Congressional Research Service
Informing the legislative debate since 1914

TESTIMONY

Statement of

Chris Jaikaran
Analyst in Cybersecurity Policy

Before

Committee on Banking, Housing, and Urban Affairs
U.S. Senate

Hearing on

"Consumer Data Security and the Credit Bureaus"

October 17, 2017

Congressional Research Service
7-5700
www.crs.gov

Introduction

Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you for the opportunity to testify on consumer data security and the credit bureaus. My name is Chris Jaikaran and I am an Analyst in Cybersecurity Policy at the Congressional Research Service. In this role, I research and analyze cybersecurity issues and their policy implications–including issues of data security, protection and management.

My testimony today will include discussion of data security as an element of cybersecurity and risk management, analysis and a case study on how data breaches occur, a description of cyber incident response, and possible options for Congress to address data security and data protection. My testimony today is based solely on publicly available information and CRS analysis.

Cybersecurity and Data Security

An increasingly used catch-phrase among industry analysts is that today "all companies are technology companies," or "all companies are data companies."[1] This concept reflects the role that information technology (IT) and data play in enabling the modern business practices that allow companies to compete and thrive in the marketplace. This reliance on IT and data also creates risk for corporate leadership to manage. Adequately controlling that risk is an objective of cybersecurity.[2]

Data security is an element of cybersecurity. At the most basic level, cybersecurity is the security of cyberspace, which includes not just data, but the networks, hardware, software, services, and infrastructure that data relies upon. It is also important to note that data does not exist by itself, but is created, manipulated and used by people. Consequently, cybersecurity is not just the security of data, hardware, software, infrastructure, networks and services—but also the human users of cyberspace.

Computer scientists view data security through three attributes:

- *Confidentiality*: that the data is only known to authorized parties. A data breach is an example of how confidentiality is breached, while encryption is a tool used to ensure confidentiality.
- *Integrity*: that the data is known to the authorized parties as intended. Data manipulation is an example of how integrity is breached, while there are data checking technologies, such as blockchain, to ensure that one can verify the integrity of data.
- *Availability*: that the data is available to authorized parties when they choose. Ransomware attacks availability, while backups are a tool that ensures availability of data.

[1] Nathaniel Fink, "Cybersecurity for a New America: What's Next for the Cybersecurity Community," conference keynote, March 20, 2017, at https://youtu.be/wfMpUpxNPAg.
Avi Gesser, Gabriel Rosenberg, and Matt Kelly, "Cybersecurity and Data Management," webinar, Davis Polk & Wardwell LLP, October 11, 2017.

[2] Risk may be managed by avoiding the risk, controlling the risk, transferring the risk, or accepting the risk. DHS Risk Steering Committee, "DHS Risk Lexicon," report, September 2010, at https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf.

Related to integrity is the concept of *authentication*, an attribute that one can verify that data is from a trusted source. The Internet was built using technologies that assumed the trust of its users, but as the Internet has grown into a global network, anonymity and the manipulation of data have proliferated.[3]

As an element of cybersecurity, data security involves risk management. Absolute security is not obtainable, so managing the risks which would impair security is generally considered to be the goal. In order to evaluate risk, managers need to understand the *threats* the enterprises may face, the *vulnerabilities* the enterprise has, and the *consequences* of an incident.[4]

Threats are generally considered to be the gamut of potential human attackers. Such attackers include nation-state actors, criminals and insiders to the network. Depending on the data an entity houses, and the services it provides, the realm of attackers may change from one day to the next, sometimes even driven by events in the news.

Vulnerabilities exist in software the moment it is shipped to users. Adding additional software to a growing enterprise creates complexities that can lead to further potential vulnerabilities. Some software vulnerabilities are known the day they are shipped and are catalogued in the Common Vulnerabilities and Exposures database with risk assessments enumerated in the National Vulnerabilities Database.[5] Others are discovered later. Vulnerabilities that are discovered but not disclosed to the vendor so they may be patched are called 0-days (zero or “oh” days). However, 0-day vulnerabilities do not necessarily create a large risk for enterprises. In addition to a vulnerability being present on a system, it must be exploited to cause some impact. The exploitation of a vulnerability may be so difficult that an entity’s risk of falling victim to that 0-day is low. Despite 0-days being a threat, most cybersecurity incidents occur through attackers exploiting known vulnerabilities for which the entity has not deployed a patch.[6]

Consequences may vary based on the business of an entity, the data that entity houses, and the stakeholder community for the entity. Consequences are also multi-dimensional. The loss of data may inhibit business practices, but may also lead to reputational loss, enforcement actions, payments to stakeholders, or other impacts.

