MIS Quarterly Executive

Volume 20 | Issue 2 Article 4

June 2021

Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense

Ilya Kabanov

Stuart Madnick

MIS Quarterly Executive

Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense

The Equifax data breach in 2017 was one of the largest in history, with 148 million people affected. Using the Cybersafety method, we reconstructed the attack flow and Equifax's hierarchical safety control system structure. We identified 19 systemic failures spanning the four levels of the hierarchy and, based on our analysis of the reasons for the failures, we provide recommendations that managers can use to strengthen their organization's cybersecurity.[1,2]

Ilya Kabanov
Massachusetts Institute of Technology
(U.S.)

Stuart Madnick
Massachusetts Institute of Technology
(U.S.)

The Equifax Cybersecurity Incident Provides Learning Opportunities

On September 7, 2017, Equifax Inc., one of the largest U.S. credit reporting agencies, announced a cybersecurity incident that affected more than 143 million consumers in the United States. In this incident, cybercriminals exploited a vulnerability found in a U.S. website application and then obtained access to consumers' confidential information. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. When the news broke, Equifax's stock dropped by 13% to $123.23 and continued falling until it hit a low at $92.98, wiping out 34% of the company's $17.5 billion market value.

The incident was investigated by various federal and state agencies that collected and reviewed over 45,000 pages of related documents. Based on the evidence, the Permanent Subcommittee on Investigations of the United States Senate Committee on Homeland Security and Governmental Affairs[3] and the U.S. House of Representatives Committee on Oversight and Government Reform[4] published their reports on the Equifax data breach. The investigation resulted in "The Settlement,"[5] with the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB) and 50 U.S. states, which was announced on July 22, 2019 and required Equifax to pay at least $575 million. Although the reports describe what

1 Mary Lacity is the accepting senior editor for this article.
2 The authors thank Mary Lacity, Gabe Piccoli and the reviewers for their suggestions and guidance through the review process.
3 *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach*, Staff Report: Permanent Subcommittee on Investigations, United States Senate, March 2019.
4 *Equifax Data Breach*, U.S. House of Representatives, Committee on Oversight and Government, December 2018.
5 *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, Federal Trade Commission press release, July 22, 2019, available at https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

SIM WHERE IT LEADERS CONNECT
KELLEY SCHOOL OF BUSINESS INDIANA UNIVERSITY
DOI: 10.17705/2msqe.00044

transpired and The Settlement specifies Equifax's monetary and security recovery obligations, they did not focus on why the failures and shortcomings occurred, what should be done to prevent them and what others could learn from this event.

There is a consensus that systematic learning from information security incidents and addressing deeper root causes is worth the effort. However, some research shows that many organizations miss an opportunity to learn from incidents as they are just "focused on resolving the direct causes of incidents."[6] Most analyses of cyberattacks focus on a single cause, such as a phishing email, a patch that had not been applied on time, etc., and therefore make it seem that the root cause of an incident is a simple problem arising perhaps from one person's error or negligence. That is usually not the complete story, however. In our analysis of the Equifax incident, we applied the Cybersafety method,[7] which enabled us to identify 19 technical and organizational safety control mechanisms that failed to prevent and stop the spread of the attack.

In this article, we first provide an overview of Equifax and the credit reporting industry, and then describe the Equifax cybersecurity incident and our approach to analyzing it. The bulk of the article describes the attack's flow and the safety mechanisms that could have prevented or mitigated the attack, and the reasons why those mechanisms failed or did not exist. Finally, based on our analysis, we provide recommendations for improving cybersecurity arrangements and reducing the likelihood of successful cybersecurity attacks. Our findings and recommendations, and especially the Cybersafety analysis method, will help all organizations to strengthen their cybersecurity defenses.

Equifax and the Credit Reporting Industry

Equifax is one of the three major credit reporting agencies (CRAs) that dominate the U.S. market. Starting in 2006, Equifax embarked on an ambitious growth strategy. In 10 years, it made 18 acquisitions, making it one of the world's largest private credit-tracking firms. The company's business is based on detailed consumer and business information derived from organizations such as banks, thrifts, credit unions, and many other institutions and public record providers. The information may include historical data about credit repayments, rent payments, employment, insurance claims, arrests, bankruptcies, check writing and account management. According to Equifax's 2016 annual report, "the company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide."[8] Individual consumers—data subjects—do not voluntarily provide data to the CRAs and cannot "opt-out" of the data collection process. However, the Fair Credit Reporting Act (FCRA) states that they are entitled to a free annual report from each of the CRAs.

The enormous amount of sensitive information collected by CRAs makes them lucrative targets for cybercriminals. Before the Equifax incident in 2017, two significant data breaches had occurred at Experian, another major CRA, in 2013 and 2015, exposing more than 200 million consumers' personal and financial data.[9] Equifax had also experienced a series of data breaches prior to 2017. *The Complaint for Civil Penalties, Injunctive Relief, and Restitution filed by the State of Indiana* ("The Complaint") revealed that Equifax suffered a data breach almost every year from 2010 to 2017.[10] The Complaint confirmed that Equifax was aware it was on the radar of cybercriminals and that its information systems were susceptible to cyberattacks.

6 See McLaughlin, M-D. and Janis, G. "Challenges and Best Practices in Information Security Management," *MIS Quarterly Executive* (17:3), September 2018, pp. 237-262.

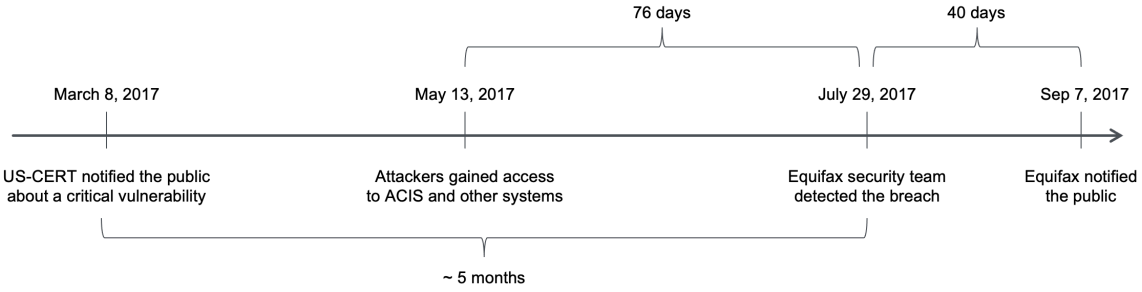
7 For information on the Cybersafety method, see Salim, H. and Madnick, S. *Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks*, Working Paper CISL# 2014-12, Massachusetts Institute of Technology, September 2014, available at, http://web.mit.edu/smadnick/www/wp/2016-09.pdf.

8 *The Power of Insights: 2016 Annual Report*, Equifax, February 22, 2017, available at https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2016-annual-report.pdf.

9 See Krebs, B. *Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records*, Krebs on Security, March 10, 2014, available at https://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records.

10 *Complaint for Civil Penalties, Injunctive Relief, and Restitution*, The State of Indiana, May 6, 2019, available at https://buckleyfirm.com/sites/default/files/Buckley%20InfoBytes-%20Indiana%20v.%20Equifax%20Complaint%202019.05.06.pdf.

