Table of Contents

Table of Figures

Abstract

This research paper is a deep and analytical dive into the 2015 Ashley Madison data breach using Blooms Taxonomy approach. It aims to look at the data breach from Ethical, Social, Legal and Professional standpoint and draw out a clear unbiased understanding of the entire situation. It explores the multidimensional repercussions of the incident and how it affected the users, the company and all the parties involved. It then draws out a conclusion on the entire situation using all the available data and research done.

1. Introduction

From the inception of the internet back in the 1970s, data has emerged as one of the most valuable assets in this digital era. A news article by The Wired touted data as the new "oil" of the digital economy, clearly stating that data infrastructure can be a huge centre for corporate profit (internetsociety.org, 2023) (Joris & Yonego, 2014). Like how various entities including countries and corporations alike hurdled and did everything they could to get hands on oil from the 18th century, the same is being repeated in this digital era but with acquisition of data.

We can be certain that because data is of much value in our modern era, there will be various entities seeking ways they can get hands on our data and use various schemes to gain massive amounts of profit. The University of Maryland published a report in 2016 that the market for big data and analytics technology will grow to over 34 billion US dollars (Maryland, 2016). In 2024 this figure has risen to a massive 348.21 billion US dollars (Fortune Busniess Insights, 2024). With the value of our data increasing day by day, and the number of entities doing everything they can to get hands on our data, we need to make sure that we are well protected from a breach of personal data and information.

A lapse in data security occurred in August of 2015 when a group or an individual calling themselves 'The Impact Team' released personal data of millions of users of the Ashley Madison website. Ashley Madison is a website that offers extra-marital or "cheating" services to married people. Millions of people had signed up and were using the services provided by Ashley Madison, unbeknownst to their partners when the impact team released the data they had collected. This data breached caused a lot of uproar in the community, causing divorces, separation, and broken families (Victor, 2015) (KerbsOnSecurity, 2022).

1.1. Statistics on data breach

In 2023 alone more than 290 million accounts were breached globally with the US and Russia being the countries with the highest data breach (Surfshark, 2023). Business Insider reports that the primary causes for data breach in 2023 were cloud misconfiguration, new types of ransomware attacks and increased exploitation of vendor systems (Harvard Business Review, 2024).

