Congressional Research Service
Informing the legislative debate since 1914

Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis

N. Eric Weiss
Specialist in Financial Economics

June 3, 2015

Congressional Research Service
7-5700
www.crs.gov
R43821

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Data breaches, such as those at Target, Home Depot, Neiman Marcus, JPMorgan Chase, and Anthem, have affected financial records of tens of millions of households and seem to occur regularly. Companies typically respond by trying to increase their cybersecurity, hiring consultants, and purchasing new hardware and software. Policy analysts have suggested that sharing information about these breaches could be an effective and inexpensive part of improving cybersecurity. Firms share information directly on an ad hoc basis and through private-sector, nonprofit organizations, such as Information Sharing and Analysis Centers (ISACs) that can analyze and disseminate information.

Firms sometimes do not share information because of perceived legal risks, such as violating privacy or antitrust laws, and economic incentives, such as giving information that will benefit their competitors. A firm that has been attacked might prefer to keep such information private out of a worry that its sales or stock price will fall. Further, there are no existing mechanisms to reward firms for sharing information. Their competitors can take advantage of the information, but not contribute in turn. This lack of reciprocity, called "free riding" by economists, may discourage firms from sharing. Information that is shared may not be applicable to those receiving it, or it might be difficult to apply.

Because firms are reluctant to share information, other firms suffer from vulnerabilities that could be corrected. Further, by not sharing information about effective cybersecurity products and techniques, the size and quality of the market for cybersecurity products suffer.

Some industry leaders call for mandatory sharing of information concerning attacks. Other experts advocate a strictly voluntary approach, because they believe it could impose fewer regulatory costs on businesses and cost less for taxpayers.

A number of bills designed to encourage cybersecurity information sharing have been introduced in the 114th Congress, including H.R. 1560, Protecting Cyber Networks Act; H.R. 1731, National Cybersecurity Protection Advancement Act of 2015; and S. 754, Cybersecurity Information Sharing Act of 2015 (CISA). In April 2015, the House passed both H.R. 1560 and H.R. 1731, and it combined them into H.R. 1560 with the original H.R. 1560 as Title I and H.R. 1731 as Title II. On March 17, 2015, the Senate Select Committee on Intelligence reported out S. 754.

Contents

Figures

Contacts

Introduction

Cybercrime continues to increase. The media reports data breaches exposing tens of millions of personal financial records at retailers, such as Target, Home Depot, and TJ Maxx. The Ponemon Institute, an independent research institute, estimates that in 2013 the number of attacks on 59 companies based in the United States increased over that of 2012 and the average cost per attack also increased.[1] The Ponemon study found the average cost of a cybercrime incident in FY2014 was $12.7 million compared with $11.6 million in FY2013.

The Center for Strategic and International Studies estimates that cybercrime costs the global economy about $445 billion in a typical year.[2] The risks to critical infrastructure and national security from cyberattacks are harder to quantify, but the Bipartisan Policy Center recently concluded that the United States has a "September 10th ability to guard against cyberattacks."[3] President Obama and some Members of Congress have identified increasing cybersecurity as a priority.[4]

It would seem that companies could increase their cybersecurity at relatively little cost by sharing information about cyberattacks. The costs of a data breach can include detection, containment, repair, incident response, investigation, fraud losses, and lost sales. The cost of sharing information, including joining a specialized sharing organization, is likely to be less than $100,000.[5]

One obstacle to reducing cybercrime is misaligned incentives, which reduce information sharing about cyberattacks. In the aftermath of a cyberattack, at least four groups could be notified: law enforcement, other companies, customers, and (for public companies) stockholders. In addition, certain regulated companies, such as banks and electrical utilities, could be required to notify their regulators of cyberattacks.

If companies notify law enforcement—typically either the Federal Bureau of Investigation (FBI) or the Secret Service—they do so in the hope that those responsible will be brought to justice and that some sort of recovery can be made. They notify other companies in the hope that greater information sharing will improve security. Customers are notified so that they can monitor their financial information to prevent financial fraud. The Securities and Exchange Commission (SEC)

[1] Ponemon Institute, *2014 Cost of Cyber Crime Study: United States*, October 2014, https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5208enw.pdf. The Ponemon report looks at the average cost of cybercrime per incident for 59 companies, not the total cost in the United States.

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

[3] Bipartisan Policy Center, *Reflections on the Tenth Anniversary of the 9/11 Commission Report*, Washington, DC, July 2014, p. 7, http://bipartisanpolicy.org/sites/default/files/files/%20BPC%209-11%20Commission.pdf. The reference to September 10th is a comparison to the relative lack of airplane security that existed prior to the September 11, 2001 attacks on the World Trade Centers and the Pentagon.

[4] See, for example, U.S. Senate Committee on Homeland Security and Governmental Affairs, "Senator Carper Introduces Bill to Increase Sharing of Cyber Threat Data," press release, February 11, 2015, http://www.hsgac.senate.gov/media/minority-media/senator-carper-introduces-bill-to-increase-sharing-of-cyber-threat-data.

[5] Financial Services ISAC, *Membership Benefits,* https://www.fsisac.com/join.

requires publicly traded companies to announce information that could affect investors' decisions to invest in a company.

This report analyzes information sharing by government with private companies, by private companies with the government, and among private companies. Sharing information with consumers is mentioned but is not the central focus of this report.