Figure 1: The Equifax Cybersecurity Incident Timeline



Description of the Equifax Cybersecurity Incident and Our Analysis Approach

Description of the Incident

On July 29, 2017, Equifax identified, and a day later confirmed, a cyberattack on its Automated Consumer Interview System (ACIS). The attack came to light after Equifax's IT team updated a secure sockets layer (SSL) certificate on the SSL visibility appliance that monitored the encrypted inbound and outbound network traffic between Equifax's systems, including ACIS, and the internet. The SSL certificates had expired nine months earlier, in November 2016. After updating the certificate, Equifax employees detected suspicious internet traffic exiting ACIS that contained image files related to consumer credit investigations. They traced the traffic to an IP address in China—a country where Equifax did not operate. After blocking the IP address, Equifax noticed suspicious traffic from a second IP address owned by a German internet service provider (ISP) and leased to a Chinese ISP. As a consequence of these discoveries, Equifax decided to shut down ACIS temporarily.

Further analysis revealed that the suspicious traffic resulted from a successful cyberattack on ACIS that started on May 13, 2017. The attackers gained access to ACIS and databases containing consumers' personal identifiable information (PII) and then exfiltrated[11] the data over a period of 78 days before the attack was detected. The timeline of the key events associated with the Equifax cybersecurity incident is shown in Figure 1.

On September 7, 2017, Equifax publicly announced a cybersecurity incident, potentially impacting 143 million U.S. consumers whose names, social security numbers (SSNs), birth dates, addresses and, in some instances, driver's license numbers were compromised. Later, Equifax concluded that the actual number of affected consumers was approximately 148 million.

Before the incident, on March 8, 2017, the United States Computer Emergency Readiness Team (US-CERT) had notified the public about a vulnerability in the open source Apache Struts 2 Web Application Framework[12] that would allow an attacker to execute commands on affected systems. That vulnerability was present in ACIS and was exploited by the attackers to gain access to the Equifax network. Interestingly, a working exploit that illustrated how to attack vulnerable websites had been made available to the public on March 11, 2017, on GitHub.

Our Analysis Approach

We used the Cybersafety method of analysis, which is inspired by causal analysis using system theory (CAST), which in turn was developed to

11 Data exfiltration is when malware and/or a malicious actor carries out unauthorized data transfer from a computer.

12 Apache Struts 2 is an open source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller architecture.

determine the cause of industrial accidents.[13] The Cybersafety method has proved to be more effective than the chain-of-events model and fault-tree analysis, which are traditionally used for incident analysis in systems. The following three sections describe the three phases of our analysis. First, we analyzed what went wrong by reconstructing the attack's flow and identifying the safety constraints that could have prevented or stopped it. We also considered the safety mechanisms that Equifax did not have at the time of the incident. Second, to provide a context for our analysis, we needed to understand the legacy nature of Equifax's environment. Third, we conducted a detailed study of why the safety mechanisms in Equifax's hierarchical safety control structure failed to protect the company from the attack. Our research is predominantly based on the Equifax cybersecurity incident details documented in the reports by the Permanent Subcommittee on Investigations of the United States Senate, March 2019, the U.S. House of Representatives Committee on Oversight and Government, December 2018, and The Complaint filed by the State of Indiana.

Reconstructing the Attack Flow and Identifying the Safety Constraints

We used the Cyber Kill Chain framework[14] to understand how the attack happened through reconstructing its flow and identifying hazards and the safety constraints that could have prevented those hazards. This framework consists of the seven phases associated with the typical steps taken by cyberattackers: 1) reconnaissance, 2) weaponization, 3) delivery, 4) exploitation, 5) installation, 6) command and control and 7) actions on objectives. Table 1 summarizes the hazards caused by attackers at each of these phases, lists the safety constraints that could have prevented the hazards and states whether those constraints were present in Equifax's defense system at the time of the incident. However, even those safety constraints that had been incorporated (marked "Yes" in the table) failed, as explained below.

Phase 1: Reconnaissance

During this first phase, the attacker identified and selected Equifax as a target. The reconnaissance phase often involves the use of network scanners and social media research. Overexposing the internals of software systems and their components to the public makes the attackers' job easier. We hypothesize that the attackers could have used open source intelligence (OSINT)[15] techniques to identify that Equifax's ACIS used a susceptible version of Apache Struts 2. It is unclear whether ACIS was revealing the presence of Apache Struts 2 in its environment and what specific approach the attackers used for reconnaissance. However, we discovered that some websites using the vulnerable version of Apache Struts 2 could be easily found through "Google dorking."[16] Therefore, as a general safety constraint, Equifax should have ensured that ACIS did not reveal its technical details and should have prevented sensitive information from being indexed by search engines.

Phase 2: Weaponization

The weaponization phase includes constructing a malicious exploit in the form of a remote access Trojan virus, ready to be delivered into the victim's computer system. This phase occurred outside of Equifax's systems, so the company could not have deployed safety constraints to counter weaponization.

Phase 3: Delivery

During this phase, the malicious exploit is delivered to the victim's system. Equifax's attackers exploited a vulnerability in Jakarta's multipart parser used by Apache Struts 2 by sending a malicious content-type header in an HTTP request. A safety constraint to counter this type of vulnerability is to use a web application

13 For information on CAST, see Leveson, N. G. *Engineering a Safer World*, The MIT Press, 2011.

14 For information on the Cyber Kill Chain, see Hutchins, E. M., Cloppert, M. J. and Amin, R. M. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* (1:1), January 2011, pp. 113-125.

15 OSINT is the collection and analysis of publicly available information that can be used for planning and executing a cyberattack.

16 Google dorking is a technique that relies on powerful Google search engine data and can be used to find vulnerable web applications and servers on the internet.

17 We are not privy to the exact method the attackers used to identify an attack "vector," the path or means by which an attacker can gain access to deliver a malicious payload.

Table 1: Hazards Caused by Attackers and Safety Constraints

Cyber Kill Chain Phase	Hazard	Safety Constraint	Presence of Safety Constraint
1. Reconnaissance	Publicly accessible information about vulnerabilities in Equifax's IT systems	Nondisclosure of unnecessary details about software used in IT systems[17]	Unknown
2. Weaponization	A malicious exploit is prepared and ready for use	Not applicable because actions occur outside the system and can't be prevented by safety constraints	
3. Delivery	Payload with an exploit delivered to the system	Blockage of malicious requests sent by the attackers	No
4. Exploitation	Operation of the system with an exploitable vulnerability	Elimination of critical vulnerabilities in the systems through patching and vulnerability management	Yes
5. Installation	The attack spreads beyond its entry point	System's secure design (isolation, authentication, least privilege)	No
6. Command and Control	The attacker's covert actions in the network	Detection of suspicious traffic in the network with the Intrusion detection and prevention systems (IDS/IPS)	Yes
7. Actions on Objectives	Unauthorized access to unencrypted data	System's secure design (encryption of personal identifiable information)	No
	Bulk exfiltration of sensitive data	Limited data retention	No
		Identification and potential blockage of unauthorized data exfiltration	No

firewall (WAF). According to Memon's analysis,[18] even an open source WAF (e.g., ModSecurity) could have protected Equifax against the attack by detecting the malicious strings passed in the HTTP headers and blocking such traffic, should it be tasked to whitelist valid content types or blacklist object-graph navigation language (OGNL) expressions. However, because there is no reference to a WAF either in the reports we used as our main source of information or in other publicly available documents, we concluded that ACIS was not protected by a WAF and left open to accepting malicious requests at the time of the attack. Interestingly, the other two large U.S. CRAs, TransUnion and Experian, had a WAF in place configured to block attacks using the Apache Struts 2 vulnerability.