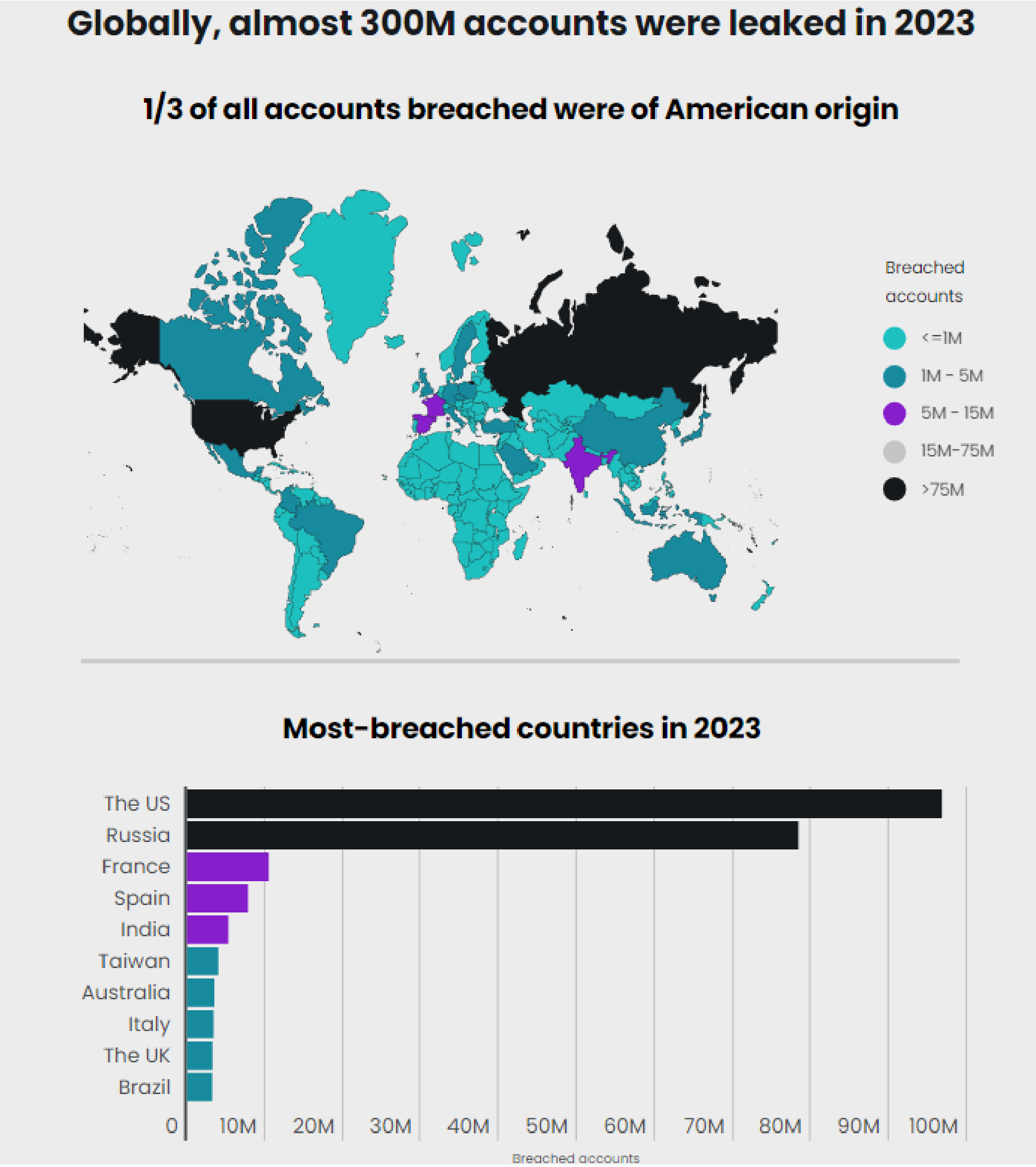
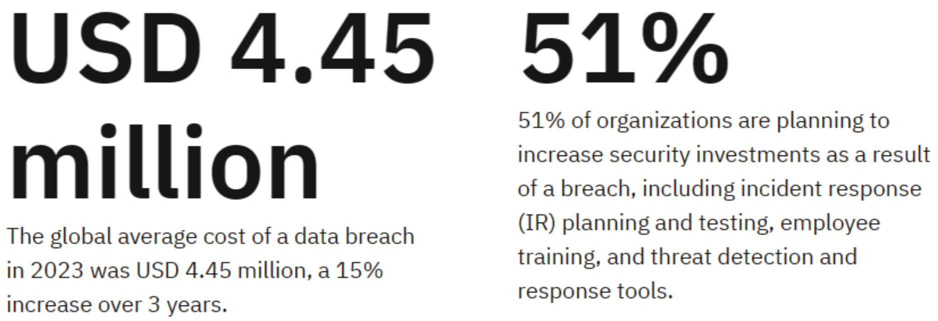


Figure 1: Global Data Breach Statistics 2023 (Surfshark, 2023).



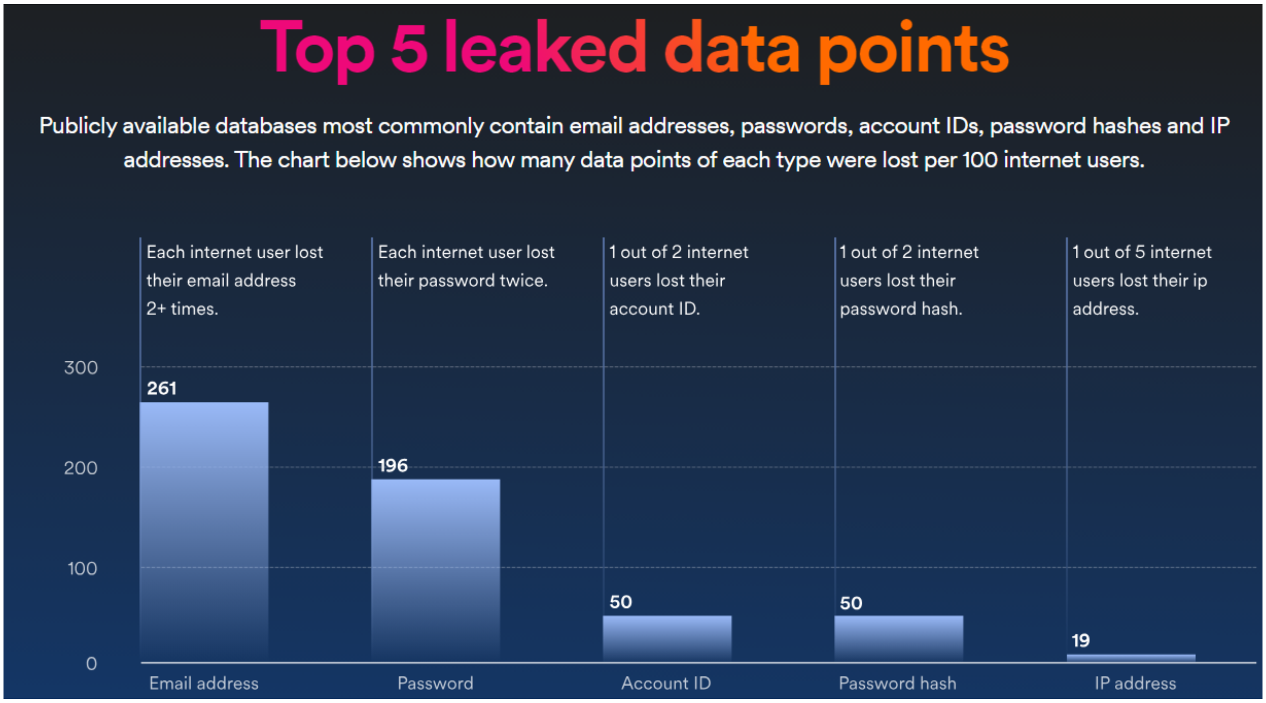
USD 4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

