EQUIFAX CASE STUDY

Team 7

Michael Schultz, Huy Tran, Jorge Vargas, Abdullah Shahid

George Mason University

IT 429 - Security Accreditation of Information Systems

Professor Hussna Azamy

November 02, 2025

Abstract (Michael, Abdullah)

Equifax suffered one of the largest data breaches ever in 2017, resulting in the personal information of over 145 million people (Srinivasan et al., 2019). In this paper, our group identifies and analyzes the causes of the breach and finds that the breach occurred due to negligent cybersecurity practices, and organizational mismanagement, and could've ultimately been avoided. The research investigates what led to the Equifax data breach and evaluates how internal choices made the incident worse while demonstrating methods to minimize organizational vulnerability. The analysis uses multiple frameworks and standards like NIST SP 800-37 (Risk Management Framework), NIST SP 800-53 (Security and Privacy Controls), NIST SP 800-61 (Incident Response), and NIST SP 800-34 (Contingency Planning) to identify the specific controls and processes that Equifax should have implemented. The Equifax breach was preventable through comprehensive governance, continuous monitoring, and risk management, and associated controls, as guided by these NIST protocols.

Introduction (Abdullah)

Equifax, one of the three major consumer credit reporting agencies in the United States, suffered a major data breach in 2017 that resulted in the loss and compromise of the data of over 145 million people (Srinivasan et al., 2019). The stolen data included personally identifiable information including Social Security, dates of birth and home addresses, exposing over 145 million people to identity theft and fraud risks. The security breach occurred because of internal system weaknesses which existed for an extended period. The incident exposed fundamental organizational weaknesses which extended beyond basic technical errors. The organization faced multiple security risks because its expired SSL certificates combined with non-existent asset inventory and fragmented organizational structure indicated weak governance and oversight at all levels. The breach established itself as one of the worst data breaches in American history because it demonstrated how weak corporate leadership and lack of accountability threaten information security and that organizations need to look to established frameworks for guidance, designate clear and proper responsibilities, maintain active security monitoring and lead their cybersecurity efforts proactively. Therefore, this paper will examine the specific NIST-aligned frameworks and security controls that, if properly implemented, would have prevented or significantly reduced the impact of the Equifax breach.

Summary of Incident (Michael)

In 2017, Equifax suffered one of the largest data breaches in history. The breach exposed the data of over 145 million people, including personally identifiable information (PII) like social security numbers and addresses. Equifax had been warned on multiple occasions about the vulnerability in the Apache Strut software months prior to the breach by both internal audits and the Department of Homeland Security. Despite these warnings, Equifax failed to implement the available security patch, in violation of their own policies regarding the implementation of critical updates within 48 hours. The breach occurred on May 12th, however Equifax was unaware of the attack for 76 days, until July 29th; when they updated their SSL certificate. Equifax then failed to disclose the data breach for an additional six weeks.

In further investigation, it was found that Equifax’s organizational structure created an accountability gap and divided responsibility. It was discovered that Equifax lacked an up-to-date component inventory of their IT assets. Additionally, at the time of the breach, Equifax spent less than one percent of its operating revenue on cybersecurity infrastructure. Rather than acknowledge institutional negligence, senior management attempted to blame a single engineer for failing to patch the vulnerability. In the ensuing fallout, the CEO Richard Smith resigned, and a class action lawsuit against Equifax was launched.

How does Equifax’s business model work? Who is the customer, and what is the product? (Michael, Abdullah)

The business model of Equifax depends on data analysis to generate money from consumer information through financial solutions and analytical products. The company obtains financial and personal data through its access to banks and credit card companies and public records and lender databases (Srinivasan, Pitcher, & Goldberg, 2019). The company processes raw data to create credit reports and identity-verification tools and predictive analytics which organizations use for lending and employment and housing selection. The company earns money through data subscription services and analytics platform sales and licensing agreements with corporate and government organizations (Srinivasan et al., 2019).

The model separates consumers from customers through separate functions. The data subjects who make up Equifax's product base include consumers whose credit records and personal information serve as the basis for their products. The service recipients who pay for Equifax's products include banks and landlords and insurance providers and employers who need credit reports and risk assessment data (Srinivasan et al., 2019). The company generates profits through consumer data collection while maintaining financial ties with institutional clients who require dependable credit information.