Phase 4: Exploitation

During the exploitation phase, the attacker's code is executed, targeting a vulnerability in one or several elements of the victim's software stack. The malicious request sent to ACIS exploited a critical vulnerability in Apache Struts 2 and led to the remote execution of unauthorized code delivered in the payload. At the time of the incident, Equifax had implemented vulnerability identification and patching mechanisms, the safety mechanisms which should have prevented the incident from happening. Later, in our analysis of shortcomings in Equifax's hierarchical safety control structure, we explain why these safety elements failed.

18 Memon, F. *Using ModSecurity to Virtually Patch Apache Struts CVE-2017-5638*, F5 Tech Blog, January 22, 2018, available at https://www.nginx.com/blog/modsecurity-apache-struts-cve-2017-5638/.

Phase 5: Installation

In the installation phase, a remote access tool is deployed on the victim's system to establish a presence inside the network and spread the attack. Our investigation revealed that other Equifax systems permitted access to their sensitive data through ACIS. This enabled the attackers to gain access to unencrypted application credentials for other sensitive Equifax databases, which stored confidential information and personal identifiable information. We identified three secure design principles that were not included in the design of ACIS:

- *Isolation principle:* This fundamental principle of secure software design requires computer subsystems to be separated from each other using physical devices and/or security controls to minimize the number of possible ways an attacker can get into a device or network (known as the "attack surface") and extract data.[19] The U.S. House of Representatives report found that "the ACIS application was not segmented off from other, unrelated databases." Furthermore, Sun Solaris, which hosts ACIS, has a shared file system across the environment that allowed access to administrator files across all systems. As a result, the attackers could move laterally throughout Equifax's networks and reach systems beyond ACIS.
- *Authentication principle:* Equifax did not follow this second secure design principle. A software system should assume that other systems are untrusted and require authentication before granting access to its data. Two major authentication issues were discovered in ACIS and other Equifax systems. The first was the use of weak passwords for privilege accounts. For instance, one of the databases accessed by the attackers was protected with a four lower-case letter password, which matched the database's name. The second was Equifax's improper authentication practice of storing the application credentials in an unencrypted format in a file that could be shared. In his testimony for the U.S. House of Representatives investigation, Russ Ayres, Equifax's interim chief security officer, said "if Equifax had limited access to sensitive files across its systems, the attackers may not have found the stored application credentials used to access sensitive databases outside the ACIS environment."
- *Least privilege principle*: Equifax also disregarded the least privilege principle in the design of ACIS. This principle restricts the rights and access of a user and system to only those needed to execute a task and thus limits the spread and potential impact of an attack. ACIS had excessive permissions to access data in other systems not required for its operations. In his testimony, Russ Ayres said: "ACIS only needed access to three databases to function, but it was unnecessarily connected [and had access rights] to many more," thus confirming that Equifax disregarded the least privilege principle.

Phase 6: Command and Control

In this phase, the attackers create a command-and-control channel that enables them to control the victim's systems. The attackers were able to establish control over ACIS and other databases in the Equifax network because the intrusion detection and prevention systems (IDS/IPS) failed to identify and block them. The technical reason for this failure was that the SSL certificates necessary to analyze the encrypted network traffic entering and leaving Equifax's systems had expired. We provide more information on the causes of this failure below when we discuss the shortcomings in Equifax's hierarchical safety control structure.

Phase 7: Actions on Objectives

In this final phase of an attack, intruders harvest and exfiltrate unencrypted sensitive data. We identified three safety mechanisms that were not present in Equifax's systems and could have stopped the attack:

- *Encryption*: Proper encryption of data and effective management of encryption

19 For an overview of security and privacy architecture principles, see Mardjan, M. and Jahan, A., *Open Security and Privacy Reference Architecture*, Business Management Support Foundation, The Netherlands, 2021, available at https://security-and-privacy-reference-architecture.readthedocs.io/en/latest/.

keys can protect the confidentiality and integrity of data even when attackers obtain unauthorized access to computer systems. If the sensitive and personal identifiable information stored in the Equifax databases had been encrypted with the effective management of encryption keys, the attack's consequences would have been minimized or even nonexistent. We hypothesize that Equifax made a conscious architectural decision not to encrypt its data because none of the systems impacted by the attack employed encryption. Moreover, since ACIS was subject to the Payment Card Industry Data Security Standard (PCI DSS), at least credit cardholder data should have been protected. Later, we describe the reasons why Equifax failed to make ACIS PCI DSS-compliant.

- *Limit the data retained*: In designing its systems, Equifax failed to ensure that only necessary data was retained. Graeme Payne, formerly senior vice president and chief information officer for Global Corporate Platforms at Equifax, told us: "there was another factor that did not get a lot of coverage in the incident report … was it necessary to have that much data on these systems at all?" A similar pattern of collecting and storing customer information that was not required to make a purchase or a return (e.g., driver's license number) led to the broader exposure of customer information during the attack on TJX in 2006.[20]
- *Data loss prevention*: The third missing safety mechanism in Equifax's systems was data loss prevention (DLP), which could have detected and blocked the bulk transfer of sensitive data outside of the network. We estimate that the attackers stole at least 14 Gb of data they had harvested from Equifax's databases during the 76 days they remained undetected. That Equifax did not have a DLP system is surprising because requirement A3.2.6 of the Payment Card Industry Data Security Standard recommends the use of such a mechanism for detecting and preventing clear-text payment card numbers from leaving the controlled environment via unauthorized channels.[21]

Those who attacked Equifax's systems succeeded at all seven of the phases described above. The safety constraints that should have been enforced through the system design and architecture, and (as described below) by the hierarchical safety control structure, did not exist or failed to prevent them.

