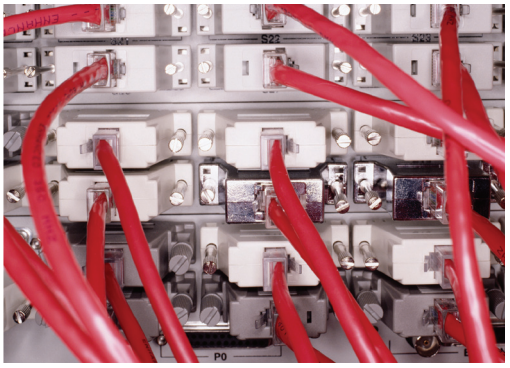
National Security Program

Homeland Security Project

Cyber Security Task Force:

Public-Private Information Sharing



July 2012

BIPARTISAN POLICY CENTER

DISCLAIMER

This report is the product of the Bipartisan Policy Center's Homeland Security Project. The findings and recommendations expressed herein are solely those of the Homeland Security Project and do not necessarily represent the views or opinions of the Bipartisan Policy Center, its founders or its board of directors.

Table of Contents

National Security Program
Homeland Security Project

Cyber Security Task Force

CO-CHAIRS

General (ret.) Michael Hayden
Former Director, CIA and NSA

Mortimer B. Zuckerman
CEO and Chairman of the Board of Directors, Boston Properties, Inc.

MEMBERS

Stewart Baker
Former Assistant Secretary for Policy, DHS

Bryan Cunningham
Former Deputy Legal Advisor to the National Security Advisor

Richard Falkenrath
Former NYPD Deputy Commissioner for Counterterrorism

Marcus Sachs
Vice President, National Security Policy, Verizon Communication

General (ret.) Ron Keys
Former Commander, Air Combat Command, U.S. Air Force

Benjamin Powell
Former General Counsel of the Office of the Director of National Intelligence

Jeffrey Rosen
Professor of Law at George Washington University

Frances Townsend
Former Homeland Security Advisor and Deputy National Security Advisor for Combating Terrorism

TASK FORCE DIRECTOR

Rob Strayer
Director, Homeland Security Project

National Security Program
Homeland Security Project

Chapter 1: A Time for Action

The attacks on information technology systems from a wide range of adversaries – including hacktivists, criminals, and nation-states – continue to grow.[1] From October 2011 through February 2012, over 50,000 cyber attacks on private and government networks were reported to the Department of Homeland Security (DHS), with 86 of those attacks taking place on critical infrastructure networks.[2] The incidents reported to DHS represent only a small fraction of cyber attacks carried out in the United States. The financial losses resulting from the theft of intellectual property and other sensitive information continue to increase dramatically, to say nothing of the loss of state secrets and damage to our national security.

Improvements in information sharing between the federal government and private sector about cyber threats and vulnerabilities show great promise for improving our cyber defenses and potential response measures. Public-private cyber information sharing can bolster and speed identification and detection of threats and will be critical to a coordinated response to a cyber incident. This type of information sharing can and must be done in a manner that protects privacy and civil liberties.

Despite general agreement that we need to do it, cyber information sharing is not meeting our needs today. The resolution of numerous legal impediments – some real, some perceived – is asserted by various stakeholders as a predicate to more robust cyber threat information sharing among private sector entities and between the private sector and the government. Perceptions of such impediments have created a collective action problem in which companies hold threat and vulnerability information close, rather than sharing it with each other or the government. Information that should be shared includes, but is not limited to, malware threat signatures, known malicious IP addresses, and immediate cyber attack incident details.

The public disclosure in April 2012 of attempted attacks against natural gas pipeline company systems provides an example of why this is necessary.[3] The coordinated attacks began in December 2011, but were not recognized and analyzed by DHS until March 2012.[4] In an era of light-speed attacks, that was far too long. Systems could have been disrupted or damaged long before other companies were aware of the attack vectors and possible remedial steps.

A more robust sharing of private and public network security information as well as threat information, in real time, would yield a level of situational awareness about the nation's information technology and communications systems that would enable operational and strategic decisions to be made about how to better protect them and respond to attackers. To be effective, such information sharing will require the automated exchange of data from computer to computer (so-called "machine-to-machine" sharing). While malware can be quarantined and communications with bad IP addresses blocked almost immediately after information on them is received, decisions about undertaking protective actions and active response measures often will require human evaluation of this data. This analysis turns data into intelligence. Both the government and private-sector companies need the capability to quickly be alerted, analyze data, develop courses of actions, and execute decisions, sometimes in the face of a rapidly changing threat.