A Cybersecurity Problem: Misaligned Incentives

Understanding the economic incentives involved in cybersecurity and information sharing can improve the analysis of cybersecurity.

Companies that suffer a cybersecurity breach such as the theft of credit card information do not pay the full cost of the breach. Retailers honoring stolen credit cards have charges reversed (so-called chargebacks) and end up without merchandise or payment. Credit card issuers say that they are not fully compensated for replacing stolen cards.[6] Consumers must monitor their financial accounts and update automated bill payment accounts to guard against cyberattacks.[7]

Meanwhile, software companies frequently weigh the benefits of delays to improve security against the costs of late releases.[8] According to some industry observers, software developers can be under pressure to "ship early, ship often" and fix security and other bugs in a later iteration.[9] Similarly, companies may act in ways that they believe will preserve or increase their market share or profitability even at the expense of cybersecurity.

The Problem of Underused Information

Many in the cybersecurity field have suggested increasing cybersecurity information sharing between individuals, companies, nongovernmental organizations, and governments as a way to increase security.

Many kinds of information can be shared to improve cybersecurity. This can include sharing ways to detect specific attacks and more general information about hardware, software, and procedures. It can include specific and general information about recovering from a data breach. The cost of sharing is relatively small, but the benefits can be large. Michael Daniel, the White House cybersecurity coordinator, described information sharing as "critical to effective cybersecurity," and legislation was introduced in 112th and 113th Congresses to promote information sharing.[10]

---

[6] Nicholas Ballasy, "Home Depot Breach Costs CUs $60 M," *Credit Union Times*, October 30, 2014, http://www.cutimes.com/2014/10/30/home-depot-breach-costs-cus-60m.

[7] Tyler Moore and Ross Anderson, *Economics and Internet Security: a Survey of Recent Analytical, Empirical, and Behavioral Research*, Computer Science Group, Harvard University, 2011, p. 1, ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf.

[8] Ross Anderson, "Why Information Security Is Hard—An Economic Perspective," 17th Annual Computer Security Applications Conference, December 10, 2001, http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf.

[9] Andrew Leonard, "Triumph of the Free-Software Will," *Salon*, October 31, 2000, http://www.salon.com/2000/10/31/software_passion/.

[10] For details, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current* (continued...)

One kind of information sharing occurs when organizations learn from third parties (such as law enforcement) that information has been compromised.[11] For example, the Secret Service reportedly notified Target[12] and Home Depot[13] that their data systems had been breached.

Information sharing can also flow in the other direction: According to media reports, JPMorgan discovered that it had cybersecurity problems and asked the FBI for assistance.[14]

Sharing information has benefits. If a firm reports a cyberattack, law enforcement can begin searching for those responsible and possibly alert other organizations, which can review their cybersecurity arrangements to prevent similar attacks.

In some cases, broader sharing of information would benefit the attacked firm; if it does not have the resources for defense or other countermeasures, sharing information might allow another entity, such as a security consultant or the software developer, to develop a countermeasure. But sharing cybersecurity information with a competitor can give away security lessons that were learned at great expense. Moreover, some may fear that publicly revealing a cyber breach can scare customers away to competitors leading to reduced revenue and possibly stock price declines. In other words, the hacked company's competitors might benefit from the information or its revenue or stock price might decline.[15]

In 47 states and the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, companies can be required to notify consumers if personally identifiable information (PII) is breached.[16]

(...continued)

Laws, and Proposed Legislation, by Eric A. Fischer.

[11] Ellen Nakashima, "U.S. Notified 3,000 Companies in 2013 about Cyberattacks," *Washington Post*, March 24, 2014, http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html.

[12] Matt Townsend, Lindsey Rupp, and Lauren Coleman-Lochner, "U.S. Secret Service Probes Card Security Breach at Target," *Bloomberg*, December 19, 2013, http://www.bloomberg.com/news/2013-12-19/u-s-secret-service-investigating-card-security-breach-at-target.html.

[13] Mark Hosenball and Nandita Bose, "UPDATE 3: Home Depot in Contact with Secret Service over Alleged Breach—Source," September 4, 2014, http://www.reuters.com/article/2014/09/04/usa-homedepot-dataprotection-idUSL1N0R517720140904.

[14] Michael Corkery, Jessica Silver-Greenberg, and David E. Sanger, "Obama Had Security Fears on JPMorgan Data Breach," *New York Times*, October 8, 2014, http://dealbook.nytimes.com/2014/10/08/cyberattack-on-jpmorgan-raises-alarms-at-white-house-and-on-wall-street/.

[15] Academic research suggests that cybersecurity breaches depress stock prices. See, for example, Griselda Sinanaj and Jan Muntermann, "Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis," 26th Bled e Conference, Bled, Slovenia, June 2013, https://domino.fov.uni-mb.si/proceedings.nsf/Proceedings/820BFAD242085887C1257B8A002F0B02/$File/07_Sinanaj.pdf; and Edward A. Morse, Vasant Raval, and John R. Wingender Jr., "Market Price Effects of Data Security Breaches," *Information Security Journal: A Global Perspective*, vol. 20, no. 6 (November 11, 2011), pp. 263-273. For a contrary view by reporters, see Sarah Halzack, "Home Depot and JPMorgan Are Doing Fine. Is It a Sign We're Numb to Data Breaches?" *Washington Post*, October 6, 2012, http://www.washingtonpost.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/.