Understanding the Legacy Nature of Equifax's Environment

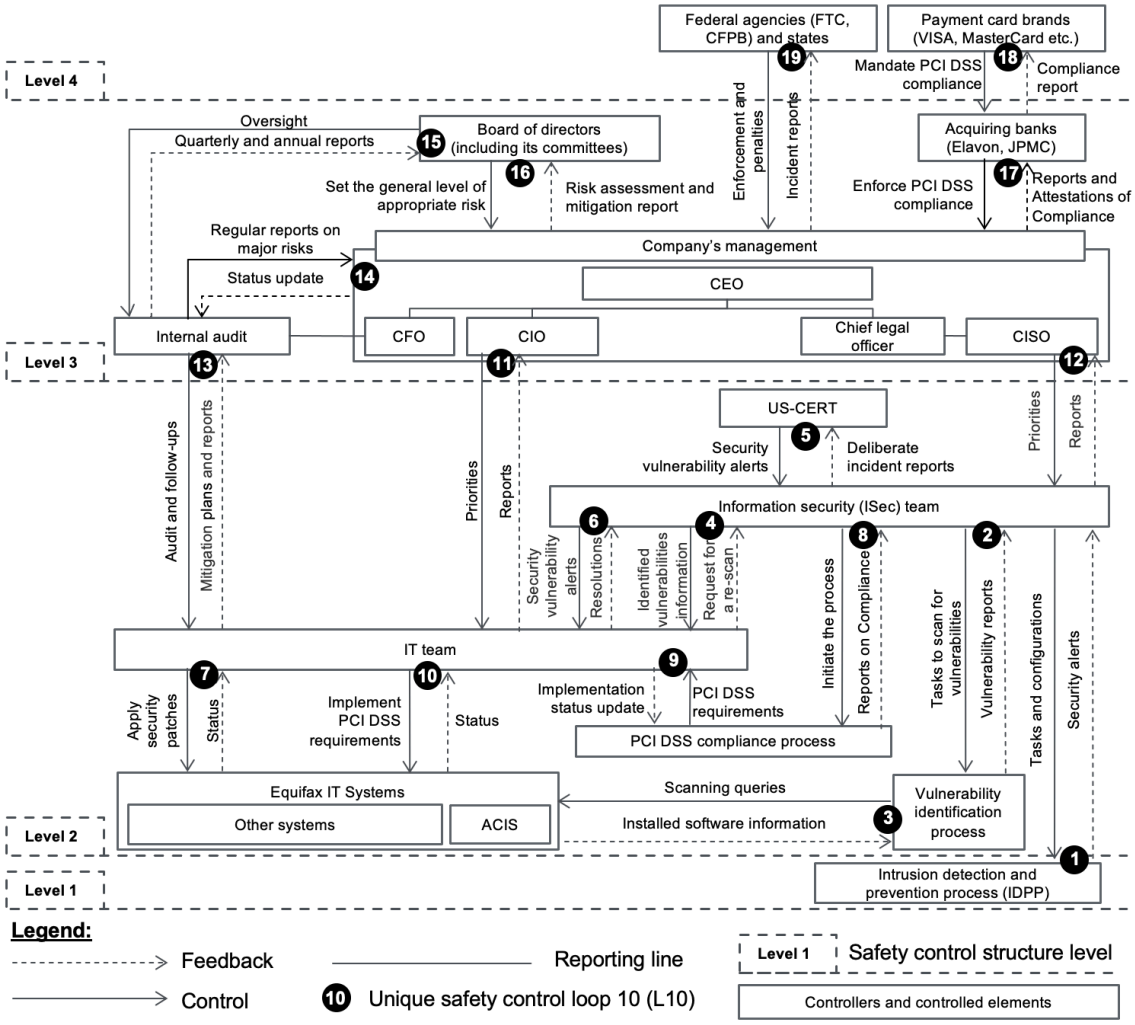
After reconstructing the timeline of the incident and identifying the safety constraints in place or missing, we needed to understand the impact of the absence of secure, design-enabled safety constraints. To gain this understanding, it was necessary to review our findings in the context of the environment and time frame over which Equifax's systems were developed and implemented. In his testimony to the House of Representatives investigation, Graeme Payne said "ACIS was the dispute and disclosure system that was built in … the late 1970s to address the requirements of the [Fair Credit Reporting Act]." The fact that the systems were created more than 40 years ago explains the lack of data encryption. However, the system's legacy nature could not excuse the lack of secure design controls because Sun Solaris, the operating system that hosts ACIS, can properly isolate individual systems and support the principle of least privilege. Moreover, Apache Struts 2 used in the web part of ACIS had been released in 2006. Therefore, the Equifax cybersecurity incident cannot be purely attributed to the legacy nature of ACIS.

The original system design and security architecture decisions were made when cyberattacks were almost nonexistent, and many of the protective measures now deemed

20 TJX Companies, a large U.S. retailer that operates more than 2,000 retail stores under brands such as Bob's Stores, HomeGoods, Marshalls, T.J. Maxx and A. J. Wright, discovered in December 2006 that it had suffered a massive computer breach on a portion of its network that handles credit card, debit card, check and merchandise transactions in the United States and abroad.

21 See *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version*, PCI Security Standards Council, available at https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

Figure 2: The Equifax Hierarchical Safety Control Structure



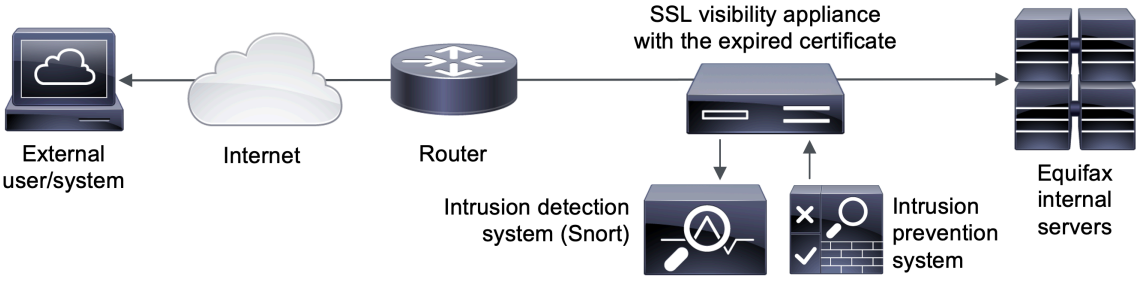
mandatory were not necessary. Since the late 1970s, however, the attack landscape has changed beyond all recognition, and Equifax should have introduced the essential safety constraints to address the evolving threats that have emerged since the initial development of the systems.

Identifying Shortcomings in Equifax's Hierarchical Safety Control Structure

Earlier, we identified the safety constraints that either failed or were missing from ACIS's design and Equifax's security architecture. We now describe the four-level hierarchical safety control structure employed by Equifax and use this structure to reveal the reasons for the failures:

- *Level 1*: Equifax's intrusion detection and prevention process (IDPP); the purpose of this process is to identify and block malicious activities in network traffic
- *Level 2*: Equifax's IT and information security (ISec) team that operates vulnerability identification and PCI DSS compliance processes
- *Level 3*: Equifax's management and board of directors that oversee the company's strategy and operations, including risk management

Figure 3: Most Likely Architecture of Equifax's IDS/IPS



- *Level 4*: Federal agencies (Federal Trade Commission and Consumer Financial Protection Bureau) and the U.S. states that have enforcement authority over the CRAs, and the payment card brands that enforce compliance with PCI DSS.

Figure 2 shows the 19 unique safety control loops (referred to below as L1, L2, … L19) that span across the four levels of the safety control structure. Below, we analyze the roles that those control loops played in the incident and the reasons for their failure.

Level 1: Equifax Intrusion Detection and Prevention Process

Control Loop L1 is Equifax's intrusion detection and prevention process (IDPP), which monitors and analyzes inbound and outbound internet traffic, and identifies and block malicious activities within the company's systems, including ACIS. The process is powered by the intrusion detection and prevention system (IDS/IPS) and operated by the ISec team. Figure 3 depicts what we believe is the most likely architecture of IDS/IPS. This architecture includes an intrusion detection component powered by an open source traffic analyzer called Snort, which identifies suspicious activities in the network traffic and prohibits them or raises an alert. The architecture also includes an SSL visibility appliance, which intercepts traffic, decrypts it, analyzes it and then re-encrypts it, and passes the traffic either to servers in case of inbound traffic or to the internet for outbound traffic.

However, SSL certificates installed in the visibility appliance and necessary to decrypt traffic had expired in November 2016. As a consequence, IDS/IPS could not analyze traffic and all the traffic passed through without any checks. On March 14, 2017, the ISec team installed a Snort rule on IDS/IPS coded to detect Apache Struts 2 exploitation attempts but continued to rely on IDS/IPS's protective capability. However, IDS/IPS was not functioning because of expired certificates.

