IY3501: Security Management Coursework

IY3501: Incident Report - Equifax Data Breach 2017

Candidate Number: 2411828

A report submitted in part fulfilment of the degree of

BSc (Hons) in Computer Science

Department of Computer Science
Royal Holloway, University of London

March 6, 2024

1 Executive Summary and Business Context

This document presents a detailed investigation into the Equifax data breach of 2017, a pivotal event that emphasised the paramount importance of data security in today's interconnected financial ecosystem. Equifax, incorporated in 1899, experienced a massive security lapse that compromised the personal information of over 140 million consumers and numerous businesses worldwide (Novak and Vilceanu, 2019). This breach not only highlighted the vulnerabilities within Equifax's data management systems but also underscored the systemic risks such incidents pose to financial stability and consumer trust globally.

Equifax's role as a leading credit reporting agency involves the collection and analysis of sensitive data—ranging from social security numbers to credit scores—for credit reporting, analytics, and scoring purposes (Lending Stream, 2024; Primoff and Kess, 2017). The integrity of this data is crucial not only for Equifax but for the entire financial market, as it influences lending decisions, risk management, and provides vital financial insights. With approximately 14,000 employees worldwide (Beske and Stallings, 1998), the company's operations span multiple countries, each with its unique regulatory standards and practices, thereby complicating the task of data protection.

The 2017 breach served as a stark reminder of the critical need for stringent security measures and the adherence to regulatory frameworks like the United States' Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA) (Aubuchon, 2020) (Bureau, 2022). These regulations are designed to safeguard consumer information, dictating the protocols that entities like Equifax must follow to protect sensitive data from unauthorised access and breaches.

