Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated April 29, 2015

Cybersecurity and Information Sharing

This *In Focus* summarizes the issues related to sharing information about cybersecurity breaches (the theft of information from computer networks) to prevent similar incidents in the future. Legislation has been introduced in the 113th and 114th Congresses to remove what some perceive to be legal obstacles to information sharing.

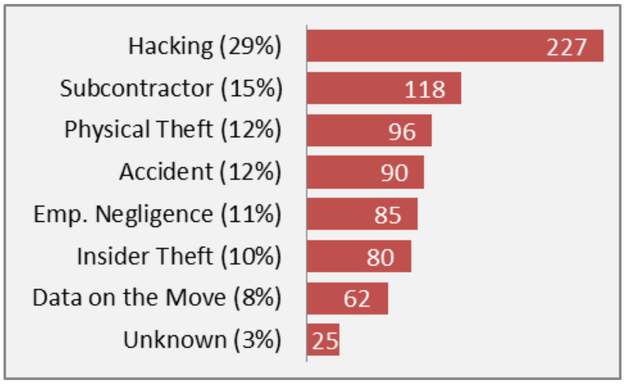
Overview

What Is Information Sharing? The discussion of cybersecurity data breach *information sharing* usually refers to sharing information within an industry or between industry and government about a cyberattack. Sharing data breach information with consumers is usually discussed separately and called *data breach notification*.

What Is Stolen in a Data Breach? Confidential information is usually copied in a data breach and sold or used in ways that adversely impact the rightful owners of the information. This can include credit and debit card information, medical records, personally identifiable information, or an organization's proprietary information. Historically, credit card information has been the most stolen information.

How Do Data Breaches Occur? In 2014, according to the Identity Theft Resource Center, hacking was involved in 29% of 783 data breaches analyzed. Other causes were subcontractors and third parties (15%), physical theft (13%), accidental exposure (12%), employee negligence (11%), insider theft (10%), and data moving over a network (8%).

Figure 1. Techniques Used in Data Breaches



Source: Identity Theft Resource Center, ITRC Breach Statistics 2005-2014, http://www.idtheftcenter.org/images/breach/MultiYearStatistics.pdf.

Costs and Who Bears Them? Merchants that honor stolen credit cards can have charges reversed (a chargeback) and end up without the merchandise or the payment. Credit card issuers say they are not fully reimbursed when they have to replace a compromised credit card. Companies that produce software with security flaws may not bear the cost of the flaws. The result is that those responsible for cybersecurity breaches rarely pay the full cost of those breaches.

Use of Shared Information. Sharing information about cyber breaches could help other organizations to implement lessons learned from the breaches. This does not always occur. Recently data breaches have used similar techniques that were disclosed in the media. For example, memory skimming was used in the Target data breach to capture information in the chain's point of sale terminals. Target was not the first company to suffer from this attack method; other companies that have been victimized by the same malware are reported to include Home Depot and three parking services.

> The biggest question is whether this information sharing proposal will contribute to the stated purpose, namely "to better protect information systems and more effectively respond to cybersecurity incidents."
> —Richard Bejtlich, Chief Security Strategist at FireEye

More generally point of sale terminals have reportedly been compromised in various ways at the Mandarin Oriental Hotel Group, Natural Grocers, gas station pumps, White Lodging Services (twice), ATMs, Chick-fil-A, Staples, Bebe, Michaels, and Kmart to list a few.

Efficiency Considerations. A lack of information sharing can lead organizations to duplicate each others' work. Sharing information could, in theory, lead to more security at less cost.

Perceived Legal Barriers. Firms and industry groups have cited concerns over violating privacy and antitrust laws as a reason that they are reluctant to share information. In an attempt to assuage such fears, the Department of Justice and the Federal Trade Commission have issued a joint statement that "properly designed sharing [is] not likely to raise antitrust concerns."