Below, we outline a series of proposals that would enhance information sharing. Our recommendations have two major components: 1) mitigation of perceived legal impediments to information sharing, and 2) incentivizing private sector information sharing by alleviating statutory and regulatory obstacles. We begin with a description of information sharing today and then will explain how that framework must change.

Information Sharing Today

There are numerous sources of data about cyber threats and vulnerabilities. The government, commercial security service providers, Internet Service Providers (ISPs), non-profit groups, industry associations, and individual companies' networks can all be sources of information. Among other information, they provide threat signatures for malware, IP addresses and domain names involved in cyber attacks, and descriptions of particular cyber attacks. But this information sharing currently is far from comprehensive or sufficient, coming from only companies and organizations that choose to share cyber attack information. Many do not do so because of fears, some justified, including harm to their reputations and potential loss of customers.

Another chilling effect on sharing comes from the concern that private proprietary information compiled in government databases will be discoverable through Freedom of Information Act (FOIA) requests. Entities also are concerned that they may be held liable for the threat information they share if it turns out to be inaccurate. On the more technical side, another problem is that the data often arrives in the form of paper documents and email alerts that are not machine-readable or that must be acquired from website postings. This means that the information is not usable rapidly enough to prevent an attack or detect one that is ongoing.

In 2011, the Department of Defense (DoD) began testing an information-sharing program called the Defense Industrial Base (DIB) cyber security pilot program, intended to enhance the defensive capacity of its partners in private industry against cyber attacks.[5] Under the DIB pilot program, DoD provided classified malicious signatures that it had identified to industrial defense contractors, expanding their set of known threats. DoD disseminated the signature data by hard copy to defense contractors, who then entered the signature information into their systems manually, rather than through a secure method of automatic transfer.[6] The DIB pilot only involved a few dozen companies that met a set of security and operational requirements.[7]

DoD has released an interim rule that builds upon the DIB pilot and will establish an expanded cyber information-sharing program, allowing many more companies to participate.[8] Implementing a secure, automated method should increase the effectiveness of, and participation in, this program among private contractors.

The lessons learned from the DoD cyber pilot for establishing active and reliable methods of sharing threat data can be applied to other economic sectors as well. It is particularly important for companies in other sectors to establish such mechanisms because they typically are not cleared to receive and retain classified cyber threat data.

Reportedly, efforts are underway to automate more of the information sharing between the government and private sector. DHS is working with industry-led Information Sharing and Analysis Centers (ISACs) to achieve this goal.[9] (Originally sponsored by the government, but now operating independently of government funding or control, ISACs cover specific industry sectors, such as financial services and universities.) For years, ISACs have coordinated the sharing of terrorism and homeland security-related information with particular sectors. Some have now ventured into sharing cyber security threat information, but there are only a few industry sectors with ISACs active in cyber security and much work remains to be done to achieve automated sharing.

In addition to ISACs, DHS provides alerts through emails generally open to all subscribers. The problem with these types of alerts is that they often do not contain sufficient detail to be actionable. Such detail may be something that DHS and other federal agencies would be willing to share, but only with a limited number of trusted companies to

protect their source or method of acquiring the information. The federal government could also be criticized as showing favoritism to some if it did not provide the information to all in a transparent way.

Information Sharing in the Future

The government should empower cyber security officials to make judgments about which companies are likely to benefit from cyber intelligence, and be authorized to share information with these companies when circumstances warrant. Additionally, when less sensitive information is available, it should be shared as widely as possible across economic sectors.

The government should also attempt to tailor its information sharing and analyses to companies that have sought to share information with it. More specifically, a company that shares information with the government about a particular type of malware or intruder should receive the government's analysis about the attacker and methods, which could help the company to better protect its networks in the future. This intelligence might let a company know what type of data the attacker was seeking and might seek again. Federal law enforcement should also warn other key stakeholders in a particular economic sector about which they have emerging cyber threat information, even if other stakeholders may not be currently under the same type of attack. This type of tailored, more responsive sharing by the government will act as an incentive for companies to share with the government, even without a legal requirement to do so.