[16] The definition of PII and the thresholds for consumer notification vary by state. For more information on state laws, see CRS Report R42475, *Data Security Breach Notification Laws*, by Gina Stevens. PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. For more on PII, see Erika McCallister, Tim Grance, and Karen Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of (continued...)

Typically, consumers are notified of the breach, advised to monitor financial accounts closely, and sometimes offered free credit monitoring or other assistance.[17] Some, including the chief information officer of the retailer Urban Outfitters, have argued that public disclosure can tip off attackers or waste time if information is breached but not stolen.[18]

Industry participants and outside observers appear to generally agree that there is less than optimal information sharing about attacks.[19] Although the amount of harm caused by inadequate information sharing is hard to measure, and increasing information sharing can be difficult, it has at times increased security. By contrast, while the broad outline of the Target credit card hack[20] had been widely discussed, Home Depot was the victim of a similar attack through a vendor whose security had been compromised.[21]

Information sharing would appear to be a relatively inexpensive way for a group of companies to improve their cybersecurity, but a review of recent data breaches shows that most of the details about breaches are released by third party experts, not the firms involved. The next section analyzes some of the reasons for this apparent reticence by firms.

Perceived Legal Barriers to Information Sharing

Firms and industry groups have expressed reluctance to share information in part because doing so might violate privacy or antitrust laws.[22] Another concern is exposing proprietary business information.[23]

To help assuage these fears, the Department of Justice (DOJ) has provided guidance that it will not consider generally accepted cybersecurity information sharing to be anticompetitive behavior.[24] Some cybersecurity experts, industry participants, and several Members of Congress

(...continued)

the National Institute of Standards and Technology," U.S. Department of Commerce, National Institute of Standards and Technology, April 2010, p. 2-1, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. See, also, National Council of State Legislatures, "Security Breach Notification Laws," September 3, 2014, http:// http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[17] For example, see Home Depot's recent data breach announcement. Home Depot, "The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores: Provides Further Investigation Details, Updates Outlook," press release, September 18, 2014, https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.

[18] Danny Yadron, "Executives Rethink Merits of Going Public with Data Breaches," *Wall Street Journal*, August 4, 2013, http://online.wsj.com/articles/a-contrarian-view-on-data-breaches-1407194237?mod=mktw.

[19] Ray Suarez, "Examining Cyber Security with Homeland Security Secretary Janet Napolitano," *PBS NewsHour*, February 15, 2013, http://www.pbs.org/newshour/bb/science-jan-june13-cybersecurity_02-15/.

[20] For more information about the Target data breach, see CRS Report R43496, *The Target and Other Financial Data Breaches: Frequently Asked Questions*, by N. Eric Weiss and Rena S. Miller.

[21] Jeffrey Roman, "Home Depot, Target: Same Breach Script," *Bank Info Security*, November 10, 2014, http://www.bankinfosecurity.com/home-depot-target-same-breach-script-a-7544/op-1.

[22] Securities Industry and Financial Markets Association, "Principles for Effective Cybersecurity Regulatory Guidance," press release, October 20, 2014, http://www.sifma.org/issues/item.aspx?id=8589951691.

[23] For more information, see CRS Legal Sidebar WSLG483, Obstacles to Private Sector Cyber Threat Information Sharing, by Edward C. Liu.

[24] Department of Justice, "Department of Justice, Federal Trade Commission Issue Antitrust Policy Statement on Sharing Cybersecurity Information," press release, April 10, 2014, http://www.justice.gov/opa/pr/justice-department-(continued...)

remain concerned that firms are holding back information that could make cyberspace more secure.[25]

Economic Incentives to Not Share Information

In theory, sharing information about cybersecurity attacks and defenses has many benefits:

- Everyone would appear to benefit from eliminating duplication of costs and efforts.
- Sharing efforts could detect breaches faster and reduce damage caused by breaches.
- Sharing breach information and joint research efforts could lead to new ways to protect information.

In practice, there are also other considerations:

- Some argue that, despite official pronouncements, there are unresolved legal questions concerning privacy and antitrust issues surrounding sharing cybersecurity information.
- Some organizations may be reluctant to help competitors and, in extreme cases, might listen to what others share but offer nothing in return (free-riding in economic terms).
- If the shared information itself is breached by hackers, the organizations could be worse off than if they had not shared the information.
- Public disclosure of a breach may cost an organization customers and sales and affect its stock price.

Although there is some evidence that such fears have been exaggerated, evidence also suggests that they may be the primary factors preventing firms from sharing cybersecurity information.[26]

Comparing Target's stock price to those of three competitors—Walmart, Best Buy, and Costco—from the day before Target's data breach was first revealed on December 18, 2013, to three months afterwards, its stock price increased 19%. In the same time period, Costco's stock price increased 9%, while Walmart's declined 3% and Best Buy's declined 22%.

The Information Sharing and Analysis Center (ISAC) Council emphasized to the Government Accountability Office (GAO) that "the benefits of sharing information are often difficult to

(...continued)

federal-trade-commission-issue-antitrust-policy-statement-sharing.

[25] Office of Management and Budget, "Statement of Administration Policy, H.R. 624—Cyber Intelligence Sharing and Protection Act," April 16, 2013, http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf.