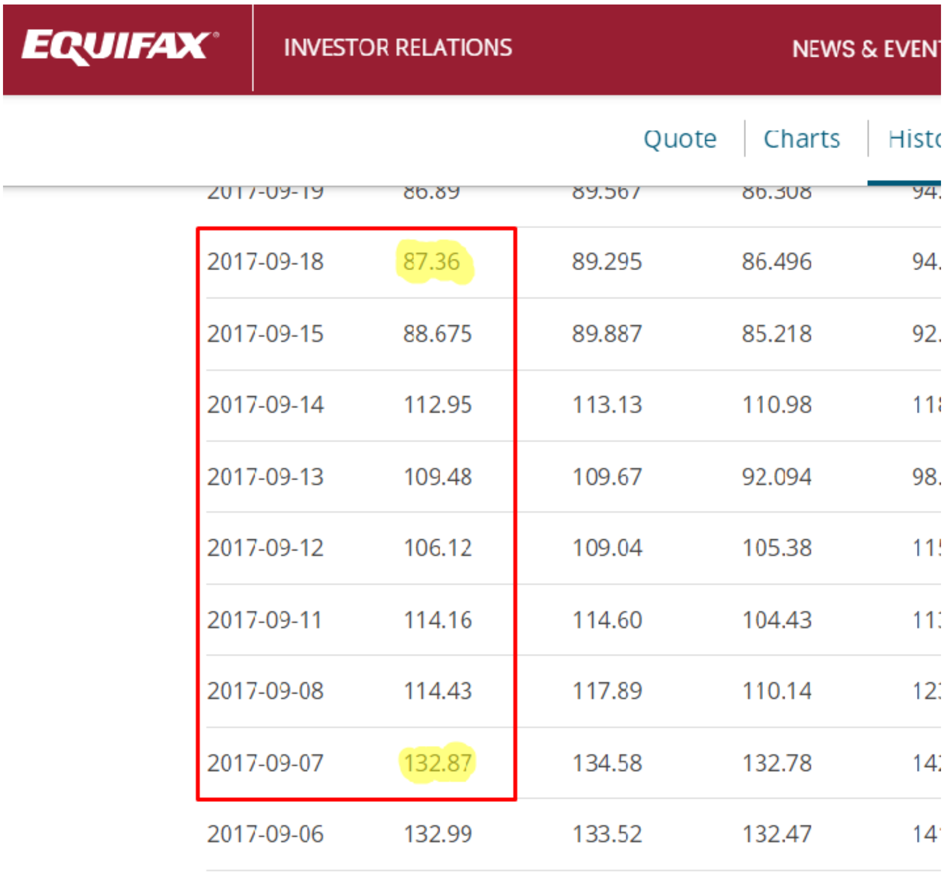
2 Aftermath & Novelty

The immediate aftermath of the security breach saw Equifax's stock price plummet, with a 15% drop on the first trading day post-disclosure and a total decline of nearly 36% within the week (LaCroix, 2020). **Figure 1** shows the sudden drop in the stock price of the Equifax shares moments after official disclosure of the data breach. Furthermore, not only did the stock price plummet but it also took just over a year for the share price of Equifax to recover; this can be seen very clearly in **Figure 2**.

Shortly after the data breach was announced, it was expected by multiple experts that identity theft cases within the nation would rise given the large scale nature of the breach. Eyes on popular dark web forums were constant, anticipating this data to be put on sale by attackers. This did not happen. Instead, this data was nowhere to be seen online, which resulted in law-enforcement agencies believing that the motivation behind this breach was not financial, rather it was cyber espionage (Staff, 2017). Fast forward to 10th February, after months of investigation and forensic analysis, 4 members of the Chinese Military were indicted with 9 charges related to the attack (Federal Bureau of Investigation, 2020).

What makes this security breach notably novel is the fact that the victims of this breach were not direct consumers of Equifax but individuals whose data was provided by other financial institutions for processing. This means that most of these individual were not even aware of the fact that their data would be a part of this breach (Thomas, 2019) (Equifax UK, 2024).

The Equifax data breach is easily one of the largest and most notable data breaches of all time evidenced by the amount of data that was leaked. Below is a bullet-point representation



2017-09-19	86.89	89.567	86.308	94.
2017-09-18	87.36	89.295	86.496	94.
2017-09-15	88.675	89.887	85.218	92.
2017-09-14	112.95	113.13	110.98	11
2017-09-13	109.48	109.67	92.094	98.
2017-09-12	106.12	109.04	105.38	11
2017-09-11	114.16	114.60	104.43	11
2017-09-08	114.43	117.89	110.14	12
2017-09-07	132.87	134.58	132.78	14
2017-09-06	132.99	133.52	132.47	14

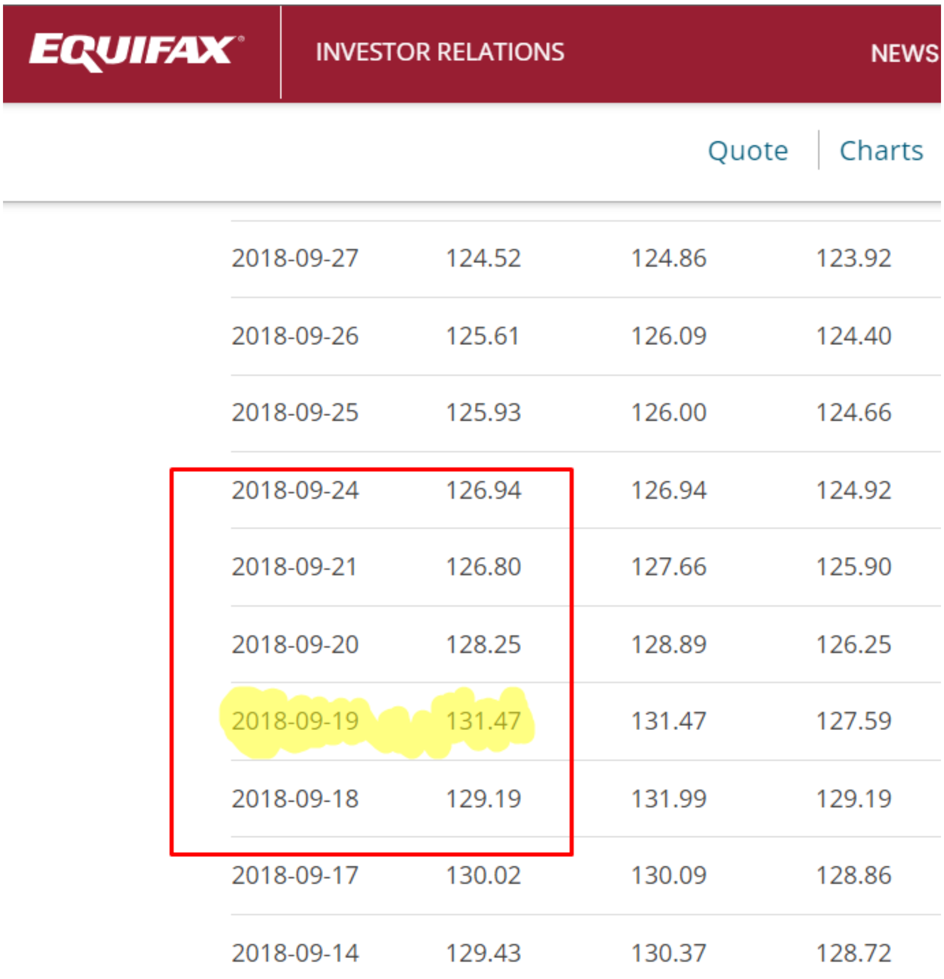
Figure 1: The stock plummet data as shown on the official Equifax investor website (Equifax, 2024)