With more robust information sharing, there can be greater situational awareness about the health of the nation's information technology architecture. A real-time understanding of threats and vulnerabilities is necessary for government officials and industry leaders to make decisions about tactical protective and response measures. The real-time sharing of threatening IP addresses and other threat indicators can occur both through government-operated or private-sector aggregators of this information. In addition to our specific recommendations below, immediate enhancements of information sharing – within the private sector as well as between the government and private sector, to the greatest extent legally feasible – should not wait for new comprehensive legislation.

Protecting Privacy When Sharing Information

Enhanced cyber threat information sharing should be permitted only in environments utilizing currently available technological, administrative and physical protections for the security of shared information, particularly where such information is likely to include personally identifiable information (PII) or other potentially sensitive information. Currently available technology, procedures and best practices should be required for enhanced cyber threat information sharing including, but not limited to, privacy-enhancing technologies to support: 1) proportionality, which balances competing values by enabling sharing of all information reasonably necessary to accomplish the purpose of the sharing, but not more; 2) authorized uses of information and protections against repurposing; 3) differentiated access and selective revelation; 4) robust real-time and immutable auditing capabilities; and 5) effective oversight mechanisms.

While enhanced, and legally protected, cyber threat information sharing is necessary to meet the increasing threats to our critical infrastructure, it need not, and must not, come at the expense of Americans' privacy and civil liberties, particularly given the current availability of cost-effective technology to protect such information.

National Security Program
Homeland Security Project

Chapter 2: Mitigating Legal Impediments to Information Sharing

Protect Cyber Threat Information Provided to the Government

Corporations often are reluctant to share cyber vulnerability information with the government because they consider their system vulnerabilities to be sensitive information and do not want proprietary documents and information to be disclosed to the public and competitors. Stakeholders worry that such disclosures could result in reputational harm, competitive disadvantage, lost profits and shareholder derivative actions or other lawsuits. Information shared with the government could potentially be released through government employee error or as the result of a FOIA request. Companies also are concerned that an agency with regulatory authority over it could use information about a cyber incident to pursue enforcement or other unrelated regulatory action.

The Critical Infrastructure Information Act (CIIA) (section 211 of the Homeland Security Act)[10] provides a mechanism for the protection of sensitive cyber security information shared with DHS. Information protected under the CIIA cannot be disclosed to any other part of the government or under the authority of a FOIA request, except under very limited circumstances.

Currently, DHS signs Cooperative Research and Development Agreements (CRADAs)[11] with companies that are willing to share information with the government, thereby invoking the protections of the CIIA. These protections can be enhanced by amending the CIIA to clarify that cyber threat and vulnerability information submitted to the government cannot be disclosed without consent of the submitter. Its scope should also be expanded to cover such information provided by companies that are not necessarily owners or operators of critical infrastructure networks.

While it still may be necessary to sign agreements with individual companies that have particular concerns about the treatment of information that they share, to the extent practicable, DHS should standardize the agreements to limit lengthy negotiations over their provisions. The goal should be to establish an easily replicable framework for sharing (and protecting) information from thousands of companies.

Provide Liability Protection for Cyber Threat Information Clearinghouses that Gather the Information

Some industry ISACs have begun to serve as clearinghouses for information such as IP addresses and domain names that distribute malware or are destinations for packets sent by corrupted computers.[12] These ISACs collect information from sector industry members and share information among those members.

There are also for-profit and non-profit entities engaged in identifying and sharing such IP addresses and domain names. One of the more successful non-profit efforts is the Anti-Phishing Working Group (APWG)[13] that receives contributions from many different industry members and government entities (both domestic and foreign), including law enforcement. They are able to act as clearinghouse by consolidating malicious IP addresses and then providing them to all subscribers to a listserv with periodic updates. These mechanisms for sharing cyber security threat information are important and should be encouraged.

Unfortunately, entities that collect and aggregate cyber threat information have been threatened with lawsuits by owners of domain names and companies who host websites that are the sources of Botnet control servers or phishing attacks, but also host other websites that are innocuous. The ability of these entities to share information will be chilled if subject to lawsuits about the accuracy of their

data. To date, ISACs have only shared with members who they know and trust from their particular industry sectors, rather than distributing the information more broadly. The potential for lawsuits should not be an impediment to enhanced cyber threat information sharing.

To mitigate such fears, good faith actions of these sharing entities should be protected from litigation. In other words, if the sharing is not done with the intent to harm the owner of a domain name or IP address, there should be no basis for a lawsuit. These protections are particularly important as these entities act as clearinghouses for others' information based on cyber attacks occurring at light speed. To be useful, this information must be shared before the malware can be exploited against other victims. This requires real-time exchanges and potentially automated transfers of information. Network administrators should be empowered with such information and should determine how best it should be applied on their systems.