51%

51% of organizations are planning to increase security investments as a result of a breach, including incident response (IR) planning and testing, employee training, and threat detection and response tools.

Figure 2: Average Cost of Data Breach (IBM).



Top 5 leaked data points

Publicly available databases most commonly contain email addresses, passwords, account IDs, password hashes and IP addresses. The chart below shows how many data points of each type were lost per 100 internet users.

Each internet user lost their email address 2+ times.

Each internet user lost their password twice.

1 out of 2 internet users lost their account ID.

1 out of 2 internet users lost their password hash.

1 out of 5 internet users lost their ip address.

Figure 3: Top Leaked Data Points (Surfshark).

Because most of our data is stored in the cloud, and how valuable personal data can be, there will always be attempts from individuals and groups to extract as much data as they can and use it to their advantage. Organizations that hold data need to be careful on how the data is handled and make sure that there are robust data protection measures in place to prevent any type data leak from happening. Users should also be careful about who they are giving their data too and make sure that the organization is trustworthy.

1.2. Ashley Madison

Ashley Madison is an online dating platform specifically for married people to have affairs. Their tagline in their website is “Life is Short. Have an Affair”. They claim to be the worlds number one and most discreet place to find, in their words, open minded people and explore. In their website they put a huge focus on how secure and discreet everything is. They claim that their “state of the art” website is designed with the user and privacy in mind (Ruby Life Inc., 2024). Ashley madison also offered users a £19 paid service to “remove all user data” (Pearl, 2023).