An entity may be able to better predict consequences through understanding the data in its possession. Using a data model or framework can help an entity identify attributes of its data. Such attributes include: where data is acquired; what other data the entity generates from acquired data; what types (both descriptively and by file type) of data is acquired or generated; how the entity will use and access data; how the data will be shared with other parties; where data is stored, accessed, and transmitted; and what policies exist for data retention and data disposal. Such a data model is essentially an architecture of the entity’s data, similar to the network architecture of their IT systems or the blueprints for their building.

The National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Framework) provides functions, activities and categories in a common format to assist entities in thinking through cybersecurity issues and identifying resources to assist in completing activities. [7] (Some of these activities include asset management, data security, and detection processes.) However, the Cybersecurity Framework is not the only reference for organizations to consider

[3] CRS In Focus IF10559, *Cybersecurity: An Introduction*, by Chris Jaikaran.

[4] Davis Hake, “Threat, Vulnerability, Consequence,” interview with *The Cipher Brief*, December 15, 2015, at https://www.thecipherbrief.com/threat-vulnerability-consequence.

[5] https://cve.mitre.org. https://nvd.nist.gov.

[6] Jory Heckman, “Hackers Not Yet Pulling Out Big Guns for Data Breaches, NSA Official Warns,” *Federal News Radio* article, October 18, 2016, at https://federalnewsradio.com/technology/2016/10/hackers-not-yet-pulling-big-guns-data-breaches-nsa-official-warns/.

[7] NIST, “Cybersecurity Framework,” webpage, at https://www.nist.gov/cyberframework.

using, or a document which they can only use exclusively. The Center for Internet Security, the International Standards Organization, and ISACA also publish cybersecurity frameworks which an entity may use in conjunction with or in replacement of the NIST Cybersecurity Framework.[8]

The Anatomy of a Breach

The recent breach of Equifax provides a timely case study on how breaches occur.[9] While a single command may be executed at a speed fast enough for the computer to process it, full attacks are done by humans, and as such, occur at human speed. Breaches can be understood through an attack framework.[10]

First, an attacker examines the target. Through this examination the attacker learns about the target system. This examination is both online and off. Business cards provide the naming convention for user accounts on the system (in the form of email addresses), while digital tools can provide information on services running on Internet-facing services. In the case of Equifax, scans of their credit report dispute website may discover that Apache Struts was an available service and that it was running under a vulnerable version.[11]

Second, an attacker exploits a vulnerability. This initial exploitation provides the entryway for an attacker into the system or network. As stated earlier, vulnerabilities themselves do not necessarily create a significant risk scenario for an enterprise, but an exploitation of that vulnerability may. In some cases, a single vulnerability is required to gain access, while in others multiple vulnerabilities may be used to create an effective exploit. In the case of Equifax, a vulnerability in an earlier version of Apache Struts allowed for remote code execution.[12] NIST deemed this type of vulnerability as critical, and the Apache Foundation patched it and provided an additional work around.[13] At the time it was patched, it was also added to penetration testing software so that system administrators could test to see if they were still vulnerable to exploitation.[14]

Third, after the initial exploitation, attackers entrench into the system. By entrenching into a system, attackers are discovering more about the network they have penetrated. In this phase, they gain access to additional systems in that network, escalate their privileges so that they have further access, and acquire additional credentials. In the case of Equifax, how attackers entrenched into the system is publicly

[8] Cybersecurity frameworks from these organizations can be found at https://www.cisecurity.org/controls/; https://www.iso.org/standard/54533.html ; and http://www.isaca.org/cobit/pages/default.aspx. ISACA was previously known as the Information Systems Audit and Control Association, but now goes by its acronym only.

[9] Information on the Equifax breach is derived from testimony provided by former CEO Richard Smith before the U.S. Senate Committee on Banking, Housing, and Urban Affairs. Richard Smith, "Prepared Testimony of Richard Smith," testimony, October 4, 2017, at https://www.banking.senate.gov/public/_cache/files/da2d3277-d6f4-493a-ad88-c809781f7011/F143CC8431E6CD31C86ADB64041FB31B.smith-testimony-10-4-17.pdf.