The failure of Control Loop L1 was caused by two major factors. The first was Equifax's manual and error-prone process for tracking and updating the several hundred SSL certificates. Equifax had recognized that this was a problem and had begun to deploy an automated SSL certification management tool in 2016 but had not completed the deployment before the cybersecurity incident. The second factor was the lack of alerts to the ISec team that IDS/IPS was nonoperational for almost nine months (until July 29, 2017). The lack of warnings was a consequence of the system being set to allow traffic to bypass IDS/IPS if the visibility appliance failed to decrypt it.

Level 2: Equifax's IT and Information Security (ISec) Teams

The ISec team's objectives are to identify, notify and remediate vulnerabilities through Control Loops L2 to L7 and ensure compliance with PCI DSS through Loops L8, L9 and L10.

Shortcomings in Identifying Vulnerabilities. In Control Loops L2 and L3, vulnerability scans of

Equifax's systems are performed and any issues reported to the ISec team for remediation. After learning about the vulnerability in Apache Struts 2, the ISec team scanned all systems exposed to the internet using an unspecified scanner and the McAfee Vulnerability Manager to determine their vulnerability status. However, as stated in the U.S. House of Representatives data breach report, because "the scan was on the root directory, not the subdirectory where the Apache Struts was listed," the scan failed to identify the Apache Struts 2 CVE-2017-5638 vulnerability in ACIS. The primary cause of this failure was that the team had a limited understanding of how Apache Struts 2 works and that the two different scanners produced false-negative results. As a result, the IT team was not informed of the vulnerability in ACIS (Control Loop L4). The fact that the IT and ISec teams rarely collaborated further contributed to the ineffective flow of information between them.

Shortcomings in Notifying Vulnerabilities. Control Loops L5 and L6 provide another safety mechanism for the ISec team to alert the IT team about recent critical vulnerabilities in software systems. The ISec team receives security alerts from US-CERT (Control Loop L5) and disseminates messages about the alerts to more than 400 recipients across the organization, including IT team members (Control Loop L6). The investigation revealed that the ISec team received an alert from US-CERT on March 8, 2017 (i.e., well before the cybersecurity incident on May 13, 2017) about the Apache Struts 2 vulnerability. However, Control Loop L6 failed to prevent the incident because the ACIS operator did not receive the alert because the operator was not on the recipient list. In his testimony to the Senate Banking Committee, Equifax's former CEO also identified a failure of a senior vice president, whose team was responsible for ACIS, to inform the team members about the vulnerability in Apache Struts 2, which he was made aware of through the alert received from the ISec team.[22] However, we argue that the overall design of this control loop was error prone. It relied on the unrealistic assumption that managers—the primary recipients of vulnerability alerts—can and will correlate vulnerabilities with the versions and types of software systems used by their teams and demand that they are patched.

Shortcomings in Remediating Vulnerabilities. The objective of Control Loop L7 is to promptly patch Equifax's IT systems to ensure that their components do not contain publicly known security vulnerabilities. At the time of the incident, however, the patching process was reactive and relied on vulnerability scanners and notifications. When both of those mechanisms failed, the patching process was not triggered for the Apache Struts 2 vulnerability in ACIS, thus leaving the system vulnerable. We conclude that the reactive design of the patching process caused the failure of Control Loop L7.

Interestingly, the internal audit conducted in October 2015 of Equifax's configuration and patch management recommended that the company implement a proactive patching process. Management responded with an action plan, with an estimated completion date of December 31, 2016. However, the upgrade was not a priority for the IT team and had not been completed by May 2017 when the cybersecurity incident began.

Another significant finding was that the contractual patching requirements for the third party that operated ACIS contradicted Equifax's patch management policy. For instance, The Complaint revealed that the third party had a contractual obligation to apply patches to ACIS within six months, thus breaching Equifax's policy to patch critical vulnerabilities within 48 hours. The discrepancy between policy requirements and the procedures for complying with them remains a challenge for many organizations. In his research on employee compliance with cybersecurity policies, Cram highlighted that "employees are busy with their job responsibilities. Many are happy to say they understand the policy even though they have never read it."[23] The Equifax cybersecurity incident shows that such gaps can result in costly data breaches.

Shortcomings in Ensuring PCI DSS Compliance. The objective of Control Loops L8, L9 and L10 is to ensure that ACIS complies

22 "Former Equifax CEO testifies before Senate Banking Committee," PBS NewsHour, October 4, 2017, available at https://www.youtube.com/watch?v=11Ft3Ts3mfY.

23 For the in-depth analysis of practices for promoting employee compliance with cybersecurity policies, see Cram, W. A., Proudfoot, J. G. and D'Arcy, J. "Maximizing Employee Compliance with Cybersecurity Policies," *MIS Quarterly Executive* (19:3), September 2020, pp. 183-198.

with PCI DSS. This is necessary because ACIS stores credit card payment details, and Equifax is classified as a Level 1 merchant since it processes more than 6 million credit card transactions per year. The post-incident PCI DSS forensic report revealed that ACIS failed all 12 requirement categories because PCI DSS compliance was not a priority for the IT and ISec teams. In his testimony to the U.S. House of Representatives investigation, Equifax's former chief information security officer (CISO) stated, "the PCI preparation started about a year before [the incident but] … the plan fell behind, and these items did not get addressed." We later discuss the factors that led to Equifax's management failing to prioritize ACIS PCI DSS compliance for the IT and ISec teams.

Level 3: Equifax's Management and Board of Directors

We now analyze the roles that Equifax's management, internal audit, the board of directors and the acquiring banks[24] played in prioritizing the work of the IT and ISec teams, and how Control Loops L11 to L17 contributed to the failure of the safety controls at Level 2.

Management Shortcomings. The company's management is responsible for setting priorities for the IT and ISec teams through Control Loops L11 and L12. However, management failed to do this, even though it was aware of the deficiencies in Level 2 safety control loops. First, management was aware of the patching process deficiencies but failed to prioritize the upgrading of the patching system despite the earlier commitment to do so. Second, management knew the risks of operating Equifax's IT systems on the legacy Sun servers and, in 2015, started their migration into a new data center. However, in his testimony Graeme Payne said that the initiative was "enduring multiple delays as the company prioritized the completion of other initiatives." Third, management failed to prioritize the deployment of an automated SSL certificates management system, thus keeping the SSL update process manual and error prone. Finally, management knew that ACIS must be PCI DSS-compliant. Instead of prioritizing these activities to the ISec and IT teams, management deliberately excluded ACIS and Automated Credit Report On-line (ACRO), Equifax's primary credit reporting database, from the compliance scope, as they could not meet PCI DSS requirements.

Moreover, as recorded in The Complaint, multiple Reports on Compliance (ROCs) and Attestations of Compliance (AOCs) filed by Equifax "contained false and misleading information." As a result, the IT and ISec teams did not receive appropriate prioritization from management (Control Loops L11 and L12), and ACIS remained noncompliant with PCI DSS at the time of the cybersecurity incident.

Equifax's management also failed to establish effective collaboration between the IT and ISec teams, which led to an accountability and communication gap. The House of Representatives report highlighted that the reporting structure created a siloed environment where "information rarely flowed from one group to the other. Collaboration between IT and Security mostly occurred when required." Before the incident, Equifax's CIO reported to the CEO, while the chief security officer (CSO) reported to the chief legal officer (CLO). Therefore, the CSO was not considered part of the senior leadership team and often was not invited to the CEO's quarterly senior leadership team meetings, where the CIO was always present. After the incident, the company established the chief information security officer's role, reporting to the CEO, thus ensuring a productive security approach. It is interesting to note that the lack of cybersecurity executive leadership was a significant contributor to the successful attack on TJX in 2007, but this lesson had still not been learned by many companies almost a decade later.