[26] See Alessandro Acquisti, Allan Friedman, and Rahul Telang, "Is There a Cost to Privacy Breaches? An Event Study," presented at the Workshop on the Economics of Information Security 2006, http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf; and Ali Alper Yayla and Qing Hu, "The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors," *Journal of Information Technology*, vol. 26, no. 1 (May 4, 2010), http://www.palgrave-journals.com/jit/journal/v26/n1/abs/jit20104a.html.

discern, while the risks and costs of sharing are direct and foreseeable."[27] A survey of information technology executives found that their chief worry about data breaches was the loss in consumer confidence and resultant decline in revenue, not the losses directly caused by the breach.[28]

Analysis of Firms' Incentives to Share

To understand why companies may not share cybersecurity information, some theoretical scenarios applying basic game theory are examined.

New Threats

Consider a firm that recognizes a new threat or a new (to it, at least) instance of a known threat, one to which its competitors are also potentially vulnerable. There are several possible outcomes depending on the characteristics of the threat and the firms.

If the threat to its profits is small, the firm may or may not choose to develop a countermeasure or share information about the threat, depending on its evaluation of potential reputational benefits for altruistically sharing the information. Some cyberattacks can be viewed as a cost of doing business, much like shoplifting is.

If the threat is significant, the firm may try to develop a custom countermeasure (for instance, hiring a security consultant to create a defense involving new procedures, software, or hardware). If the firm is unable to obtain a countermeasure, it may or may not have financial incentives to share information about the threat, depending on the possibility of another organization developing a countermeasure. Even if the firm believes that developing a countermeasure is unlikely or impossible, there might not be sufficient incentives to share the information compared with the advantages of not sharing with competitors.

Industries making similar products and using similar technologies can benefit more from information sharing, but as they are also more likely to be competitive, they may be less likely to share information.[29] Stronger industry associations could arguably counteract this effect.

Developing and Sharing Countermeasures

If the threat is more general, a firm that develops a countermeasure must decide whether it is better off with the competitive advantage that it now has against selling or giving away the countermeasure. Some firms, such as many in the defense industrial base, also sell cybersecurity services and could decide to sell it, while others, such as those in water treatment, might not be in a position to.

---

[27] U.S. Government Accountability Office, "Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors," July 2004, pp. 9-10, http://www.gao.gov/products/GAO-04-780.

[28] Esther Gal-Or and Anindya Ghose, "The Economic Incentives for Sharing Security Information," *Information Systems Research*, vol. 16, no. 2 (June 2005), p. 187, http://pages.stern.nyu.edu/~aghose/ISR.pdf.

[29] For more on the effects of product similarity, see Esther Gal-Or and Anindya Ghose, "The Economic Incentives for Sharing Security Information," *Information Systems Research*, vol. 16, no. 2 (June 2005), p. 187, http://pages.stern.nyu.edu/~aghose/ISR.pdf.

So Why Do Some Firms Share Information?

In most of the scenarios above, organizations might decide not to share information lest they diminish their competitive advantage. So why do organizations sometimes choose to share information?

One reason, as discussed above, may be that the threat is small and the firm wants to cultivate a reputation as a good corporate citizen. The legal requirement to maximize shareholder value does not translate into employing any means necessary to increase the stock price. Cybersecurity is arguably integral to national security and economic growth, and people may choose to share information even when it goes against the balance of their near-term economic incentive to foster a more secure nation and a more productive economy.

Role of Consultants and Insurance Companies in Information Sharing

When an organization calls in outside experts to help after a data breach, these consultants use their accumulated knowledge to investigate, document, and remediate the breach. The contract terms are negotiated between the two parties and generally not disclosed to the public. Following general practices, it is likely that the outside experts agree not to disclose proprietary information. Nevertheless, the consultants leave with knowledge about the data breach, and this information can be used in consulting with other companies.

Following existing practices for property and casualty insurance, companies writing cyberinsurance are likely to assess the cybersecurity practices of a (potential) client. Following a data breach claim, a cyberinsurance company would be likely to conduct or monitor a third-party investigation of the breach. Thus, cyberinsurance companies could gather detailed, technical information on breaches and use this knowledge to prevent future breaches at other clients.

How Can Organizations Share Information?

This section analyzes how organizations share information and legislation that was introduced in the 113th Congress to encourage information sharing.

Categories of Information

Organizations primarily share information about new types of threats, new instances of known threats, and best practices. Information about the effects of an attack can also be shared, even if the method of attack is unknown—for example, by notifying other firms that information has been stolen or that a resource is not operational.

Methods of Information Sharing

Certain types of information can be shared automatically to maximize its value. For instance, when some antivirus software detects malware, it automatically notifies the software vendor, which can analyze the information and update the antivirus software.

Prior to Target's 2013 data breach, which led to the theft of more than 40 million payment card details, Target had recently installed a security system to isolate new malware before it could damage the real system. This software reportedly includes the option to delete malware automatically, but according to a media investigation, "Target's security team turned that function off."[30] The report quoted a chief information security officer of another company who described the choice as normal, because "typically, as a security team, you want to have that last decision point of 'what do I do.'"

Machine autonomy has its issues. Machines generally are not as skilled as individuals in identifying proprietary or PII that should not be shared. Attackers could subvert autonomous information sharing software to further spread their reach or put their attacks on a list of approved programs (a "whitelist"). For effective machine-to-machine sharing to occur, firms need to have high levels of trust with each other and share technical expertise.