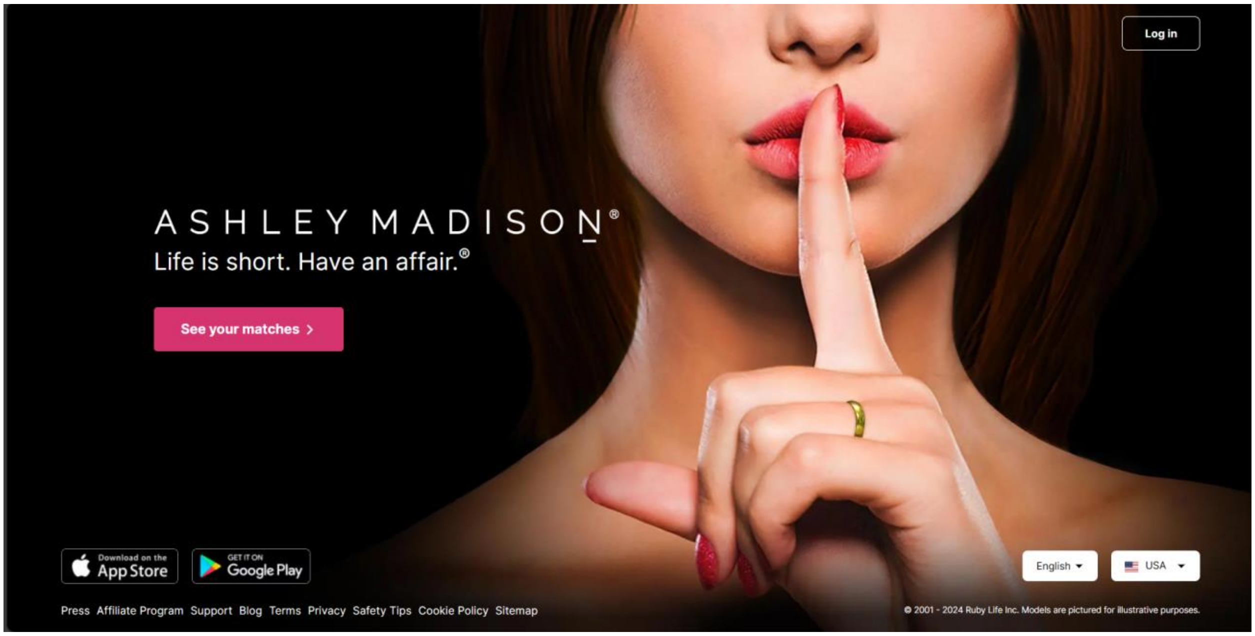
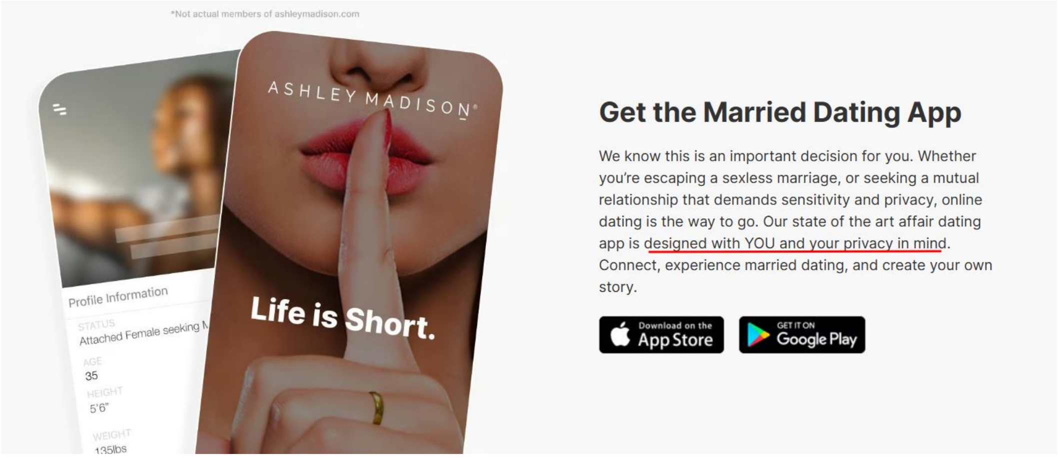

Log in
ASHLEY MADISON®
Life is short. Have an affair.®
See your matches ›
Download on the App Store
GET IT ON Google Play
English
USA
Press Affiliate Program Support Blog Terms Privacy Safety Tips Cookie Policy Sitemap
© 2001 - 2024 Ruby Life Inc. Models are pictured for illustrative purposes.

Figure 4: Ashley Madison Website



Get the Married Dating App

We know this is an important decision for you. Whether you're escaping a sexless marriage, or seeking a mutual relationship that demands sensitivity and privacy, online dating is the way to go. Our state of the art affair dating app is designed with YOU and your privacy in mind. Connect, experience married dating, and create your own story.

Figure 5: Ashley Madison focus on privacy.

2. Background of The Data Breach

On July 12, 2015, as Ashley Madison employees logged in to their devices, they were greeted with a message from a hacker group known as “The Impact Team”. The group had threatened to release user data from their website unless they permanently shut down the Ashley Madison website along with its sister websites Cougar Love and Established Men. The message has been said to be accompanied by the AC/DC song Thunderstruck (Lord, 2017). It is reported that the group also released a small portion of the data they collected, although not clear exactly how much they released, it was enough for then CEO Noel Biderman to confirm that there has been a data breach. Biderman quoted to the media “Like us or not, this is still a criminal act” (Kerbs, 2015).

The hackers had given the company one month time to take down all their online dating websites. The hacker group claimed that the £19 full delete feature was a scam and Ashley Madison never deleted any of the user data. The hackers seemed to have no financial demands, rather they poured their frustrations about the ethics of the website itself and also said “Too bad for those men, they’re cheating dirtbags and deserve no such discretion” regarding the people whose data had been breached (Kerbs, 2015).