The organization needed to classify sensitive personally identifiable information (PII) as high impact because Equifax depends on this data for its product operations (National Institute of Standards and Technology, 2004). The Categorize step of NIST SP 800-37 Risk Management Framework requires agencies to determine information system security impact levels at low, moderate, or high levels based on potential damage to operations and individual data when confidentiality or integrity or availability is compromised (Joint Task Force Transformation Initiative, 2018). The proper classification process would have shown that consumer credit data from Equifax needed maximum protection through ongoing monitoring. NIST SP 800-53 requires high-impact systems to implement additional security measures which include continuous vulnerability scanning and configuration management and flaw remediation (National Institute of Standards and Technology, 2020). The organization would have detected security vulnerabilities earlier and minimized breach severity through consistent framework implementation (Joint Task Force Transformation Initiative, 2018; National Institute of Standards and Technology, 2020).

Was Equifax lax or unlucky to be cyber-breached in this way? (Michael, Huy)

Equifax was not unlucky. Equifax was absolutely lax. There were many points at which the vulnerability could've been patched, the breach could've been detected, or the public could've been informed earlier. Equifax failed to adhere to their own cybersecurity policies, failed to maintain their systems appropriately, and failed to assign clear and proper oversight or designate responsibility.

According to NIST SP 800-53, organizations should implement continuous and systematic processes that maintain the security of their systems. Some instances of that include controls like SI-2 (Flaw Remediation) that requires timely identification and patching of known vulnerabilities, and CM-2 (Baseline Configuration), which requires the systems to be securely configured and deviations documented (National Institute of Standards and Technology, 2020). Had Equifax followed these standards, the patch would have been applied, and SSL certificates would have been updated regularly.

Additionally, per NIST SP 800 37, in the Assess Phase and the Monitor Phase, organizations must continuously evaluate the effectiveness of controls, monitor for risks, and evaluate the overall security posture (Joint Task Force Transformation Initiative, 2018). The Apache Struts vulnerability was not only known about beforehand, and had a patch available, but Equifax had been given multiple warnings about it. The SSL certificates being expired prevent proper monitoring and were not updated for months after the breach, which could've been solved by routine processes that updated those certificates regularly. Equifax lacked continuous evaluation and monitoring of its security posture in accordance with NIST guidelines.

Equifax also ignored best practices from NIST SP 800 61 in developing incident response plans. There was no plan to detect, contain, and recover from the breach, nor were there clear roles and communication protocols for detection, response, or escalation (National Institute of Standards and Technology, 2025). Combined with the failures in patching and monitoring, there was a failure in being prepared for an incident and another result of systemic organizational neglect rather than bad luck.

Additionally, per NIST SP 800 37, in the Authorization Phase, leadership is responsible for ensuring that risk decisions are properly reviewed and approved, and that controls are maintained effectively (Joint Task Force Transformation Initiative, 2018). The leadership of Equifax failed in this responsibility, neglecting to have proper oversight and accountability, and effectively maintain the controls.

At so many points the attack could've been prevented or halted earlier. The actions of the company show a consistent pattern of neglect and lack of responsibility and proper data handling. The leadership failed to communicate, the executive officials failed to take proper responsibility, and to some extent, could not due to the terrible structure of the chains of command. With no incident response plan, the response was reactive, ill-prepared, and disorganized, a trend in the case of Equifax. The breach was not a case of bad luck but an obvious outcome of lax policy and failed oversight.

Where would you assign accountability for the breach? (Michael, Abdullah)

Accountability for the Equifax breach should be shared between them all because there were so many failures at so many levels - however the greatest responsibility for the breach falls to the senior management and the Board of Directors. According to NIST SP 800 37 in the Authorize Phase, organizational leadership is responsible for reviewing and approving decisions regarding risk management, ensuring that the implemented security controls are effective and have continuous monitoring strategies in place, and maintaining oversight over the security posture of the organization (Joint Task Force Transformation Initiative, 2018). Senior management and the Board of Directors failed to meet these responsibilities. Senior management failed to provide proper oversight. They failed to heed the warnings from Homeland Security and their own internal auditors. They failed to ensure cybersecurity policies were being implemented and followed. Leadership neglected their duty to maintain continuous authorization of the organization's systems.

Per NIST SP 800-53, the PL-2 control (Systems and Communication Protection Planning) requires that leadership develop, publish and continuously update formal system security plans. Additionally, CA-6 (Security Authorization), mandates that management regularly reviews, reapproves, and continuously monitors the implementation of the system security plans (National Institute of Standards and Technology, 2020). The Equifax leadership; senior management and the Board of Directors, failed to do either. Had system security plans been implemented, properly authorized, updated and monitored, there would have been a structured process that ensured patches were applied, component inventories were updated, and certificates were not left to expire.