Public and Private Sector Information Sharing

Information can be shared within the private sector, within the public sector, and between the two. Government contractors may be subject to more stringent information sharing and disclosure requirements depending on the nature of the work and what department they are working with: the Department of Defense (DOD), for example, requires contractors to report potential exfiltration of classified information.[31] A subset of the private sector, the critical infrastructure industries, operates slightly differently than the rest by relying heavily on Information Sharing and Analysis Centers (ISACs).

ISACs

In 1998, Presidential Decision Directive 63, on critical infrastructure protection, authorized the creation of ISACs and critical infrastructure sector coordinators to assist in their creation.[32]

ISACs are private-sector, nonprofit entities that collect, analyze, and share information on cybersecurity threats and best practices.[33] Some, such as the Defense Industrial Base ISAC and the Oil and Natural Gas ISAC, have mechanisms to share information anonymously between members and with the government. The government also uses ISACs as a tool to communicate with sectors rapidly, particularly in emergency situations. The government also runs some ISAC-like entities, such as the Financial Sector Cyber Intelligence Group.[34]

---

[30] Michael Riley et al., "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *Bloomberg Businessweek*, March 13, 2014, http://www.businessweek.com/printer/articles/189573-missed-alarms-and-40-million-stolen-credit-card-numbers-how-target-blew-it.

[31] Jon W. Burd, "Cybersecurity Developments: Does the NIST "Voluntary" Framework Portend New Requirements for Contractors," Wiley Rein LLP, 2013, http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=3&id=9264.

[32] The critical sectors are chemicals, communications, commercial facilities, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government, healthcare and public health, information technology, nuclear, transportation, and water and waste water. For more information, see National Telecommunications and Information Administration, "Presidential Decision Directive 63 on Critical Infrastructure Protection," 63 *Federal Register* 41804-41806, August 5, 1998.

[33] ISAC Council, "Government–Private Sector Relations," January 31, 2004, http://www.isaccouncil.org/images/Government_Private_Sector_Relations_013104.pdf.

[34] Zachary Goldfarb and Ellen Nakashima, "Lew Says Financial Industry Could Do More to Prevent Cyberattacks," (continued...)

Sectors outside of critical infrastructure have also created ISACs, such as the Retail ISAC. Additionally, the Food ISAC, though classified as a critical infrastructure sector by the DHS, ceased operating due to a lack of information sharing.[35]

The Multi-State ISAC includes all 50 states, four U.S. territories, the District of Columbia, and many local governments. The electricity sector ISAC, run by the North American Electric Reliability Corporation, counts virtually all registered electricity providers as members.

Although the ISACs are sector specific, the multifaceted nature of modern corporations means that these boundaries are not always clear. For example, because the retailer Target owns a bank, the company became the first retailer to join the Financial Services ISAC (FS-ISAC).[36]

Membership in ISACs is voluntary, and levels of participation in ISACs vary. As shown in **Figure 1** and **Figure 2**, the FS-ISAC offers membership tiers ranging from free (with limited benefits) to platinum (with full benefits) and costing $49,950 annually.

This has not equalized the participation rates among firms with varying levels of resources. New York State found that 60% of large banking organizations and 25% of small organizations were members of the FS-ISAC.[37] Nonetheless, the FS-ISAC has helped its members combat cybersecurity issues such as denial-of-service attacks.[38]

Although cybersecurity is important to the information technology industry, the IT-ISAC has 33 members. Many large cybersecurity vendors—such as Symantec, FireEye, and DocuSign—are members but many of the biggest companies in IT, including Google, Mozilla, Adobe, Apple, and Facebook, are not.[39] However, IT-ISAC shares information with other organizations, such as the IT Sector Coordinating Council, which has a broader membership to include, through other alliances, companies, such as Google and Facebook.[40]

Generally, ISACs cannot prevent free-riding. If a company joins, there is usually no mechanism preventing it from receiving information even if it does not contribute information of its own. Free-riding has the potential to discourage information sharing. If a sharer consistently contributes without receiving information in return, it may decide that it is helping its competitors more than it is benefitting from sharing.

(...continued)

Washington Post, July 16, 2014, http://www.washingtonpost.com/business/economy/lew-says-financial-industry-could-do-more-to-prevent-cyberattacks/2014/07/16/6909e970-0d22-11e4-8341-b8072b1e7348_story.html.

[35] Joseph Straw, "Food Sector Abandons Its ISAC," *Security Management*, http://www.securitymanagement.com/article/food-sector-abandons-its-isac-004590.

[36] CRS Report R43496, *The Target and Other Financial Data Breaches: Frequently Asked Questions*, by N. Eric Weiss and Rena S. Miller.

[37] New York State Department of Financial Services, *Report on Cyber Security in the Banking Sector*, May 2014, p. 4, http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf.

[38] The White House, "Getting Serious about Information Sharing for Cybersecurity," April 10, 2014, http://www.whitehouse.gov/blog/2014/04/10/getting-serious-about-information-sharing-cybersecurity.

[39] IT-ISAC, *Members*, August 7 2014, http://www.it-isac.org/#!members/c1tsl.

[40] Letter from Brian Willis, president, IT-ISAC, to Dr. Melissa Hathaway, acting senior director for cyberspace, NSC, February 27, 2009, http://www.whitehouse.gov/files/documents/cyber/Willis%20Brian%20-%20IT%20ISAC%20Final%20Letter%20to%20Dr%20Hathaway.pdf.