Internal Audit Shortcomings. Control Loops L13, L14 and L15 form a control mechanism operated by Equifax's internal audit team to assess the state of the Level 2 safety control loops and the associated risks. As mentioned earlier, and included in the House of Representatives report, an internal audit had identified that "current patch and configuration management controls are not adequately designed." Even though IT leadership had formally committed to address this issue by December 31, 2016, the patching process remained deficient at the time of the incident, and the internal audit team neither followed up nor reaudited to confirm that the

24 An acquiring bank is a bank or financial institution that processes credit or debit card payments on behalf of a merchant.

management commitment had been executed (control L14). Moreover, Control Loop L15, where the board oversees the work of the internal audit team, also failed.

Equifax's *Notice of 2017 Annual Meeting* (The Notice)[25] provides the reason for the failure of Control Loop L15. At the time, internal audit was overseen by the board of directors' audit committee through quarterly and annual reporting to the full board, with the committee's objective being holistically overseeing risk management at Equifax. However, cybersecurity-related risks were not in the scope of the board's audit committee but were the responsibility of "[the Technology committee, which] focuses on technology-related risks and opportunities, including data security." Our hypothesis is that this explains the gap in the board's cybersecurity risk oversight. Confirmation of this hypothesis is contained in the Consent Order issued by Multi-State Regulatory Agencies in June 2018[26] in response to the incident. The Consent Order required that "within 30 days from the effective date of this Order, the Board or Audit Committee shall improve the oversight of the Audit function."

Board-Level Shortcomings. Equifax's board of directors should have played a critical role in setting and monitoring the company's overall risk appetite through Control Loop L16. The Notice confirms that Equifax's board of directors was responsible for establishing the company's general risk appetite level, including data security risks. We argue that Control Loop L16 failed to fulfill its objective to establish an appropriate risk level because of three factors. First, The Notice states that the overall incident-related expenses were between $1.24 billion and $1.36 billion (approximately 35% of Equifax's annual revenue), which cannot be called an "acceptable risk level" for any enterprise. Second, the board did not adjust the acceptable risk level based on previous data breaches at the company in 2010 and between 2012 and 2017. Third, executive compensation rules approved by the board were focused entirely on business growth, which, as recorded in The Complaint, resulted in "motivating them [executives] to prioritize revenue above all other considerations, including information security." These factors meant that Equifax's board of directors failed to set an acceptable risk threshold and prioritized growth without setting limits on cybersecurity risk. As a result, the company assigned a low priority to establishing and maintaining safety control mechanisms.

Shortcomings at Acquiring Banks. Acquiring banks (acquirers) play a significant role in enforcing credit card merchants' compliance with PCI DSS. Merchants pay acquirers to accept credit card payments, and acquirers are obliged to ensure that their merchants are PCI DSS-compliant through contractual requirements. Equifax partnered with two acquirers, JP Morgan Chase and Elavon, which failed to impose PCI DSS compliance requirements on Equifax as part of Control Loop L17.

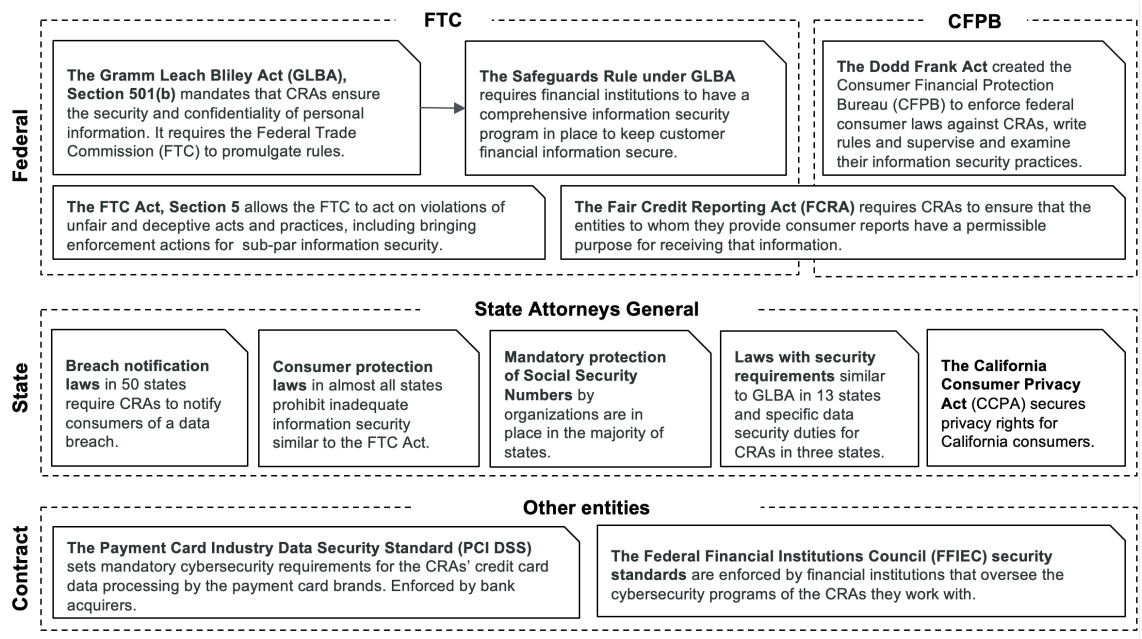
We identified three reasons for the failure of Control Loop L17. First, there was a conflict of interest between the acquirers' PCI DSS enforcement duty and their desire to retain their revenue-generating customers. Moreover, PCI DSS compliance is neither required by federal law in the United States nor by individual state laws (with the exception of Nevada). Second, it was problematic for the acquirers to determine merchants' status of PCI DSS compliance. The Equifax case revealed that the complexity of the IT systems and their integrations allowed the company to misrepresent the genuine compliance status in its attestations. Third, the acquirers were not empowered to perform technical validations or verifications of merchants' compliance but had to rely on the merchants' AOCs, supported by the ROCs[27] prepared by a qualified security assessor (QSA) hired by the merchant. But, as noted above, ACIS was explicitly excluded from the security assessment, thus was not reported in any AOC or ROC. In short, though acquirers are held accountable for their merchants' compliance, they rely on verification instruments that cannot guarantee proper validations. In summary, Control Loops L11 to L17 failed to meet their objectives of prioritizing the work of the IT and ISec teams to protect the company and achieve PCI DSS compliance.

25 *Notice of 2017 Annual Meeting and Proxy Statement*, Equifax, March 24, 2017, available at https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2017-proxy-statement.pdf.

26 The full text of the Consent Order is available at https://dbf.georgia.gov/document/publication/equifax-final-consent-order-dated-6-25-2018/download.

27 ROCs and AOCs are mandatory for Level 1 merchants such as Equifax.

Figure 4: The CRAs' Regulatory Landscape



Level 4: Federal Agencies and State Enforcement Authorities

Level 4 of the control structure includes two safety control loops: L18, for enforcing PCI DSS compliance by the payment card brands, and L19, for enforcing the federal and state regulations governing CRAs, including Equifax.