The technology security team also failed, because as IT professionals, they should've known better. They failed to follow the company policy of applying critical patches within 48 hours. They also failed to maintain SSL certificates, not only allowing them to expire, but neglecting to renew them for several months. These are basic preventable failures that any single person on the security team could've solved with their own initiative and common sense, even if it wasn't ordered by senior management.

The Board of Directors takes significant responsibility. Boards together with senior management have a legal and ethical responsibility to properly oversee cybersecurity as part of their professional obligations to safeguarding digital assets and consumer information (Edwards, 2019). While senior management failed to have proper oversight, the Equifax board of Directors created a siloed and ineffective command structure, which placed the legal executives in charge of technical functions, and failed to assign clear responsibilities to senior management. Poor communication and isolated, uncoordinated decision-making prevented critical information from reaching the right people.

Adhering to NIST guidance like NIST SP 800 37 promotes enterprise-wide coordination and shared accountability for security, by recognizing that cybersecurity is not a single department's task but a collective organizational responsibility and appropriately assigning that responsibility (Joint Task Force Transformation Initiative, 2018). The Board of Directors and senior executives did not establish proper cybersecurity standards, assign clear responsibility or roles, nor allocate enough funds for risk management and infrastructure even though they needed to protect consumer data. Overall, responsibility for the breach lies with the Board of Directors and senior management, as their failure to enforce NIST's prescribed oversight, authorization, and communication standards led directly to systemic weaknesses throughout the company. However, it was a cascading combination of failures that occurred at every role that made the breach possible and so catastrophic.

How would you characterize Equifax's response in the wake of the breach? (Huy)

We characterize Equifax's response as terribly executed, careless, and completely preventable. Using the NIST SP 800 - 61 Incident Response framework, we can see how Equifax's actions and response failed at every level. In the Preparation phase, Equifax lacked an effective incident response plan and proper leadership oversight. According to NIST SP 800-61, the Preparation phase involves establishing an incident-response policy, procedures, roles and responsibilities, and ensuring the organization is ready (National Institute of Standards and Technology, 2025). Equifax had a non-existent asset inventory and lax patching policies in place. Equifax lacked timely notification and escalation, as the CEO and board were not properly notified, nor was the issue escalated in time. The company waited six weeks to inform the public of the breach, which was unacceptable and against normal standards for breach notifications; in many states companies are required to notify the data owners without unreasonable delay (IT Governance USA, 2018).

During the Detection and Analysis phase, Equifax had been warned and was aware of the vulnerability, it had been detected, and yet Equifax failed to act on, remediate, or escalate the issue. Per NIST SP 600 61, in the Detection and Analysis phase, organizations must monitor for incidents, analyze alerts to determine whether an incident has occurred, assess its scope and impact, and prioritize response (National Institute of Standards and Technology, 2025). But Equifax's breach went undetected for 76 days, and when it was, Equifax did not act with urgency. Equifax did not detect the breach in a timely manner, nor did they respond to the breach in a manner that NIST guides.

In the Containment, Eradication, and Recovery phase, Equifax did not contain the threat in time, allowing attackers to exploit the system for months, and the recovery efforts were slow and poorly coordinated. NIST guides that organizations design their containment, eradication and recovery plans ahead of time, and act to minimize damage and downtime (National Institute of Standards and Technology, 2025).

Per NIST SP 800 61, in the Post-Incident Activity phase, organizations are supposed to review the incident, update policies and procedures according to lessons learned, and feed those improvements back into the Preparation phase, in order to reduce future occurrences, and improve future responses (National Institute of Standards and Technology, 2025). Instead, the CEO attempted to blame a single employee for not forwarding a patch notice, which was later overruled by the IT leadership. It was clear that Equifax was not looking to examine the incident, take accountability, and use the lessons learned to inform a better response. The delay in public disclosure and lack of clear accountability show poor, if any, post incident response handling. This shows that to the very end, Equifax leadership could not take responsibility, even though it was very clear there were many issues in the structure and leadership.