of the amount of data that was leaked as reported by Equifax after they hired Mandiant - a cyber security company to conduct forensic analysis.

- **147 million** - Number of people who's data was breached (Federal Trade Commission, 2024).
- **209, 000** - Number credit card details breached (Electronic Privacy Information Center, 2017).
- **15.2 million** - Number of consumers from the UK who's data was breached (Equifax, 2017).
- **34** - Number of servers that were accessed by attackers during the breach (Bomey, 2020).

3 Timeline

As mentioned earlier, the security incident at Equifax was a result of an un-patched security flaw in the Apache Struts Framerwork (National Vulnerability Database (NVD), 2017). This security flaw introduces a remote code execution possibility when a user tries to conduct a file upload. More details on the specifics of the vulnerability and reproduction can be found on the official apache.org website (Lenart and Gielen, 2017). Additionally a GitHub repository named **struts-pwn** also goes over this (Elzanaty, 2017).



2018-09-27	124.52	124.86	123.92
2018-09-26	125.61	126.09	124.40
2018-09-25	125.93	126.00	124.66
2018-09-24	126.94	126.94	124.92
2018-09-21	126.80	127.66	125.90
2018-09-20	128.25	128.89	126.25
2018-09-19	131.47	131.47	127.59
2018-09-18	129.19	131.99	129.19
2018-09-17	130.02	130.09	128.86
2018-09-14	129.43	130.37	128.72

Figure 2: Stock price returning to 130 after year (Equifax, 2024)

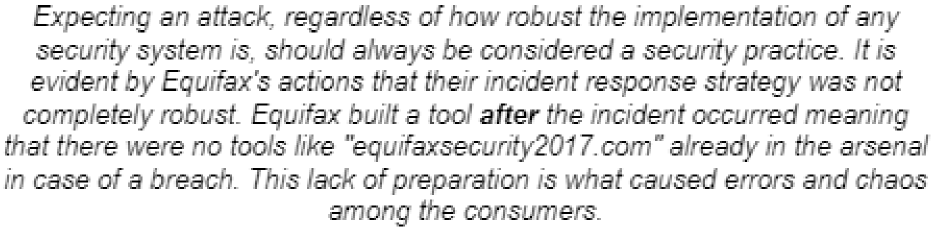
The vulnerability was found and patched by Apache on the 7th of March 2017 (The Apache Software Foundation, 2017) (Lenart and Gielen, 2017). This should have given enough time for Equifax and other companies using the Apache Struts Framework to fix the issue. However, this was not the case. On the 8th of March, Equifax along with TransUnion and Experian were notified of this vulnerability by United States Homeland Security (Electronic Privacy Information Center, 2017) and on 15th March 2017 Equifax even ran a vulnerability scanner to see if any instances of Apache Struts existed in their code base. The result of a scan was a false negative.