Shortcomings of Payment Card Brands' Enforcement of PCI DSS Compliance. Payment card brands play an essential role in enforcing PCI DSS compliance through Control Loop L18. However, as mentioned earlier, compliance and its comprehensiveness are not guaranteed. The failure of the payment card brands to ensure Equifax's compliance with PCI DSS was not unique, and the unsatisfactory level of merchants' compliance with PCI DSS had been known for more than a decade. Salim and Madnick identified that payment card brands failed to ensure TJX's compliance with PCI DSS and confirmed that "the lack of full compliance with PCI DSS also contributed to the cyberattack."[28] In addition, Verizon reported that, though the percentage of merchants fully compliant with PCI DSS had increased since 2004, it had reached a mere 55.4% in 2016 and dropped to 36.7% in 2018.[29] We conclude that the design of Control Loop L18 was error prone because it relied on an acquirer-driven enforcement mechanism that failed to achieve its objectives and was not supported by any law.

Shortcomings of Federal and State Regulators. Equifax and other CRAs are subject to various regulations and data security obligations imposed by CRAs' partners through their contracts. An overview of the CRAs' regulatory landscape is shown in Figure 4. The three primary federal laws regulating CRAs are The Fair Credit Reporting Act (FCRA), the Financial Services Modernization Act of 1999, called the Gramm-Leach-Bliley Act (GLBA), and the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). Those regulations are mainly enforced by the Federal Trade Commission (FTC) in accordance with the Federal Trade Commission Act and the Safeguard Rule under GLBA, and the Consumer Financial Protection Bureau (CFPB). CRAs are also subject to multiple state regulations enforced by State Attorneys General that aim to protect consumers' personal information. All

28 Salim, H. and Madnick, S., op. cit., September 2014.

29 2019 *Payment Security Report*, Verizon, 2019.

U.S. states have data breach laws that require CRAs to notify consumers of a data breach, and almost all states have strong consumer protection laws that prohibit unfair and deceptive acts and practices similar to the Federal Trade Commission Act. As emphasized earlier, CRAs also need to be PCI DSS-compliant and comply with the security requirements of their partners—financial institutions that have legal requirements specified by the Federal Financial Institutions Council (FFIEC) and enforced by federal regulators.

Control Loop L19 was supposed to ensure that Equifax complied with the federal and state regulations described above but failed to do this for three reasons. First, both the FTC and the CFPB lacked the legal basis for taking proactive enforcement actions. Second, the FTC did not have supervisory authority to examine a CRA's compliance. Third, the CFPB did not proactively examine CRAs because the outcomes of any examination would be limited to recommendations and would not result in enforcement actions.

Although the FTC, CFPB and State Attorneys General lacked the ability to proactively carry out data security examinations, they took massive enforcement actions after the Equifax cybersecurity incident. Those actions led to more than 60 government investigations from federal agencies and State Attorneys General and resulted in The Settlement, which required Equifax to pay at least $575 million and up to $700 million.

In summary, we conclude that the root causes of the Equifax cybersecurity incident were the lack of multiple protection mechanisms and systematic failures of the existing safety control elements at all four levels of the company's hierarchical safety control structure. The designs of most control elements in Equifax's safety structure were subpar; they were based on invalid assumptions and were not supported by controls at higher levels of the hierarchy. Most parts of the safety control structure contributed in some way to the propagation of the cybersecurity incident and thus needed to be improved. Regrettably, the shortcomings found at Equifax are not uncommon, as confirmed by analyses of other major cybersecurity incidents.

Recommendations for Strengthening Cybersecurity

Based on our analysis of the shortcomings found in Equifax's cybersecurity defenses, we provide 11 recommendations for strengthening an organization's safety control structure and reducing the probability of future catastrophic cybersecurity incidents. These recommendations are grouped under three headings—building in-depth defenses into IT systems (four recommendations); embedding cybersecurity practices in the organization (three recommendations); and ensuring the board prioritizes cybersecurity (four recommendations).

Recommendations for Building In-Depth Defenses into IT Systems

The Equifax incident showed that shortcomings in safety control mechanisms played a key role in making the attack successful. Therefore, organizations should build "defense in depth" by layering security mechanisms in order to increase the difficulty of an attack. Below we provided four recommendations based on the learnings from the Equifax incident.

1. Limit Sensitive Data Stored in the Systems. The storage of sensitive data should be limited to only the information needed to provide a service. Moreover, this data should not be retained beyond the time necessary to provide the service. The data should then be deleted, anonymized or aggregated for statistical purposes. There is a common management assumption that "data is gold" and should never be discarded. But that assumption should be balanced by the rarely stated fact: "excessive data is a big risk." The elimination of unnecessary sensitive data significantly reduces the value for attackers and makes it easier to protect the data. Nobody can steal what you do not have.

2. Embed Security into Software Design and Development. Embedding security into software design and development will enable organizations to address security vulnerabilities and mitigate security flaws earlier in the software lifecycle. It is not possible to write flawless software code, so software should be designed following secure design principles (e.g., isolation, the principle of least privilege, data encryption).

Software development should make use of secure development frameworks, and include design reviews, automated testing tools and penetration tests throughout the development cycle. Until fairly recently, cyberattacks were rare and did not attract much attention. The Equifax case shows that companies are not yet prioritizing adjustments of their software development practices to address the new security risks.

3. Protect Systems in Operation from Attacks. The vulnerability in Apache Struts 2 is just one of more than 18,000 vulnerabilities discovered in software systems every year, confirming that it is practically impossible to find and remediate all software "bugs" that make systems vulnerable to cyberattacks. Organizations should therefore limit the exposure of security vulnerabilities to attackers and protect software systems from the exploitation of such vulnerabilities. In a blog post,[30] Truta reported that the majority of breaches in 2019 involved unpatched vulnerabilities, and the Equifax incident emphasizes the importance of having proactive security patching prioritized toward high-risk vulnerabilities and high-value systems. There are several reasons why organizations don't do a better job at patching, including the difficulties of overcoming significant impediments such as the lack of an up-to-date software inventory, unsupported legacy systems and the risk that a system will break after being patched. Organizations also need to make trade-offs between spending resources on efforts to add new features that will provide business benefits and fixing flaws in features that superficially appear to be working fine.

4. Identify Attacks and Block Their Spread. The Equifax case shows that vulnerability detection mechanisms can be useless if they are misconfigured or are not managed properly. Companies making efforts to increase their cybersecurity by adding these mechanisms need to realize that the mechanisms are new and, in many cases, quite complex, and require professional operations throughout their life cycle. They cannot be treated as an "install-and-forget" solution. Furthermore, organizations tend to focus on "trying to keep the bad guys out" (i.e., on perimeter defense). They do too little in considering how to minimize damage if the bad guys do get in. Organizations should therefore augment intrusion detection and prevention (IDS/IPS) systems with data loss protection (DLP) systems to identify, monitor and potentially avert exfiltration of sensitive data after a successful attack. Deployed with an appropriate level of granularity, the combination of IDS/IPS and DLP systems can also identify and block the spread of attacks inside the network.

Building in-depth defenses requires a massive cross-functional effort that spans various teams, technologies and processes. Organizations should therefore ensure that cybersecurity practices are embedded throughout the business to ensure that protections are built into software and operations.

Recommendations for Embedding Cybersecurity Practices in the Organization

The Equifax incident highlights the importance of having cybersecurity as a shared goal throughout the organization; no single function can secure the organization holistically regardless of where it reports to. Based on our analysis of the Equifax incident, we provide three recommendations for embedding cybersecurity practices into the organization.