According to NIST SP 800-37, Equifax leadership should have ensured that the organization's security posture was continuously authorized and monitored, per the Authorize and Monitor phases. This includes reviewing and approving risk management decisions, ensuring that controls are effectively implemented, and maintaining ongoing oversight to detect vulnerabilities and emerging threats (Joint Task Force Transformation Initiative, 2018). However, Equifax failed to meet these standards: the leadership did not enforce accountability, authorize proper remediation measures, or monitor the company's exposure. Overall, we characterize Equifax’s response as a systemic failure that violates every established standard of incident response.

In your view, how should Equifax have prepared for the breach and the subsequent response? (Huy)

Equifax should have prepared for the breach by establishing a clear, accountable organizational structure. They needed to align IT and security together - where the CIO oversees the CSO, so that the leadership has the proper technical experience for the role, and aren’t reporting to an unrelated executive, like the CLO. To proactively manage risk, Equifax should have followed the Risk Management Framework, as outlined in NIST SP 800-37. In Phase 2 (the Select Phase) of RMF, controls are identified, and tailored, to be implemented in Phase 3 (the Implement Phase). This includes controls that ensure regular, proper patching, management of security certificates, and monitoring of the assets and systems (Joint Task Force Transformation Initiative, 2018). Equifax would have implemented a centralized and updated-to-date system component inventory of all the IT assets as part of the CM-8 System Component Inventory control. This ensures that Equifax always maintains an accurate and comprehensive list of all hardware, software, and network components that are managed securely and in order (National Institute of Standards and Technology, 2020), and can identify the vulnerable systems, unpatched systems, and expired certificates. Furthermore, in Phase 7 (the Monitor Phase), the regular, continuous monitoring of all the assets would detect threats and vulnerabilities as they emerge, and before they could be exploited (Joint Task Force Transformation Initiative, 2018). Had Equifax adhered to RMF, these steps in particular that they would have gone through would have reduced the likelihood and the impact of the breach.

In the aftermath of the breach, the subsequent response from Equifax’s senior management should’ve been to identify and take responsibility for the organizational failures that led to the lax security posture of the firm. Instead, they chose to blame a single security engineer. A well-prepared organization would’ve had a clear crisis response plan and would have a coordinated response that was clear and transparent, rather than trying to shift blame.

Equifax needed to have contingency plans that clearly define the roles, communication protocols, and recovery procedures to minimize operational disruption and data loss (National Institute of Standards and Technology, 2010).

Equifax should have structured its breach response according to the NIST SP 800-61 Computer Security Incident Handling Guide. As mentioned earlier, the company failed at every phase of the framework. In the Preparation Phase, they should have had a clear incident response plan, defined roles, and strong patch management. During Detection and Analysis, they should have acted on the vulnerability immediately and communicated promptly to regulators and affected consumers and in the Containment, Eradication, and Recovery phase Equifax needed to isolate the affected systems and acted quickly to restore operations. Finally, in the Post-Incident Activity phase, they should have focused on accountability and using lessons learned to strengthen policy and leadership oversight, rather than blaming a single engineer, or failing to communicate with the public (National Institute of Standards and Technology, 2025). Equifax should have followed these established frameworks and guides, which would have ensured a more transparent, coordinated, and responsible response.

Conclusion – Explain how the breach could have been avoided (Jorge)

At the organizational level, the Equifax breach occurred due to failures in oversight and proper governance, a lack of accountability and responsibility, and little investment into the cybersecurity infrastructure. Equifax spent less than 1% of its operating revenue on cybersecurity. The industry average spending was 8% in 2024 (IANS & Artico Search, 2024). Equifax significantly underinvested into their systems and security infrastructure. Executives without technical expertise were placed into leadership positions, which impacted communication, created misalignments in role functions, and impacted the decision-making processes. Equifax needed to have a clear chain of command that aligned the responsibilities of the executives with their expertise and ensure compliance from the top-down. With more accountability, security patches and certificate renewals would most likely not have been neglected. Following NIST SP 800-37, the Authorize Phase would require leadership to maintain continuous authorization and oversight of security controls, ensuring that risk decisions and remediation efforts were properly reviewed and approved. Additionally, controls such as PL-2 (System and Communications Protection Planning) and CA-6 (Security Authorization) would require senior management to develop, maintain, and regularly review formal system security plans to ensure compliance and accountability (Joint Task Force Transformation Initiative, 2018). Adherence to NIST SP 800-61 would also have required leadership to support organized incident-response capabilities and ensured that procedures on detection, escalation, and notification were clear before an incident happened (National Institute of Standards and Technology, 2025).