Nonetheless, innocent parties should have some type of recourse for erroneous inclusion on a list of nefarious actors. This is not a new concern, as current spam and malware block lists already have to account for false positives. For example, the Spamhaus Project, which manages complex anti-spam block lists, allows for user discretion in managing mail identified as spam,[14] and provides a means for users of tagged IP addresses and domains to request a prompt removal from Spamhaus block lists following an evaluation.[15] Clearinghouses should likewise establish mechanisms for reviewing inquiries by parties who claim to be innocent. The government could certify that such mechanisms are in place in order for the clearinghouse to receive limited immunity from lawsuits.

Amend Communications Laws to Clearly Authorize Communications Companies to Monitor and Intercept Malicious Internet Communications with the Consent of a Company or Customer and Share Related Information with the Federal Government, and to Provide Authority to Take Reasonable Actions During a Cyber Emergency Certified by the President

Real and perceived legal limitations in the Electronic Communications Privacy Act (ECPA), and the Wiretap Act that ECPA amended, have deterred communications providers from monitoring communications over their networks for cyber threats, which, in turn, has limited the sharing of details about such threats.[16] Both statutes include service provider exceptions where communications interception, disclosure, or use of communications necessary incident to rendition of service or to protect rights and property of the provider.[17] However, to qualify for the exception: 1) a communications provider must have reasonable cause to suspect its property rights are being violated; 2) there must be a substantial nexus between the device targeted for interception and the fraudulent activity; 3) the interception activity must be reasonable and narrowly tailored; and 4) the communications provider cannot be acting as law enforcement's agent.[18]

Many stakeholders believe that the law is not clear as to whether, and to what extent, meaningful network-wide or subscriber-specific cyber monitoring qualifies for the service-provider exception. Court decisions on this provision have not added clarity because they are dated and focused primarily on telephone companies with reasonable grounds to suspect a specific customer is bypassing billing

procedures or placing illegal calls.[19] The analogy for Internet communications would be one computer user's connection through an ISP. Thus, effective cyber threat monitoring could be found to be overly broad under the standard that courts have applied to telephonic communications in the limited number of prior rulings.

It is also unclear if an ISP that is monitoring communications for malware signatures would be protecting *its own* network and/or the networks of *end-users* that subscribe to its service if the malware would only present a threat to *end-user* computers. Presently, only the protection of the provider's own network would qualify for the exception, limiting the ability to monitor for malware signatures on other networks.

Revising Consent

There is also much legal uncertainty about the degree to which companies and individuals can consent to communications companies' monitoring for cyber threats. Relevant statutes should be amended to clarify that consent from an individual or company is sufficient for such monitoring, which can include consent by an information technology service on behalf of its users. Valid consent should allow communications companies to share cyber threat information with the federal government and other companies. The definition of entities covered by this consent exception should be clarified and expanded to cover all stakeholders, including information technology companies in a reasonable position to identify, and help thwart, significant cyber threats, beyond just ISPs.

Applicable federal law also should make clear that consent by one party to a communication is sufficient and that such consent overrides contrary state laws. Twelve states currently require that both parties to a communication consent to its interception.[20] These are explicitly preserved by the federal Wiretap Act, as amended by ECPA, which states that its consent exceptions are limited by state laws.[21] The effect of the "two party consent rule" is to give attackers a veto on whether their packets are inspected for malicious code.

The federal interest in identifying malicious Internet activity should no longer be undercut in this way by various state laws. A narrowly tailored preemption of state law to allow the federal government to improve cyber security is appropriate.

Sharing with the Government

Some companies take the position that under current law, sharing communications with the government cannot be done without a subpoena. With the right privacy and civil liberties protections in place, there is no valid reason for cyber threat information not to be shared with the federal government and a subpoena requirement can often thwart information sharing to identify and stop cyber attacks underway. The law should be changed to explicitly permit such sharing, without a subpoena, under conditions that protect privacy and civil liberties.

The administration's cyber security legislative proposal and several bills in Congress supported by members of both parties, including the Cyber Intelligence Sharing and Protection Act that passed the House, all authorize companies to share cyber threat and vulnerability information with the federal government without consent of the parties to the communication. While these measures provide some safeguards to protect privacy and civil liberties, the specific types of protections outlined above in section I.C should be required in any cyber threat information sharing program.