Figure 1. Financial Services ISAC Membership Tiers

Compare FS-ISAC Membership Benefits	CNOP Free Join Now	Basic $250.00/yr Join Now
Limited Critical Notifications	✓	✓
CINS Crisis Notifications		✓
24x7 Access to Watch Desk		✓
Cyber/Physical Alerts from Govt, Partners, other ISACs		✓
Cyber/Physical Alerts from Members		✓
Anonymous Submissions		✓
Portal Access Credentials		✓
Document Repository		✓
Member Contact Directory		✓
Risk Mitigation Toolkit		✓
Threat Viewpoints		✓
Daily Report		✓
Monthly Cyber Security Tip Newsletter		✓
Participate in Community Institution Council Teleconferences		✓
Participate in Payment Risk Council Teleconferences		✓
Conduct Member Surveys		✓
Complimentary Webinars		✓
Invitation to Semi-Annual Meetings		✓
Complimentary Regional Workshops		✓
Inclusion in Threat Exercises		✓
Meets Regulatory Compliance Requirement		✓

Source: Financial Services ISAC, *Membership Benefits*, https://www.fsisac.com/join.

Figure 2. Financial Services ISAC Membership Tiers (Continued)

	Core	Standard	Premier	Gold	Platinum
Financial Institutions, Insurance Companies and Publicly Held Securities/Brokerage Firms	Assets: $1B - $10B	Assets: $10B - $20B	Assets: $20B - $100B	Assets: $100B - $250B	Assets: > $250B
Processors, Utilities and Privately Held Stand Alone Securities Firms*	Revenue: < $100M	Revenue: $100M - $1B	Revenue: $1B - $2.5B	Revenue: $2.5B - $5B	Revenue: > $5B

Protect your firm and valued customers while taking an active role in safeguarding our country's critical infrastructure. Join your peers by becoming a member of FS-ISAC. For more information, please email our Marketing Department, or contact us at **877-612-2622**, prompt 3.

Compare FS-ISAC Membership Benefits Click to Expand/Collapse all	Core $850.00/yr Join Now	Standard $5,000.00/yr Join Now	Premier $10,000.00/yr Join Now	Gold $24,950.00/yr Join Now	Platinum $49,950.00/yr Join Now
+ User Access Credentials	4	10	25	50	Unlimited
+ CINS Crisis Notifications	✓	✓	✓	✓	✓
+ Government, Member, and Partner Alerts	✓	✓	✓	✓	✓
+ Customized Email Notification Profile	✓	✓	✓	✓	✓
+ 24 x 7 Watch Desk	✓	✓	✓	✓	✓
+ Member Submissions	✓	✓	✓	✓	✓
+ Member Surveys	✓	✓	✓	✓	✓
+ Industry Best Practices	✓	✓	✓	✓	✓
+ Member Contact Directory	✓	✓	✓	✓	✓
+ Threat Conference Calls		✓	✓	✓	✓
+ Trusted Email Registry		✓	✓	✓	✓
+ FS-ISAC Committees/Workgroups			✓	✓	✓
+ Free Attendance at Member Meetings			✓	✓	✓
+ XML Data Feeds			✓	✓	✓
+ FS-ISAC Governance				✓	✓

Source: Financial Services ISAC, *Membership Benefits*, https://www.fsisac.com/join.

Mandatory, Voluntary, and Incentivized Sharing

The SEC requires publicly traded companies to disclose "material information," including with regard to cybersecurity risks and cyber incidents. The Supreme Court has ruled that information is material if there is "a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."[41] One open issue is how quickly information must be announced. Cybersecurity breaches can require weeks or months of investigation and remediation. Law enforcement may be concerned that a public announcement will alert those responsible and allow them to take countermeasures.

As discussed above, DOD is reported to require that its contractors share information on potential security breaches.[42]

Some, such as Dan Geer, chief information security officer of In-Q-Tel (a nonprofit venture capital firm that serves the U.S. intelligence community) have called for mandatory sharing of some information. He has noted that multiple sources have estimated that third parties discover 75% of data breaches. Geer bases his proposed model on the systems used by the aviation industry, which voluntarily reports incidents that had a significant chance of causing damage, and the Center for Disease Control, which mandates reporting incidents above a certain threshold of harm.[43] Other experts advocate a strictly voluntary approach, because they believe it could impose fewer regulatory costs on businesses and cost less for taxpayers.[44]

Consequences of Inadequate Information Sharing

Direct Effects on Security

Inadequate cybersecurity information sharing is thought to result in suboptimal security. By not sharing, organizations might duplicate the same work. If the information is shared—with or without cost—the savings could, in theory, be applied to increasing cybersecurity or some other purpose.

[41] *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438 (1976). For a discussion of recent controversies involving disclosure (or nondisclosure) of "material information," see Steven Davidoff Solomon, "In Corporate Disclosure, a Murky Definition of Material," *New York Times*, April 5, 2011, http://dealbook.nytimes.com/2011/04/05/in-corporate-disclosure-a-murky-definition-of-material/?_php=true&_type=blogs&_r=0.

[42] Jon W. Burd, "Cybersecurity Developments: Does the NIST 'Voluntary' Framework Portend New Requirements for Contractors?" Wiley Rein LLP, 2013, http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=3&id=9264.

[43] Dan Geer, "Cybersecurity as Realpolitik," keynote address at Black Hat USA 2014, Las Vegas, NV, August 6, 2014, http://geer.tinho.net/geer.blackhat.6viii14.txt.