5. Ensure that Executive Leadership Has a Say in Cybersecurity Decisions. The organization's executive leadership must be in a position to take account of cybersecurity-related risks during decision-making, resource allocation and prioritization. Massive and publicly reported breaches, such as that suffered by Equifax, are relatively recent, so most senior executives neither have had personal experience of dealing with them nor fully appreciate the magnitude of risk that they entail. As a consequence, big risk decisions are essentially delegated to lower levels of the organization. The Equifax incident shows that the lack of direct involvement at the executive level leads to unbalanced managerial decisions and insufficient consideration of the magnitude of security risks.

6. Create a Shared Responsibility. A shared responsibility helps to contextually mitigate cybersecurity risks across the enterprise and

30 Truta, F. "60% of Breaches in 2019 Involved Unpatched Vulnerabilities," Security Boulevard, October 31, 2019, available at https://securityboulevard.com/2019/10/60-of-breaches-in-2019-involved-unpatched-vulnerabilities/.

embed cybersecurity into every part of the organization. Many organizations tend to view cybersecurity as a technical matter that is best left to technologists, but every part of the organization plays a role in either helping to defend the organization or aiding the attacker (usually unintentionally). Ideally, cybersecurity should be part of the performance objectives of all executives.

7. Foster Communication and Collaboration Between Security and IT Teams. Just as new security software is often "bolted on" after an incident, the security organization is often "bolted on," leading to poor communication and collaboration between the security and IT teams. Executive leadership must establish cybersecurity goals and objectives and clearly communicate them to the security and IT teams. Collaboration between the teams can be fostered through regular cross-functional discussions on the progress toward and challenges faced in executing cybersecurity objectives, and by using an informational dashboard. Providing transparency into shared goals and commonly agreed-upon metrics, and collaboration between the security and IT or software engineering functions of the organization, are prerequisites for addressing security problems earlier in the software development cycle and effectively responding to cyberattacks.

Following these three recommendations will ensure that organizations make prompt and sound cybersecurity decisions and foster strong cross-functional collaboration that will better protect them from cyberattacks and help them respond effectively to cybersecurity incidents.

Recommendations for Ensuring the Board Prioritizes Cybersecurity

We recommend that the board explicitly prioritizes cybersecurity to the organization's management and approves acceptable risk levels to secure the company's sustainable growth and profitability. In forming our four recommendations for ensuring that the board prioritizes cybersecurity, we reflected on the learnings from the Equifax cybersecurity incident and adjusted the principles set out in *Director's Handbook on Cyber-Risk Oversight*.[31]

8. Understand the Legal Implications of Cybersecurity Risks. As highlighted earlier, an organization can be subject to a growing number of regulations and laws relating to data security, with little or no coordination among rule makers and regulators. The board should therefore assess whether the organization has comprehensively evaluated and addressed cybersecurity risks from a legal perspective. We have already noted that massive cybersecurity threats are a relatively new phenomenon; it is likely that an organization's senior management and board members have not fully adjusted their practices to be prepared for the legal liabilities arising from such threats. It is best to do that before government regulators order organizations to do it. If boards fail to do that, their organizations face the threat of substantial financial fines, as in the case of Equifax.

9. Educate Board Members. To facilitate systematic discussions with management about cybersecurity risks, board members need to have a better understanding of the threats and vulnerabilities relevant to their organization, equivalent to the level of financial literacy needed by board members: "Not everyone on the board is an auditor, but everyone should be able to read a financial statement and understand the financial language of business."[32] According to Equifax's board skills matrix,[33] most members have expertise in international business and other topics, but only two of the 12 have any cybersecurity background.

10. Ensure that There Is an Organization-Wide Cybersecurity Risk Management Framework. The organization should have a cybersecurity risk framework that includes controls to mitigate cybersecurity risks across the enterprise and ensures oversight of those controls. The board should ensure that the organization establishes continuous cybersecurity maturity measurements based on a commonly agreed-upon security framework (e.g., NIST), which some companies set up as a dashboard so that executives and the board can see which areas are doing well (usually shown as "green") and which need attention ("red").

31 *Director's Handbook on Cyber-Risk Oversight*, National Association of Corporate Directors, 2020.

32 Ibid.

33 Equifax's board skills matrix is included in *Notice of 2018 Annual Meeting and Proxy Statement*, Equifax, 2018, available at https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2018-proxy-statement-web.pdf.

11. Fully Analyze and Communicate the Organization's Cybersecurity Risk Appetite. The board should analyze and communicate the cybersecurity risk appetite as part of risk management and decide which cybersecurity risks are acceptable and which must be avoided or mitigated. As discussed earlier, the lack of such analysis and a board-level mindset that tolerates risk can be perceived by the company's management as a green light for unlimited risks in pursuit of business growth. Readers of this article might have noticed that the words "was not a priority"[34] appeared 17 times! We sometimes refer to this as "semiconscious decision-making." That is, the decision to make something a low priority is (sometimes implicitly) taken without consciously realizing that "this decision might cost our company over $1 billion,[35] and I am OK with that." There is no evidence that an explicit decision to take on such a risk ever occurred at Equifax. But maybe it has in your organization.

Concluding Comments

The Cybersafety method allowed us to discover insights from the four levels of Equifax's safety control system and identify the failures and shortcomings of the safety control loops, both inside and outside the company, that contributed to the severity of the cybersecurity incident. The Cybersafety method also enabled us to formulate recommendations for holistically strengthening cybersecurity. The lessons provided by the Equifax case can be used by all types of organizations to identify the gaps in their cyberdefense systems, ranging from technical security controls to the regulatory compliance they may be subject to. In this article, we also introduced a new approach, using the Cyber Kill Chain framework, to identifying cyberhazards. The broader adoption of such a standardized approach will facilitate the comparison of future cybersecurity incidents analyzed by using the Cybersafety method. Applying the lessons from the Equifax case should, however, reduce the number of such incidents.

About the Authors

Ilya Kabanov

Ilya Kabanov (ikabanov@mit.edu) is a Research Affiliate in Cybersecurity at MIT Sloan, and Trust & Safety Cloud Manager at Google. He holds an MBA from MIT Sloan and a PhD in Information Technology & Operations Research from the Moscow Institute of Electronics and Mathematics (MIEM). Kabanov's research interests include the largest data breaches in history, software security assurance and privacy compliance at scale, and cryptographic strategies in the post-quantum era. He is an IEEE senior member and a certified information privacy professional.

Stuart Madnick

Stuart Madnick (smadnick@mit.edu) is the John Norris Maguire Professor of Information Technologies at the MIT Sloan School of Management. His PhD in computer science was awarded by MIT and he has been an MIT faculty member since 1972. In 2014, he founded Cybersecurity at MIT Sloan. He is an author of more than 400 books or articles, including Computer Security (1979). In addition to cybersecurity, his research includes big data, semantic connectivity and database technology. Madnick was a developer of IBM's VM/370 and Lockheed's DIALOG system. He has co-founded five high-tech firms and owns the 14th-century Langley Castle Hotel in England.

34 Sometimes worded as: "instead of prioritizing," "assigned a low priority," "failure to prioritize," "prioritized other initiatives."

35 The $1 billion figure was included in *Notice of 2020 Annual Meeting and Proxy Statement*, Equifax, 2020, available at https://s1.q4cdn.com/204858996/files/doc_financials/2020/ar/Broadridge-Courtesy-PDF.pdf.