As a result of this, the vulnerability remained un-patched until it was exploited. Attacks on the Equifax's ACIS (Automated Consumer Interview System) started on the 12th of May up until the 29th of July when Equifax noticed suspicious activity associated with the portal (Goodin, 2017). This perhaps also gives us some information about **the lack of great monitoring systems** in place such that infiltrators remained in a system and **harvested data for over 75 days** without being noticed.

The next day, the 30th of July, Equifax observed further suspicious activity and took the web application offline. Three days later, the company hired a cyber security firm called Mandiant to conduct further, more meticulous security assessments and incident response (Equifax Ltd UK, 2017). This assessment demonstrated further understanding of the breach and a more accurate representation of exactly how much data was breached. After a complete assessment of the data breach, on the 7th of September Equifax officially disclosed information about the data breach and also created a domain that allowed users to check if their information was compromised. This domain was called ”equifaxsecurity2017.com”. This caused further issues:

- The domain is not linked to any other Equifax domain.
- The webpage hosted on this domain had TLS misconfigurations.
- The web-page itself was built using WordPress (which is not a great security practice).
- The name of the domain is extremely unintelligible and looks much like a phishing page.

The above issues caused the domain to be blocked by **OpenDNS** causing chaos and miscommunication about the breach online. The name of this domain caused further chaos in the the consumer base as it looked too similar to a phishing site ”securityequifax2017.com”, which Equifax themselves incorrectly publicised on their twitter account in a tweet made in the week of the official disclosure (Electronic Privacy Information Center, 2017) (Muncaster, 2017). This makes the lack of a proper incident response strategy very evident.



*Expecting an attack, regardless of how robust the implementation of any security system is, should always be considered a security practice. It is evident by Equifax's actions that their incident response strategy was not completely robust. Equifax built a tool **after** the incident occurred meaning that there were no tools like "equifaxsecurity2017.com" already in the arsenal in case of a breach. This lack of preparation is what caused errors and chaos among the consumers.*

Figure 3: My analysis

Figure 4 shows a diagrammatic representation of the timeline of all the important events relating to this breach.