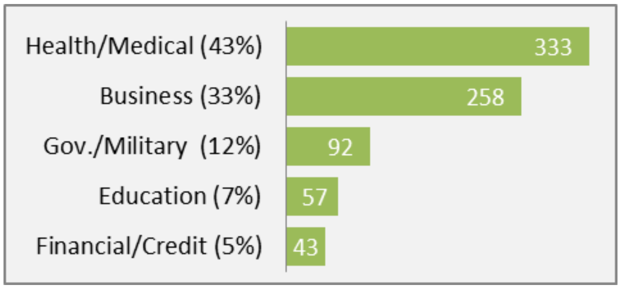
Some firms might be concerned about liability for sharing information that includes innocent third parties.

Technical Barriers. One issue in sharing information is the technical abilities of those receiving the information to use it. For example, the suggestion to "update and run an antivirus program" is unlikely to present much of a technical challenge, but "check all servers to verify that the default administrator account has been deleted and that each server has a unique password" requires more technical skills and probably more effort.

Sectors Affected. In 2014, according to the Identity Theft Resource Center,

- 43% of all known data breaches occurred in medical and healthcare facilities;
- 33% occurred in business computer systems, including retailers, hotels, professionals, and payment processors;
- 12% occurred in government (any level) or military facilities, including Veterans' Affairs hospitals;
- 7% occurred in education organizations from preschool through college; and
- 5% occurred in banking, credit, and financial institutions, such as banks, credit unions, credit card companies, and pension funds.

Figure 2. Industry Share of Data Breaches



Source: Source: Identity Theft Resource Center, ITRC Breach Statistics 2005-2014, http://www.idtheftcenter.org/images/breach/MultiYearStatistics.pdf.

How Can Organizations Share Information? Currently, 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. These ISACs were authorized in 1998 by Presidential Decision Directive 63, on critical infrastructure protection. The federal government oversees ISACs for critical infrastructure through sector-specific agencies, such as Treasury for the Financial Services ISAC and the Department of Homeland Security for the Chemical Sector ISAC.

ISACs charge for some levels of membership. For example, the Financial Services ISAC provides "limited critical notifications" to members who pay no annual fees, and more detailed information to members who pay fees that range from $250 to $49,940 per year.

In addition to these critical infrastructure ISACs, other sectors have created ISACs. More generally, Information Sharing and Analysis Organizations are an expansion of the ISAC concept. In addition, there are private, fee-based, for profit information sharing groups.

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. Any lessons learned remediating a current breach are likely to be applied to future breaches.

Sharing Networks. Shared information can be used most easily when the network environments are similar or identical. This suggests that industry-based information sharing groups could form a logical organizational structure. Nevertheless, companies in different industries may share similar network configurations. For example, information about an attack on a point-of-sale terminal could be of interest to financial services, hotels, car rental companies, restaurants, and more. Supervisory control and data acquisition (SCADA) systems are used by all types of utilities, and also control elevators, heating, ventilation, and air conditioning in large buildings.

Cyberinsurance. Insurance is a way to share risks so that when an unlikely event occurs the insured entity receives a payment to compensate for the losses. Commercial underwriting practices for property and casualty insurance include assessing the risk mitigation precautions that an insured company has taken and evaluating the remaining risk. This evaluation is used to determine insurance premiums.

Prior data breach claims help a cyberinsurance company to estimate the probability of a breach and the likely covered losses. A cyberinsurance company might use this experience to recommend cybersecurity improvements. Thus, cyberinsurance companies can gather detailed, technical information on breaches and use this knowledge to prevent future breaches at other clients.

Selected Legislation in the 114th Congress

H.R. 1560, Protecting Cyber Networks Act

H.R. 1731, National Cybersecurity Protection Advancement Act of 2015

S. 754, Cybersecurity Information Sharing Act of 2015

Additional Resources

CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer**.**

CRS Report R43821, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*, by N. Eric Weiss.

CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan**.**

CRS Report R42409, *Cybersecurity: Selected Legal Issues*, by Edward C. Liu et al.

CRS Report R43996, *Cybersecurity and Information Sharing: Comparison of H.R. 1560 and H.R. 1731*, by Eric A. Fischer.

N. Eric Weiss, Specialist in Financial Economics

IF10163

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.