The administration's proposal would require private-sector businesses that want to share cyber information with the government to first make reasonable efforts to remove PII unrelated to cyber security threats.[22] It also would require federal government agencies to follow privacy and civil

liberties protection procedures, developed in consultation with privacy and civil liberties experts and with the approval of the attorney general.[23] Finally, the use, collection, retention and sharing of cyber information is limited to protecting against cyber security threats.[24] Information may be used or disclosed for criminal law enforcement only after the attorney general's review and approval of each such application.[25]

The leading bills in the Senate and House similarly create mechanisms for oversight of information-sharing procedures to protect privacy and civil liberties and have limitations on the use of the cyber threat information shared with the government. For example, CISPA requires annual reports from the intelligence community inspector general,[26] the Lieberman-Collins Cybersecurity Act requires an evaluation by the Privacy and Civil Liberties Oversight Board (PCLOB) and annual reports from chief privacy and civil liberties officers and relevant agency inspectors general,[27] and the McCain SECURE IT Act requires biennial evaluation from the PCLOB and the agency or department heads overseeing cyber security centers[28] and annual reports from agency inspectors general.[29]

While the exact terms of these protections vary among the bills, a vigorous dialogue in Congress should be able to resolve differences among them. The critical point of agreement is that the restrictions in ECPA and other laws should not prohibit monitoring of network traffic and the sharing of information about cyber threats and vulnerabilities that is essential to protecting the nation's IT networks. In addition to embracing the privacy and civil liberties protections outlined above, any privacy guidelines required by statute should have deadlines that ensure their timely adoption or for the government to issue interim guidelines if the process of adopting comprehensive guidance is delayed.

Cyber Security Emergency

Cyber attacks have the potential to cause catastrophic losses of life and property. We should plan for these crises in advance to mitigate their effects. Moreover, the very act of showing that we are prepared to detect, mitigate and respond will provide some level of deterrence to many of those who would launch such attacks. In fact, many cyber strategists now believe that network *resilience*, as opposed to the traditional concept of *retaliation*, offers the best hope for cyber deterrence. Also important, authorities and response options that are carefully thought out and legislated prior to an attack will likely be more effective, prudent, and privacy-protective than on-the-fly reactions to a catastrophic attack already underway.

Legislation should provide that the president may certify to Congress that an emergency exists from an ongoing cyber attack or national security threat. This certification would trigger specific authorities to mandate that reasonable countermeasures be taken by companies that generate, store, route, or distribute online information and by other appropriate private-sector companies, which would be protected from liability for actions that are consistent with government instructions. Following a presidential certification, relevant companies that handle online information should have enhanced authority to access, review and share network traffic and related information in order to identify the threat and take responsive action in coordination with the federal government.

Congress and – to the extent possible – the public should be notified of the certification and actions taken. Such authorization should be limited in duration and subject to timely and reasonable oversight mechanisms, including for appropriate minimization procedures and tailoring of responsive actions.

While the president has substantial inherent authority under the Constitution to take actions in defense of the nation, Congress should clarify the authority of the president to allow, or even require, the private sector to undertake measures necessary to protect the nation from a cyber emergency.

Enhance Sharing of Threat Information With Critical Infrastructure Owners and Operators

Many critical infrastructure owners and operators currently do not have access to classified information to prevent a cyber attack because they lack clearances. While defense contractors have many employees with clearances, electricity generation and transmission companies, for example, often have few, if any, cleared personnel. In one industry sector that is generally regarded as proactive in adopting cyber security information sharing, we learned that only a small percentage of companies had any employees with the highest levels of security clearance.

Moreover, having employees at a sufficient level in the corporate hierarchy with clearances is important when decisions may affect a company's profitability. Therefore, not only do chief security officers at companies need clearances, but senior corporate officers need clearances and access to classified information in order to make decisions about how to respond to evolving cyber threats.

Congress should require the lead agency for each critical infrastructure sector to identify the companies in the sector that provide essential services that could be disrupted by a cyber attack and require them to identify the key decision makers within those companies who need access to classified threat information. The director of national intelligence should then establish a process to facilitate expedited clearances for qualified individuals.