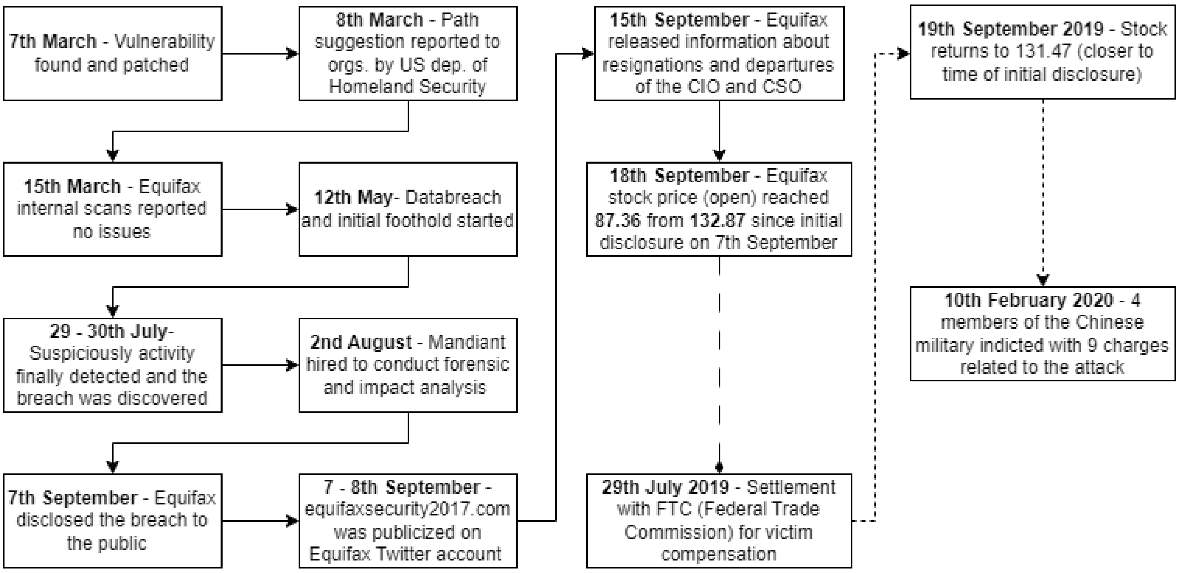

7th March - Vulnerability found and patched
8th March - Path suggestion reported to orgs. by US dep. of Homeland Security
15th March - Equifax internal scans reported no issues
12th May- Databreach and initial foothold started
29 - 30th July- Suspiciously activity finally detected and the breach was discovered
2nd August - Mandiant hired to conduct forensic and impact analysis
7th September - Equifax disclosed the breach to the public
7 - 8th September - equifaxsecurity2017.com was publicized on Equifax Twitter account
15th September - Equifax released information about resignations and departures of the CIO and CSO
18th September - Equifax stock price (open) reached **87.36** from **132.87** since initial disclosure on 7th September
29th July 2019 - Settlement with FTC (Federal Trade Commission) for victim compensation
19th September 2019 - Stock returns to 131.47 (closer to time of initial disclosure)
10th February 2020 - 4 members of the Chinese military indicted with 9 charges related to the attack

Figure 4: The timeline of events relating to the Equifax data breach 2017

4 Security Evaluation of The Incident and Mitigation Strategies

The objective of this section is to conduct a comprehensive analysis of the Equifax security incident. This analysis is designed to systematically assess how the breach happened, what security constraints were violated and what risks were **NOT** mitigated. This section follows the timeline of the incident to ensure a fluid evaluation without the necessity of recounting the event sequence, allowing for a focused critique on the response measures taken by Equifax.

More than just looking at a closer timeline, it is important to actually look at the wider picture. According to the U.S. Senate Permanent Subcommittee on Investigations (2019) ”Equifax Failed to Prioritise Cybersecurity”.

4.1 Security was not a priority

Based on the historical data we have, Equifax did not establish a specific written policy for fixing known cybersecurity flaws until 2015. Upon adopting such a policy, the company undertook a review of its patch management processes. This review uncovered a significant backlog, revealing over 8,500 un-patched known vulnerabilities, some of which were critical. This shows a very important precedent that Equifax did not indeed pay much attention to cybersecurity in the first place hence a breach was inevitable (U.S. Senate Permanent Subcommittee on Investigations, 2019).

4.2 Lack of team and information management

For an organisation to maintain security, cultivating a culture centred on cybersecurity is crucial. The absence of such a culture can lead to employees being unaware and negligent of threats that are present within their immediate environment. This deficiency in cybersecurity awareness can be attributed to the lack of proper information management within the team, a point emphasised in every security management framework through the example of audit logs. A notable shortcoming in the security practice at Equifax could be the absence of a simple document, resource, or database that could have delineated the responsibilities of developers at Equifax. Essentially giving the information of ”Who wrote/manages/knows this code/system?”.

On March 14th, shortly after the **CVE-2017-5638** was discovered and patched, information regarding the vulnerability was shared among 400 Equifax employees. However, **this communication failed to reach the developer responsible for implementing Apache Struts**. Consequently, there were no employees who were aware of both the use of Apache Struts and the vulnerability within it, underscoring a significant lapse not in security but in security management. This is a perfect example of how Equifax violated principles laid out in ISO 27001, specifically relating to information security communication, awareness, training, and the management of technical vulnerabilities **(A.5), (A.6), (A.7), (A.12.1)** (Irwin, 2023).

Equifax conducted regular assessment meetings to discuss potential threats, but participation and attendance were limited, further highlighting the issue of inadequate information dissemination. Moreover, another indication of Equifax’s insufficient information management was the lack of comprehensive inventory of technological assets. This gap meant that if an automated static analysis tool failed, there was no manual method of determining if a system was outdated, exemplifying a severe lapse in cybersecurity best practices as defined in almost all information security frameworks, including the ISO-IEC 27000, NIST, BIMCO v3 and others (ABS Group, 2023). Keeping a record of which tools and technologies are used in the vast technology stack at Equifax would have minimised the risk and mitigated the threat of an attack.