[44] David Inserra and Paul Rosenzweig, "Cybersecurity Information Sharing: One Step towards U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation, April 1, 2014, http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

Indirect Security Effects through the Market for Cybersecurity Products

Information differences between buyers and sellers of cybersecurity products could lower the size and quality of the market for cybersecurity products. Cybersecurity can be thought of as an example of a "market for lemons," a concept developed by George Akerlof, which he applied to the used car market.[45]

In a "lemon market," buyers cannot accurately assess a product's value before purchasing it, and sellers cannot credibly disclose the product's value because they have incentives to overstate the quality of their products. If the buyer cannot determine whether the product is better or worse than average, the buyer will be unwilling to pay more than the average price of all the products in the market. This means sellers of better than average quality products have difficulty selling their products for what they are worth, so they underinvest in product development, driving down the overall quality and size of the market.

Security products in general are prone to this problem. It is difficult or impossible to know whether a security product is working because it is good or because the attacks have been weak or few in number. The overall effect is that there are fewer products and relatively fewer good products to choose from, and buyers cannot be confident that they are getting a good value. One result could be less cybersecurity investment than would be optimal.

Effects of Greater Information Sharing

Sharing more information could reduce the information asymmetries and increase the size and quality of the market for cybersecurity products and make cyberspace more secure, allowing firms to better estimate the probability and costs of data breaches, for example. Sharing more information could also reduce duplication of effort, making dollars spent on cybersecurity more effective. Clear metrics of effectiveness and objective, trusted, third-party evaluation services do not appear to currently exist in the cybersecurity market.[46]

The advantages of information sharing are likely to be greatest when organizations are using similar technologies. For example, learning about a weakness in an operating system or application software has the most value to an organization using that operating system or application. It might provide a lesson to those using other software, but it is less likely to be directly applicable.

Another concern is that erroneous information could lead to new security holes. The reputation of those providing information can provide assurance that experts have reviewed and passed on the information.

[45] George Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," *Quarterly Journal of Economics*, vol. 84, no. 3 (August 1970), pp. 488-500.

[46] In addition, an organization's cybersecurity depends on all the defensive measures that it has taken. A perfect anti-virus program does not exist, but even if it did it would not protect against other types of attack.

Currently, a main enforcement mechanism for cybersecurity is the Federal Trade Commission's (FTC's) authority to sue companies for deceptive practices—for example, claiming that their products are "secure" when they do not employ common security practices.[47] Thus, a de facto standard exists for what constitutes acceptable cybersecurity, but it is based on a series of actions taken by organizations that do not need to publicize their security practices. Greater information sharing could make it easier for companies to implement uniform security practices.

Greater information sharing may, in some instances, effectively weaken cybersecurity by creating an overwhelming amount of information, eliminating the capacity to pay attention to truly important alerts. ISACs can help to mitigate this problem by analyzing information and sorting out what information is relevant to subsets of their members.

Some have argued that greater information sharing could encourage the growth of the $1.3 billion cyberinsurance market by allowing for more accurate assessment of risk and security products' effectiveness.[48] A more mature cyberinsurance market would itself make cyberspace more secure: Insurers promote practices that make the insured safer, which would decrease insurers' payouts. Insurers verify and inspect the systems they are insuring. However, some analysts believe that cyberinsurance will have limited utility as many of the losses, such as damage to one's reputation, are intangible and difficult to put a value on.[49]

Selected Legislation in the 114th Congress to Encourage Information Sharing

This section provides brief summaries of two bills that have been introduced in the 114th Congress that might affect the willingness of organizations to share cybersecurity information. The bills contain many other provisions, such as which agency would have the lead in analyzing information shared, but considerations such as these are outside the scope of this report. For more details, see CRS Report R43996, *Cybersecurity and Information Sharing: Comparison of H.R. 1560 and H.R. 1731 as Passed by the House*, by Eric A. Fischer and CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.

H.R. 1560: Protecting Cyber Networks Act (Title I) and National Cybersecurity Protection Advancement Act (Title II, formerly H.R. 1731)

On April 22, 2015, the House passed H.R. 1560, Protecting Cyber Networks Act (PCNA), and on April 23, 2015, it passed H.R. 1731, National Cybersecurity Protection Advancement Act of 2015 (NCPA). Pursuant to H.Res. 212, the text of H.R. 1731, as passed by the House, was added as

[47] *Federal Trade Commission v. Wyndham Worldwide Corporation et al.*, Civil Action No. 13-1887 (ES) (U.S. District Court of New Jersey 2014). For CRS legal analyses of these issues see, for example, CRS Legal Sidebar WSLG947, FTC v. Wyndham Worldwide Corp.: NJ Federal District Court Upholds the FTC's Authority to Regulate Data Security as an Unfair Trade Practice, by Gina Stevens.

[48] Nicole Perlroth and Elizabeth A. Harris, "Cyberattack Insurance a Challenge for Business," *New York Times*, June 8, 2014, http://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html?_r=0.

[49] Ibid.

new matter at the end of H.R. 1560. House-passed H.R. 1560 became Title I of the bill sent to the Senate, and House-passed H.R. 1731 became Title II. This report briefly discusses a possible conflict in the various provisions of H.R. 1560 and H.R. 1731.