In amending the clearance process related to cyber security, it is reasonable for the government to recognize that there are risks faced by sharing classified information with companies that have business relationships with companies the government does not trust, making it possible that classified information could be compromised. Therefore, in some cases, a clearance should not be provided to an individual at a company who would otherwise qualify for one. Such limitations make it all the more important for the government to carefully consider what information it can declassify for broad dissemination.

In addition to improving the clearance process, the government should seek to provide as much unclassified technical details about cyber threats that are needed by system administrators, who do not have clearances, to protect their networks. In many cases, technical details that would assist in protecting networks need not include "sources and methods" information. While the classified information may be relevant to senior corporate decision makers in making larger policy judgments, it may not be necessary in many cases to support basic protective measures. Often, there is delay when cleared company officials receive classified threat information and then have to request that the intelligence community declassify the technical details so that the information can be used to implement protective measures. It would save time, and likely thwart more cyber incidents, if the information was provided up front, ideally through automated systems.

National Security Program
Homeland Security Project

Chapter 3: Streamlining Data Breach Notifications

State Data Breach Laws

State data breach notification laws have served two useful purposes: 1) notifying consumers whose data may be at risk for misuse; and 2) providing an incentive for companies to improve data security protections to avoid costly notification requirements and lawsuits. However, the current patchwork of often inconsistent state laws makes compliance difficult and costly. This is made complex by having to provide a notification to each customer that complies with the law in the customer's state. Moreover, companies may be devoting too many resources to avoiding data breach liability when they should be addressing cyber threats more broadly and consistently.[30]

Streamlining and unifying the data breach notification requirements that currently exist in state laws under a national standard, while eliminating punitive lawsuits, would reduce the costs for companies to comply with these breach notification laws and make companies less worried about sharing attack incident details with the government. Even under streamlined federal breach notification requirements, consumers would be protected when breaches occur that present a credible risk of personal data being misused.

Federal Trade Commission (FTC) Authority

Some companies are reluctant to disclose information about data breaches to the federal government for fear of an FTC enforcement action. Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[31] This prohibition includes deceptive statements and unfair practices involving the use or protection of PII. Security breaches can be enforced under either the deceptiveness or unfairness prongs.

FTC Enforcement Actions

The FTC brings enforcement actions against companies for deceptive practices if they mislead consumers about how their data will be protected and used. For example, the FTC brought an enforcement action against Ceridian Corporation, a human resources services company, after hackers gained access to the company's network and compromised the PII of approximately 28,000 customers.[32] The FTC alleged that the privacy and information security representations on Ceridian's website were deceptive, because Ceridian touted a "Worry-free Safety & Reliability" security system while failing to take reasonable security measures.[33]

The FTC brings enforcement actions against companies for unfair practices that lack adequate security, even if they do not make false representations. For example, the FTC has brought enforcement actions against companies that fail to: 1) encrypt sensitive personal data,[34] 2) employ reasonable precautions when sharing data with a third party,[35] or 3) use necessary security protocols against reasonably anticipated cyber attacks.[36]

An FTC enforcement action following a security breach is very costly for companies. From beginning to end, the investigation and enforcement action can take over two years and cost millions of dollars in legal and consulting fees.[37] Further, the FTC often imposes obligations on the company that last decades into the future.

Administration Proposal

As part of its cyber security legislation, the Obama administration has proposed a data breach reporting

policy that includes a safe harbor measure,[38] which would preempt state disclosure laws in order to streamline breach reporting based on a national standard.[39] Under the administration's proposal, companies suffering a data breach would be exempt from public notification if a risk assessment conducted shortly after the breach finds that the information accessed is sufficiently encrypted to prevent any reasonable risk of misuse.[40] The company must also report these findings to the FTC for review.[41]

Our Proposal

Congress should preempt state breach notification laws and federal unfair trade practice enforcement actions and streamline notifications under a federal standard. It should also provide a safe harbor for companies when there is no actual risk of consumers having their data misused. This regime would help to encourage sharing with the government by reducing the risk that sharing about incidents would result in violations of data breach and unfair trade practice laws.