4.3 Security architectural design flaws

According to Kabanov and Madnick (2020) et al multiple software engineering and security architectural best practices were violated by Equifax. These included **isolation**, **authentication**, **least privilege** and **encryption**. This report talks about isolation and authentication as the two main reasons why the attack was able to be performed at such a large scale.

Isolation is the process of segregating different computing processes and function from each other to enhance security. This approach prevents and significantly limits the ability of a malicious actor on isolated systems (National Institute of Standards and Technology (NIST), 2024) (National Institute of Standards and Technology, 2017).

> *"The attackers were able to use these credentials to access 48 unrelated databases."*
> (U.S. House of Representatives, 2018b)

The above quote given in the report by Mandiant showed that there was an unnecessary link between the ACIS entry-point (where the attackers gained their initial foothold) and 48 unrelated databases (The ACIS application would have functioned perfectly normally if it only had access to some 3 databases (U.S. House of Representatives, 2018a)). This means, that if Equifax had maintained principles of isolation as described in the NIST framework, the impact of the attack wouldn't have been nearly as devastating. Hence, mitigating the risk.

The principle of **authentication** according to NIST roots from the explanation that - for a "system", all the external environments that are not the "system" should be treated as hostile. Which means, any requests coming into the "system" needs to be authenticated and authorised. According to Kabanov and Madnick (2020) et al this requirement was not completely met by Equifax. Even-though authentication was implemented, greater attention was not paid, perhaps with the assumption that no one would access these resources, hence root privileged accounts were only protected with extremely insecure password policies as demonstrated by the U.S. House of Representatives (2018b).

4.4 Analysis using the Cyber Kill Chain

The Cyber Kill Chain is a concept that describes the stages of a cyber attack, from initial reconnaissance to the final action on objectives. It outlines seven stages: **reconnaissance**, **weaponisation**, **delivery**, **exploitation**, **installation**, **command & control**, and **actions & objectives**. This framework helps organisations understand and defend against cyber threats by identifying and blocking attacks at each stage (Assante and Lee, 2015). In order to make this information useful, (Exabeam, 2024) goes through a 5 step process of mitigating a threat for every stage of the Cyber Kill Chain. **Detect**, **Deny**, **Disrupt**, **Degrade**, **Deceive**. In my opinion an extra step must be added here before "Detect" called **Discover**.

4.4.1 Discover

The breach of Equifax can be attributed to attackers exploiting a known vulnerability in an outdated Apache Struts version within Equifax's infrastructure, a fact unknown to Equifax at the time but known to the attackers. Equifax in practice should conduct the same kind of OSINT that attackers would to find out if any of their systems are leaking unneccary information such as 'version details' and 'asset names'. For instance, a google dorking method as shown on Exploit DB ghd (2016), showing how to make google index a list of websites currently running the vulnerable version of Struts 2. This Exploit DB record was published more than a year before Equifax was breached.

If more companies conducted **Discover** more regularly, they would be able to prevent attackers from conducting reconnaissance and perhaps reduce the risk of an attack.

4.4.2 Detect

The goal of **Detect** here would be useful for counteracting the "actions & objectives" phase of the Cyber Kill Chain. Attackers remained in the system for more than 75 days without being detected. This is because of an out of data SSL certificate. The sole purpose of an SSL certificates is to provide confidentiality, data authentication and non-repudiation; all three of which were missing because Equifax's SSL certificates for the online dispute portal were out of date. This caused a severe detection issue which resulted in the breach lasting 75+ days. If Equifax had maintained proper documentation and reminder automations, detection would have been much more robust and timely (U.S. Senate Permanent Subcommittee on Investigations, 2019).