H.R. 1560 would authorize voluntary, two-way sharing of cybersecurity information between the federal government and certain other groups, such as nonfederal entities (i.e., other levels of government, information sharing and analysis centers [ISACs], and information sharing and analysis organizations [ISAOs]). The federal government would not be able to condition sharing on receiving information from nonfederal entities. The federal government would develop ways to share its information without compromising security, privacy, and civil liberties. H.R. 1560 would preempt any federal, tribal, state, or local laws that could be used to require a government to disclose information received under the proposed legislation.

H.R. 1560 contains a provision that would require the Administrator of the Small Business Administration to provide assistance to small businesses and small financial institutions to participate in cybersecurity information sharing.

H.R. 1560 would declare that there be no cause of action against a nonfederal entity for sharing or receiving the specified cybersecurity information, except under certain circumstances, including willful misconduct.

H.R. 1560 would, in general, allow two or more nonfederal entities sharing cybersecurity information as outlined in the bill without violating antitrust laws.

Title I of the bill would amend parts of the National Security Act of 1947, and Title II amends parts of the Homeland Security Act of 2002. There are many differences in the assignment of responsibilities and definitions between the two titles. For example, Title I would give the lead role in collecting and sharing government information with nonfederal entities to the Director of National Intelligence; Title II assigns this lead role to the Department of Homeland Security.

S. 754: Cybersecurity Information Sharing Act of 2015

On March 17, 2015, the Senate Select Committee on Intelligence reported out S. 754, Cybersecurity Information Sharing Act of 2015 (CISA). On April 15, 2015, Senator Richard Burr filed S.Rept. 114-32.

S. 754, like H.R. 1560, would authorize voluntary, two-way sharing of information between the federal government and nonfederal entities, including ISACs. The legislation would prohibit the federal government from making sending cybersecurity information to it a condition for receiving information from the federal government. The federal government would have to develop ways to share its information without compromising security, privacy, and civil liberties. S. 754 would preempt any federal, tribal, state, or local laws that could be used to require a government to disclose information received under the proposed legislation.

S. 754, like Title I of H.R. 1560, would assign the lead responsibility for federal government information sharing to the Director of National Intelligence.

S. 754 states that there would be no cause of action against a nonfederal entity for sharing or receiving the specified cybersecurity information, except under certain circumstances, including gross negligence or willful misconduct.

Under S. 754, two or more nonfederal entities could, in general, share cybersecurity information without violating antitrust laws.

Analysis

Both H.R. 1560 and S. 754 are designed to encourage information sharing, but they differ in where within the federal government certain responsibilities would fall. Both propose that the federal government share information with nonfederal entities and provide for voluntary sharing of information among nonfederal entities and between nonfederal entities and the federal government. They would protect information shared against disclosure under the Freedom of Information Act (FOIA) and similar tribal, state, and local laws. They would provide some protection against private law suits and would codify current the Federal Trade Commission and the Department of Justice policy that cybersecurity information sharing does not in itself violate antitrust laws. They would limit the use of cybersecurity information to cybersecurity and to specified serious crimes.

This could encourage more cybersecurity information sharing, but some nonfederal entities are likely to be cautious and wait to see how the various provisions are applied. On the one hand, they may wait to see how the federal government shares information with nonfederal entities. On the other hand, the federal government could not limit participation in cybersecurity information sharing programs to those sending such information to the federal government.

Conclusion: How Might Incentives Change?

H.R. 1560 and S. 754 seek to make cyberspace more secure by increasing the amount and impact of information shared while not significantly increasing costs to businesses or taxpayers. Except for codifying current antitrust exemptions for information sharing, the bills do not address the competitive incentives not to share information.

However, both bills could increase the likelihood of informal information sharing networks developing. Although some informal networks might lack the technical capabilities of an ISAC, they can arguably discourage free-riding[50] by cutting "takers" out of the network, which would alter incentives in favor of more information sharing.

Some sharing is already happening. Many cybersecurity companies currently share information with clients. Some of this is being done in real time.

The "bottom line," is likely to be how nonfederal entities—particularly businesses—value the benefits from sharing information against the cost of sharing. Neither bill would address the cost of full membership in ISAOs or ISACs which, at $10,000 to $100,000, are too expensive for small- and medium-size businesses.[51]

[50] In the context of an information sharing organization, free riding refers to the possibility that some members might receive information from others without contributing information.

[51] Prepared Testimony of Martin C. Libicki, Senior Management Scientist at The RAND Corporation, before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, March 4, 2015, http://docs.house.gov/meetings/HM/HM08/20150304/103055/HHRG-114-HM08-Wstate-LibickiM-20150304.pdf.

Although most data breaches have not been expensive compared with the revenues and profits earned, recent events may change the attitude of boards of directors and senior management: the chief executive officers at Target and Sony Entertainment were forced to resign.[52]

Author Contact Information

N. Eric Weiss
Specialist in Financial Economics
eweiss@crs.loc.gov, 7-6209

Acknowledgments

Ben Bleiberg, a CRS intern from Pomona College in the summer of 2014, helped greatly in this report by conducting research and writing the first drafts.

[52] At Target, Gregg Seinhafel resigned under pressure, and at Sony, Amy Pascal resigned as co-chairman. For more details see Elizabeth A. Harris, "Faltering Target Parts Ways with Chief," *New York Times*, May 5, 2014, p. B1, New York Edition, and "Amy Pascal Sets Down as Sony Pictures Chief," *New York Times*, February 5, 2015.