[10] The framework presented in this testimony is based on previous analysis by CRS. Further case studies are available via CRS Recorded Event WRE00157, *Cybersecurity: Anatomy of a Breach*, by Chris Jaikaran.

[11] Apache Struts is a developer framework which allows for common programming languages, such as Java, to be used to develop user facing web applications. It is open source software maintained by the Apache Software Foundation, https://struts.apache.org/.

[12] CVE, "CVE-2017-5638," data base entry, at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638.

[13] NIST, "CVE-201705638 Detail," webpage, March 10, 2017, at https://nvd.nist.gov/vuln/detail/CVE-2017-5638. Apache Foundation, "S2-045," webpage, at https://struts.apache.org/docs/s2-045.html.

[14] The exploitation of CVE-2017-5638 was added to the Metasploit Framework. https://github.com/rapid7/metasploit-framework/issues/8064.

unknown. However, many instances of Apache Struts run on web servers with default administrative credentials, which may have provided the next step for an attacker to entrench into the system.[15]

While he was the Chief of the National Security Agency's Tailored Access Operations unit, current White House Cybersecurity Coordinator Rob Joyce said that "you know the things you intend to have in your network, we look for the things that are actually in your network."[16] This summarizes the relationship between defenders and attackers. Defenders know what they acquired, deployed and intend to have on their network, while attackers know the vulnerabilities and what else is running on that network. Exploiting vulnerabilities and entrenching into systems takes advantage of this asymmetric knowledge.

Fourth, after gaining access, attackers can then execute steps to achieve their objectives. These objectives could be to compromise the confidentiality of the data by stealing it. Confidentiality is not only compromised by theft, but also by access. This distinction is referred to as exposure versus exfiltration. Data is exposed when an unauthorized party may access it on an entity's network, but it is exfiltrated when they take it off that network. This relationship is akin to perusing books in a library but only checking out one. All the books are exposed to a patron, but only the borrowed book is exfiltrated. The integrity of data may be compromised by altering the data in a system. Alternatively, the availability of the data may be compromised by deleting it or otherwise making it unavailable (e.g., through encrypting data in a ransomware attack). In the case of Equifax, it appears that over 145 million people had their data exposed, while some had their dispute documents (which contain personally identifiable information) and credit card information exfiltrated.

Finally, the attackers would exit on their terms. After achieving their objectives, the attackers would seek to leave the system so that they may have access again at a later date, or to cover evidence of their activities. Deleting log files, adding connections to network whitelists and creating credentials are examples of activities an attacker would undergo to exit the compromised system on their terms. In the case of Equifax, it is unknown from publicly available sources what attackers did in this phase.

By understanding how attacks occur through such a framework, system defenders could develop defense-in-depth strategies to mitigate breaches. Defense-in-depth is an approach which uses layered countermeasures to defend against cybersecurity risks throughout a network.[17] Countermeasures could be layered to address each phase of an attack so that defenders are quickly alerted to attacks and can take actions to prevent further damage to their enterprise.

Cybersecurity Incident Response

Cybersecurity incident response describes when system administrators seek to confirm the attack, discover information about it, and mitigate against it. The response as described below is from the breached entity's perspective, and does not discuss government response options.

Incident response is not limited to the time immediately following an attack, however. Before an attack, response planning, training, and exercising can occur. Response planning helps an organization think though its risks and how it will respond to those risks, train its personnel on how to respond to attacks,

[15] Hector Monsegur, "How to Fight Hackers, with Former Black-Hat Hacker Hector Monsegur," podcast, October 2, 2017, at https://lifehacker.com/how-to-protect-yourself-from-hackers-with-hector-monse-1819075906.

[16] Rob Joyce, "USENIX Enigma 2016 – NSA TAO Chief on Disrupting Nation State Hackers," conference talk, January 28, 2016, at https://www.youtube.com/watch?v=bDJb8WOJYdA.

[17] Industrial Control Systems Cyber Emergency Response Team, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," report, September 2016, at https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

and practice its response to build confidence in staff and management as to the organization's capability and capacity to manage incidents.