4.4.3 Deny

The goal of **Deny** here is to stop the attack in the first place. In regular systems this is done using Intrusion Prevention Systems, Intrusion Detection Systems and even Firewalls. As a comparison, TransUnion, another large CRA while waiting for a patch used all three of the above. Right after the notification of the vulnerability was provided, TransUnion configured there already existing Web Application Firewalls (WAF) to recognise attacks against these vulnerabilities and stop them. This was done to maintain their vulnerable version of Apache Struts while a patch was figured out (U.S. Senate Permanent Subcommittee on Investigations, 2019). The absence of a WAF in Equifax's system was a direct violation of the Requirement 6.6 of the PCIDSS (Payment Card Industry Data Security Standards) (CompliancePoint, 2017). The fact that, Equifax did not have a WAF while TransUnion did and Equifax was victim of a cyber attack, concludes that the absense of a WAF contributed to the data breach and the data breach would have been prevented if a WAF was implemented (Kabanov and Madnick, 2020).

5 Conclusion

To conclude, the Equifax breach serves as a stark reminder of the dangers of neglecting cybersecurity practices and the importance of solid organisational management. Beyond the failure to patch a vulnerability, the core issues included poor communication, inadequate leadership, and a lack of proactive threat management. This underscores the need for both robust security measures and strong internal management to ensure these measures are effectively implemented. Moreover, the incident highlights the critical necessity for thorough documentation within every team, detailing not just what tasks are performed but also why and how they are executed, providing clear rationale and procedures. This approach ensures that all levels of the organisation contribute to its security posture, fostering a culture of transparency, competency, and informed decision-making crucial for preventing future breaches.

Bibliography

Ghdb id 4278. https://www.exploit-db.com/ghdb/4278, 2016. Accessed: 2024-03-05.

ABS Group. Cybersecurity asset management: What you need to know. https://www.abs-group.com/Knowledge-Center/Insights/Cybersecurity-Asset-Management-What-You-Need-To-Know/, 2023. Accessed: 2024-03-04.

Michael J Assante and Robert M Lee. The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, 1:24, 2015.

Alyssa L Aubuchon. Getting into court when the data has gotten out: A two-part framework. *Wash. UL Rev.*, 98:1289, 2020.

Shannon Beske and Kevin Stallings. Leading strategic change: tools and technique workshop (hrps). *Human Resource Planning*, 21(2):9–11, 1998.

Nathan Bomey. 2017 equifax data breach: Chinese military hack. https://eu.usatoday.com/story/tech/2020/02/10/2017-equifax-data-breach-chinese-military-hack/4712788002/, Feb 2020. Accessed: 2024-03-04.

Consumer Financial Protection Bureau. Consumer financial protection circular 2022-04 - insufficient data protection or security for sensitive consumer information. *Consumer Financial Protection Bureau*, 2022.

CompliancePoint. The equifax data breach, pci, and you. https://www.compliancepoint.com/information-security/equifax-data-breach-pci/, September 2017. Accessed: 2024-03-05.

Electronic Privacy Information Center. The 2017 equifax breach, 2017. URL https://archive.epic.org/privacy/data-breach/equifax/. Accessed: 2024-03-03.

Mazen Elzanaty. struts-pwn - an exploit for apache struts cve-2017-5638. https://github.com/mazen160/struts-pwn, 2017. Accessed: 2024-03-05.

Equifax. Equifax ltd uk update regarding the ongoing investigation into us cyber security incident. https://www.equifax.co.uk/about-equifax/press-releases/en_gb/-/blog/equifax-ltd-uk-update-regarding-the-ongoing-investigation-into-us-cyber-security-incid 2017. Accessed: 2024-03-04.

Equifax. Historical data - equifax investor relations. https://investor.equifax.com/stock-info/historical-data, 2024. Accessed: 2024-03-04.

Equifax Ltd UK. Uk information update regarding the ongoing investigation into us cybersecurity incident: Mandiant completes initial review. Equifax UK Press Releases, 2017. URL https://www.equifax.co.uk/about-equifax/press-releases/en_gb/-/blog/equifax-ltd-uk-information-update-regarding-the-ongoing-investigation-into-us-cybersec Accessed: 2024-03-04.

Equifax UK. Credit reference agency data handling. Web Page, 2024. URL https://www.equifax.co.uk/ein.html. Accessed: 2024-03-03.

