. L. 107-296,Sec. 202. SAFETY Act and qualifying cyber incidents.

23 Ashley Carman, "FireEye first cybersecurity firm awarded DHS SAFETY Act certification," SC Magazine. May 1, 2015. www.scmagazine.com/dhs-certifies-fireeye-products-under-safety-act/article/412563

24. "Frequently Asked Questions on General Safety Act Information," Homeland Security Science and Technology, 2002. www.safetyact.gov/jsp/faq/samsFAQSearch.do?action=SearchFAQForPublic

25 Leign Ann Pusey, "Time for House to pass the Terrorism Risk Insurance Act," The Hill, September 11, 2014. thehill.com/blogs/congress-blog/homeland-security/217342-time-for-house-to-pass-the-terrorism-risk-insurance-act

26 Federal Register, "Rules and Regulations," Government Publishing Office, February 6, 2015. www.gpo.gov/fdsys/pkg/FR-2015-02-06/pdf/2015-02556.pdf

27 President's Working Group On Financial Markets, "The Long-Term Availability and Affordability of Insurance for Terrorism Risk 2014," Coalition to Insure Against Terrorism, April 2014. www.insureagainstterrorism.org/PWGTRIAReport2014_FINAL.pdf

28 Gregory J Millman, "The Morning Risk Report: Cyberinsurance Little Help against Cyberterrorism." The Wall Street Journal, February 25, 2015. blogs.wsj.com/riskandcompliance/2015/02/25/the-morning-risk-report-cyberinsurance-little-help-against-cyberterrorism

29 David Perera and Joseph Marks, "Newly disclosed hack got 'crown jewels,'" Politico, June 12, 2015. www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954

30 United States Court of Appeals for the Third Circuit, "Federal Trade Commission v. Wyndham Worldwide Corporation," March 3, 2015. www2.ca3.uscourts.gov/opinarch/143514p.pdf