Recommendations

Our recommendations for securing public-private information sharing include the following:

- Protect cyber threat information provided to the government.
- Establish mechanisms to protect privacy and civil liberties for information shared with the government.
- Provide liability protections for cyber threat information clearinghouses that collect and disseminate cyber threat and vulnerability information.
- Amend communications laws to clearly authorize communications companies to monitor and intercept malicious Internet communications with the consent of a company or customer, and share related information with the federal government.
- Legislation should provide that the president may certify to Congress that an emergency exists from an ongoing cyber attack or national security threat. This certification would trigger specific authorities to mandate that reasonable countermeasures be taken by companies that generate, store, route or distribute online information and by other appropriate private-sector companies, which would be protected from liability for actions that are consistent with government instructions.
- Require the government to push technical cyber threat data, which can be used to protect networks, to the private sector in an unclassified format.
- Require the government to work with critical infrastructure companies to identify key personnel who should receive clearance to review cyber threat and vulnerability information.
- Streamline data breach notification requirements to incidents where there is a credible risk of harm to consumers and establish a “safe harbor” policy that would exempt a company from state data breach notification laws and federal unfair trade practice enforcement actions following a security breach.

National Security Program
Homeland Security Project

Endnotes

1. We would like to acknowledge and thank BPC research assistant, David Beardwood, and the students in the Georgetown University Law School Federal Legislation and Administrative Law Clinic – Jason Crawford, Rebecca Givner-Forbes, Jonathan Miller, Brittany Muetzel, Aarthy Thamodaran, Jacob Wolf, Amanda Blunt, Eric Bolinder, Christopher Lamar, Katrine Lazar, Leah Schloss, and David Silvers – for the valuable legal research they provided for this report.
2. Schmidt, Michael. "New Interest in Hacking as Threat to Security." *The New York Times*, March 13, 2012. http://www.nytimes.com/2012/03/14/us/new-interest-in-hacking-as-threat-to-us-security.html?_r=2&ref=fb
3. Clayton, Mark. "Alert: Major Cyber Attack Aimed at Natural Gas Pipeline Companies." *The Christian Science Monitor*, May 5, 2012. http://www.csmonitor.com/USA/2012/0505/Alert-Major-cyber-attack-aimed-at-natural-gas-pipeline-companies
4. U.S. Dept. of Homeland Security. "Gas Pipeline Cyber Intrusion Campaign." *ICS-CERT Monthly Monitor*, April 2012. http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf
5. U.S. Dept. of Defense. "DIB CS/IA Program." Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program. http://dibnet.dod.mil/staticweb/index.html
6. Nakashima, Ellen. "Cyber Defense Effort is Mixed, Study Finds." *The Washington Post*, January 12, 2012. http://www.washingtonpost.com/world/national-security/cyber-defense-effort-is-mixed-study-finds/2012/01/11/gIQAAu0YtP_story.html
7. U.S. Dept. of Defense. "Minimum Requirements." Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program. http://dibnet.dod.mil/staticweb/MinReqmts.html
8. U.S. Dept. of Defense. "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities." *Federal Register*, Vol, 77, No. 92. May 11, 2012. Rules and Regulations. Pp. 27615. http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf
9. National Council of ISACs. http://www.isaccouncil.org/
10. 6 U.S.C. Part B § 131-134– Critical Infrastructure Information. http://www.law.cornell.edu/uscode/text/6/chapter-1/subchapter-II/part-B
11. U.S. Dept. of Homeland Security. "Technology Transfer Mechanisms." http://www.dhs.gov/xabout/structure/gc_1264625623653.shtm
12. Some companies have raised concerns about potential violations of antitrust laws as a reason for not sharing cyber information with other private sector entities. The Department of Justice should outline a safe harbor for cyber information clearinghouses, providing the assurance that participation in them will not lead to prosecution under antitrust laws.
13. Anti-Phishing Working Group (APWG). http://www.antiphishing.org/
14. "Understanding DNSBL Filtering." White paper. The Spamhaus Project. http://www.spamhaus.org/whitepapers/dnsbl_function/
15. "Blocklist Removal Center." Webpage. The Spamhaus Project. http://www.spamhaus.org/lookup/
16. Electronic Communications Privacy Act, 18 U.S.C. 119 §2510-2522. http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119
17. 18 U.S.C. § 2511(2)(a)(i), 18 U.S.C. § 2702(b)(4) and (c)(3) (emphasis added).
18. See, e.g., *United States v. McLaren*, 957 F. Supp. 215, 218-19 (M.D. Fla. 1997).