At the technical level, the Equifax breach could've been prevented had they implemented and adhered to a framework such as the Risk Management Framework and developed Information Security Continuous Monitoring (ISCM) strategies. During the process of the RMF, systems are categorized, controls are implemented and then everything is continuously monitored and assessed - which ensures that risks and threats are systematically identified and remediated (Joint Task Force Transformation Initiative, 2018; National Institute of Standards and Technology, 2004). The vulnerability that led to the breach would've been identified and patched throughout the process, or during continuous monitoring and remediation. The SSL certificates would not have left to expire and would have been renewed much sooner. Additionally, these issues would've been identified in POAMs, and clear responsibility would be assigned. The implementation of ICSM strategies would have also provided continuous monitoring and visibility into the networks (National Institute of Standards and Technology, 2011). The expiration of the SSL certificates and vulnerability in Apache Struts would've been caught and solved before they were exploited. Controls such as SI-2 (Flaw Remediation) and CM-2 (Baseline Configuration) from NIST SP 800-53 would address these types of technical failures by requiring timely identification and patching of vulnerabilities, regular maintenance of secure configurations, and documentation of any deviations (National Institute of Standards and Technology, 2020). NIST SP 800-61 complements these controls by requiring Detection and Analysis practices like monitoring, alert triage, and forensic readiness, all which would have improved Equifax's ability to detect the Apache Struts vulnerability quickly and actually analyze it (National Institute of Standards and Technology, 2025).

Equifax's lack of a comprehensive system component inventory directly contributed to the oversight of the system and the SSL certificates expiring. Implementing a Business Contingency Plan as according to NIST SP 800-34 would have prepared Equifax to properly respond to the breach, both during the breach and in the wake of the breach. In a BCP, roles and responsibilities during an incident are clearly defined, a system inventory is created, and policies and procedures are implemented that can be followed (National Institute of Standards and Technology, 2010). These procedures are tested regularly, and the system inventory is regularly reviewed and updated. This is also consistent with the implementation of a control from NIST SP 800 53; CM-8: System Component Inventory, which requires maintaining an accurate and up-to-date record of all assets to support monitoring and response (National Institute of Standards and Technology, 2020). Documentation and implementation of systematic processes would prove to be vital when identifying and patching vulnerabilities which is why SI-2 (Flaw Remediation) and CM-2 (Baseline Configuration) are so essential. Not only systematic processes but also the CA-6 (Security Authorization) and PL-2 (System and Communications Protection Planning) controls are critical in ensuring that oversight and formal security plans are continuously reviewed and updated (National Institute of Standards and Technology NIST, 2020). Guidance from NIST SP 800-61 would have established formal steps for containment and recovery, required lessons-learned reviews, and required updating of plans and POAMs so that the same failures would be less likely to repeat (National Institute of Standards and Technology, 2025). A properly implemented contingency plan, with a system inventory, would've ensured a better response and recovery from Equifax, and minimized the impact of the breach and the resulting data loss.

References

Edwards, B. P. (2019). *Cybersecurity oversight liability. 35 Georgia State University Law Review,* 663. https://scholars.law.unlv.edu/facpub/1220

IANS & Artico Search. (2024). *2024 Security Budget Benchmark Summary Report.* IANS Research. https://sf-cdn.iansresearch.com/sitefinity/docs/default-source/reports/ians-2024-security-budget-benchmark-summary-report.pdf?sfvrsn=6ac1b09a_1

IT Governance USA. (2018). *Data breach notification laws by state*. IT Governance. https://www.itgovernanceusa.com/data-breach-notification-laws

Joint Task Force Transformation Initiative. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST SP 800-37 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2004). *Standards for security categorization of federal information and information systems* (FIPS PUB 199). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.199

National Institute of Standards and Technology. (2010). Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-34r1

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2025). *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile* (NIST SP 800-61 Rev. 3). https://doi.org/10.6028/NIST.SP.800-61r3

National Institute of Standards and Technology. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations* (NIST SP 800-137). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-137

Srinivasan, S., Pitcher, Q., & Goldberg, J. S. (2019). *Data breach at Equifax*. Harvard Business School. Case No. 9-118-031

Team Members and Contributions

Group 7 Team Member	**Contribution**
Michael Schultz	Editing/formatting Summary/Q1, Q2, Q3, Abstract
Huy Tran	Q2, Q4, Q5 Research
Jorge	Conclusion Research References
Abdullah	Editing Abstract, Introduction, Q3, Q1 References