Exabeam. Cyber kill chain: Understanding and mitigating advanced threats, 2024. URL https://www.exabeam.com/explainers/information-security/cyber-kill-chain-understanding-and-mitigating-advanced-threats/. Accessed: 2024-03-05.

Federal Bureau of Investigation. Chinese pla members 54th research institute. `https://www.fbi.gov/wanted/cyber/chinese-pla-members-54th-research-institute`, February 2020. Accessed: 2024-03-04.

Federal Trade Commission. Equifax data breach settlement. `https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement`, 2024.

Dan Goodin. Massive equifax breach caused by failure to patch two-month-old bug. `https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/`, Sep 2017. Accessed: 2024-03-04.

Luke Irwin. Iso 27001: The 14 control sets of annex a explained, 2023. URL `https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained`. Accessed: 2024-03-04.

Ilya Kabanov and Stuart Madnick. A systematic study of the control failures in the equifax cybersecurity incident. 2020.

Kevin LaCroix. Equifax data breach-related securities suit settled for $149 million. *The D&O Diary*, February 2020. URL `https://www.dandodiary.com/2020/02/articles/securities-litigation/equifax-data-breach-related-securities-suit-settled-for-149-million/`. Accessed: 2024-03-03.

Lukasz Lenart and René Gielen. S2-045 Security Bulletin. `https://cwiki.apache.org/confluence/display/WW/S2-045`, March 2017. Accessed: 2024-03-03.

Lending Stream. Equifax – Who are They? Everything You Should Know About Equifax. `https://www.lendingstream.co.uk/blog/equifax/`, 2024. Accessed: 03/03/2024.

Phil Muncaster. Why the equifax breach is very possibly the worst leak of personal info ever. `https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/`, Sep 2017. Accessed: 2024-03-04.

National Institute of Standards and Technology. Application container security guide. Special Publication 800-190, National Institute of Standards and Technology, Gaithersburg, MD, September 2017. URL `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf`.

National Institute of Standards and Technology (NIST). Isolation - glossary — csrc, 2024. URL `https://csrc.nist.gov/glossary/term/isolation`. Accessed: 2024-03-05.

National Vulnerability Database (NVD). CVE-2017-5638. `https://nvd.nist.gov/vuln/detail/CVE-2017-5638`, 2017. Accessed: 2024-03-03.

Alison N Novak and M Olguta Vilceanu. “the internet is not pleased”: twitter and the 2017 equifax data breach. *The Communication Review*, 22(3):196–221, 2019.

Walter Primoff and Sidney Kess. The equifax data breach: What cpas and firms need to know now. *The CPA Journal*, 87(12):14–17, 2017.

CSO Staff. Equifax data breach faq: What happened, who was affected, what was the impact. `https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html`, 2017. Accessed: 2024-03-04.

The Apache Software Foundation. Media alert: The apache software foundation confirms equifax data breach due to failure to install patches provided for apache® struts™ exploit, September 2017. URL `https://news.apache.org/foundation/entry/media-alert-the-apache-software`. Accessed: [insert date here].

Jason Thomas. A case study analysis of the equifax data breach 1 a case study analysis of the equifax data breach. `https://www.researchgate.net/publication/337916068_A_Case_Study_Analysis_of_the_Equifax_Data_Breach_1_A_Case_Study_Analysis_of_the_Equifax_Data_Breach`, 12 2019.

U.S. House of Representatives. Report on the equifax data breach. Technical report, House Oversight and Government Reform Committee, Washington, D.C., December 2018a. URL `https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf`.

U.S. House of Representatives. Committee on oversight and government reform - the equifax data breach. SlideShare, December 2018b. URL `https://www.slideshare.net/ouldparis/us-house-of-representatives-committee-on-oversight-and-gdocx`. Accessed: 2024-03-05.

U.S. Senate Permanent Subcommittee on Investigations. How equifax neglected cybersecurity and suffered a devastating data breach. `https://nsarchive.gwu.edu/sites/default/files/documents/5794667/National-Security-Archive-U-S-Senate-Permanent.pdf`, 2019. Accessed: 2024-03-04.