19. See, e.g., *McLaren*, 957 F. Supp. at 220, *United States v. Clegg*, 509 F.2d 605, 612 (5th Cir. 1975).
20. The states with "two party consent" are California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania and Washington.
21. 18 U.S.C. 119 §2510-2522. http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119
22. Department of Homeland Security Cybersecurity Authority and Information Sharing Act of 2011 § 248(a)(2) http://democrats.senate.gov/pdfs/WH-cyber-general-authorities.pdf
23. Ibid. § 248
24. Ibid. § 244(b)
25. Ibid. § 244(b)(3)
26. H.R. 3523 (RFS) § 1104(e)
27. S. 2105 (PCS) § 242, 704(g)(5-6)
28. S. 2151 (IS) 104(a)
29. Ibid. § 3554(a)(4)
30. Forty-six states and the District of Columbia have data breach notification and disclosure laws. The states without these laws are Alabama, Kentucky, New Mexico and South Dakota. *See, State Security Breach Notification Laws*. National Conference of State Legislatures. Available at http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.
    State laws vary across the following dimensions: 1) kinds of personally identifiable information (PII) that trigger notification requirements; 2) time in which notification is required; 3) how certain a company must be that PII was breached; 4) content of the breach notice; 5) method of notice; 6) whether notice must be given to parties other than affected customers; and 7) method of enforcement.
    E.g., North Dakota requires breach notification if customers' names are released in combination with a date of birth, mother's maiden name, or electronic signature. ND Cent. Code § 51-31-01; *E.g.*, FL Stat. § 817.5681 (requiring notification to affected Florida residents within 45 days of discovering a breach, and imposing a fine up to $500,000 for failure to disclose within that time frame); CT Gen. Stat. Ann. § 36a-701b (requiring notice within 15 days of discovery of a breach). Other states require notification without "unreasonable delay." *E.g.*, 815 IL Com. Stat. 530/5. Some states require notification if a company is "reasonably certain" a customer has been affected by the breach. However, different states have interpreted this threshold differently. MAKING SENSE OF THE PATCHWORK OF STATE SECURITY BREACH NOTIFICATION STATUTES, *supra*.
    Some states do not specify the content of notice, but others do. *E.g.*, HI Rev. Stat. § 487N-1 (requiring a description of the incident in general terms, the type of personal information that was acquired, acts taken to protect information from being further compromised, telephone number to contact for more information about the breach, and advice to remain vigilant in reviewing account statements and monitoring credit reports); MD Code § 14-3501 (requiring notice to include, among other things, telephone numbers for credit reporting agencies, the Federal Trade Commission, and the Maryland Attorney General).
    Most states allow for notice by telephone, writing or email. MAKING SENSE OF THE PATCHWORK OF STATE SECURITY BREACH NOTIFICATION STATUTES, *supra* note 7. Some require the customer's consent to send notice via email. *E.g.*, FL Stat. Ann. § 817.5681. Some states allow only for written or email notice. *E.g.*, DC Code § 28-3851.
    E.g., CO Rev. Stat § 6-1-716 (notice required to credit reporting agencies if number of affected customers exceeds 1,000); DE Code Ann. tit. 6 § 12B-101 *et seq.* (requiring notice to Consumer Protection Division of the Delaware Department of Justice).
    E.g., CT Gen. Stat. Ann. § 36a-701(b) (providing for enforcement by attorney general only); CA Civ. Code § 1798.82 (providing a private right of action for individuals harmed by a business's failure to comply with the notification statute).

31. 15 U.S.C. § 45 (2006).
32. “In the Matter of Ceridian Corporation.” FTC File No.1023160 (2011).
33. Ibid.
34. “In the Matter of BJ’s Wholesale Club, Inc.” FTC File No. 0423160 (2005) (finding that the failure to encrypt personal data on BJ’s computer networks was an unfair practice).
35. Kennedy, John B. ”A Primer on Key Information Security Laws in the United States.” PLI Pat., Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. 14648161-62 (2008).
36. “In the Matter of ACRAnet, Inc.” FTC File No. 0923088 (2011).
37. ”Surviving an FTC Investigation After a Data Breach.” 1048 PLI/Pat 467, 473.
38. Data Breach Notification § 102(b) http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification.pdf
39. § 109
40. § 102(b)(1)(A)
41. § 102(b)(1)(B)

Founded in 2007 by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole and George Mitchell, the Bipartisan Policy Center (BPC) is a non-profit organization that drives principled solutions through rigorous analysis, reasoned negotiation and respectful dialogue. With projects in multiple issue areas, BPC combines politically balanced policymaking with strong, proactive advocacy and outreach.

BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000
Washington, DC 20005
(202) 204-2400

WWW.BIPARTISANPOLICY.ORG