For incident response, staff is not limited to just IT personnel. Response planning should also include, among others, communications staff that are able to craft messages to both internal and external stakeholders, legal teams who can help with reporting and compliance requirements, and management and corporate boards who are accountable for the operations of a corporation.

There will be a delay between the discovery of an attack and public notification of that attack because analysis of what transpired will need to be conducted. This analysis will inform the entity of how they were breached and what data or systems were compromised. This type of analysis may be conducted by the entity itself, a business partner of the entity, government response teams and law enforcement. With a variety of potential forensic investigators, determining how they will coordinate in their response and how they will share information among one another is a factor that can be determined during the planning and training phase. With information on how the breach happened and the extent of the breach, the entity can proceed to mitigate its affects. These two phases need not occur in succession, but may be able to occur concurrently.

Finally, the organization can improve their data security and response planning by learning from their efforts and applying insights gained.

Potential Options for Congress

Three options for Congress are presented below to generate discussion. They are not recommendations from CRS. Given time constraints, these options are provided with limited policy discussion and are not exhaustive.

Authorize a Federal Agency to Examine for Information Security

Congress can authorize a federal agency to engage in supervisory examinations of the credit reporting agencies (CRAs) for compliance with the safeguards rule.[18]

As an example, the Consumer Financial Protection Board (CFPB) has broad authority to bring enforcement cases against corporations for unfair and deceptive business practices. CRS research could not identify an enforcement case or issued guidance where CFPB sought to address information security. This may be because CFPB has an express prohibition against issuing rules concerning information security and bringing enforcement actions against an entity concerning information security. Instead, the authority to issue a standard for the protection of nonpublic personal information, and enforce that standard, is retained by the Federal Trade Commission (FTC).[19] The FTC issued the safeguards rule in 2002 pursuant to the authority referenced above and is currently seeking public comment on an update.[20]

Instead of engaging with CRAs after a cybersecurity incident, CFPB has the authority to supervise CRAs prior to an incident occurring.[21] Congress could explicitly authorize CFPB to examine CRAs for their adherence to the safeguards rule, as promulgated by the FTC. The dialogue created by CFPB and a CRA could lead to greater understanding of the cybersecurity risk faced by the CRAs and allow CRAs with deficiencies to correct their data security measures prior to referral to FTC for enforcement action. As this

[18] 16 C.F.R. §314

[19] 15 U.S.C. §6801, §6804, §6805.

[20] 16 C.F.R. §314. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule.

[21] 12 U.S.C. §5514.

is not an activity CFPB currently engages in during an examination, a new program may need to be established in the CFPB to recruit the talent to manage such a technical examination.[22]

Regulate Personal Data Collection and Use

Congress could regulate the collection, use, and retention of data regardless of the type of entity housing that data. The European Union has such a regulation known as the General Data Protection Regulation (GDPR), and Canada is in the process of updating their Personal Information Protection and Electronics Document Act (PIPEDA).[23] In proactively regulating data, Congress can establish data use requirements. Some of those requirements may include what data may be collected, how data must be stored (e.g., encryption, location, etc.), the consumer's rights to collection and use of data about them, and under which circumstances data may be shared with other parties. While the United States does not have an overarching law governing data use, U.S. agencies have promulgated guidance on data protection. [24]

Require Data Transparency

Congress could require CRAs, or any entity that profits from consumer data, to identify and disclose their data model to consumers. Disclosure of all elements of the model may not be necessary (i.e., where data is stored). However, some elements such as where data is acquired, how it is used, and what other data the entity generates about the consumer may provide consumers with additional information and affect their decisions in the marketplace. For example, if a consumer knew that a CRA acquired data from a company they have a business relationship with, they may choose to limit their interactions with that company or seek out an opt-out/opt-in form from that business to limit how their data may be shared.

Conclusion

Thank you for the opportunity to testify today. I look forward to your questions. If you require further analysis of these options, or other policy issues before Congress, my colleagues and I at the CRS stand ready to assist you.

[22] Current CFPB examination procedures may be found online at https://www.consumerfinance.gov/policy-compliance/guidance/supervision-examinations/.

[23] http://www.eugdpr.org/ . https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

[24] FTC, "Protecting Personal Information," guide, October 2016, at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.