On August 18, 2015, The Impact Team made good on their promise and released the data of more than 37 million users of the Ashley Madison website. After a lot of speculation and analysis, it was confirmed that the data dump was authentic and contained real data of actual users. The Impact Team also did another major data dump on August 20, this time containing the internal structure of the company along with 19 GB of the CEO’s email data (Lord, 2017).

The Ashley Madison breach impacted an estimated 37 million users. With more than 60 GB of data being released to the public on the dark net (Business Insider, 2015). The data breach revealed that this website was hugely dominated by male accounts. Out of the roughly 5.5 million female accounts, only 12 thousand were shown to be “active” users of the website (Reed, 2015). The data breach also revealed the passwords of 11 million users as they had been hashed with an insecure algorithm (Goodin, 2015). Thousands of .gov and .mil email addresses of the US government and US military were also found in the leaked data. The data also contained accounts with email form Saudi Arabia ending with .sa (Gibbons-Nef, 2015).

The following figure shows the timeline of the Ashley Madison data breach. From the first news of the attack on July 12 to the second major data dump on August 20. The Impact team had their demands very clearly set out and released the data one month after the warning after Ashley Madison didn't comply.

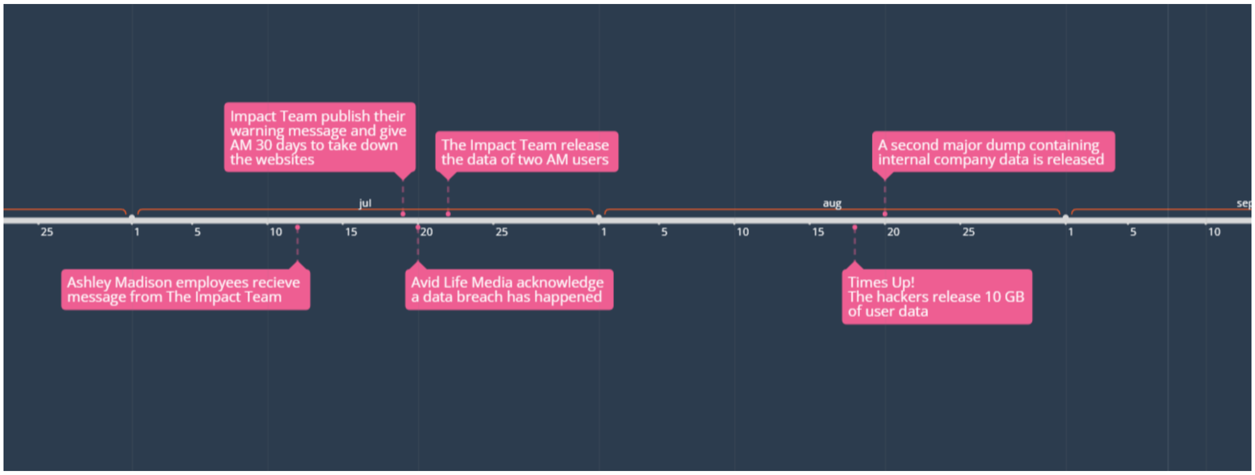
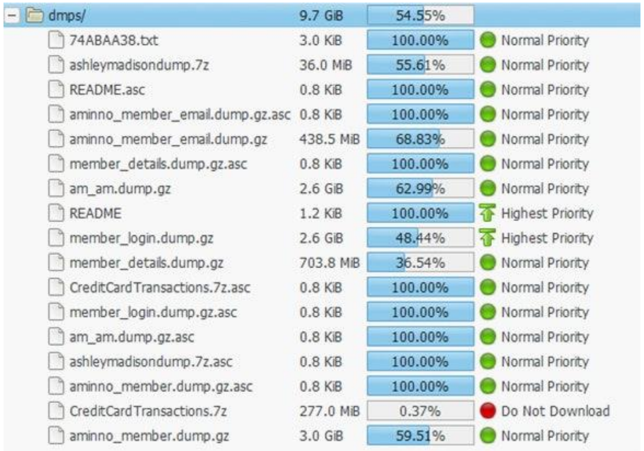

Impact Team publish their warning message and give AM 30 days to take down the websites
The Impact Team release the data of two AM users
A second major dump containing internal company data is released
jul
aug
sep
25
1
5
10
15
20
25
1
5
10
15
20
25
1
5
10
Ashley Madison employees recieve message from The Impact Team
Avid Life Media acknowledge a data breach has happened
Times Up! The hackers release 10 GB of user data

Figure 6: Timeline of the AM hack.

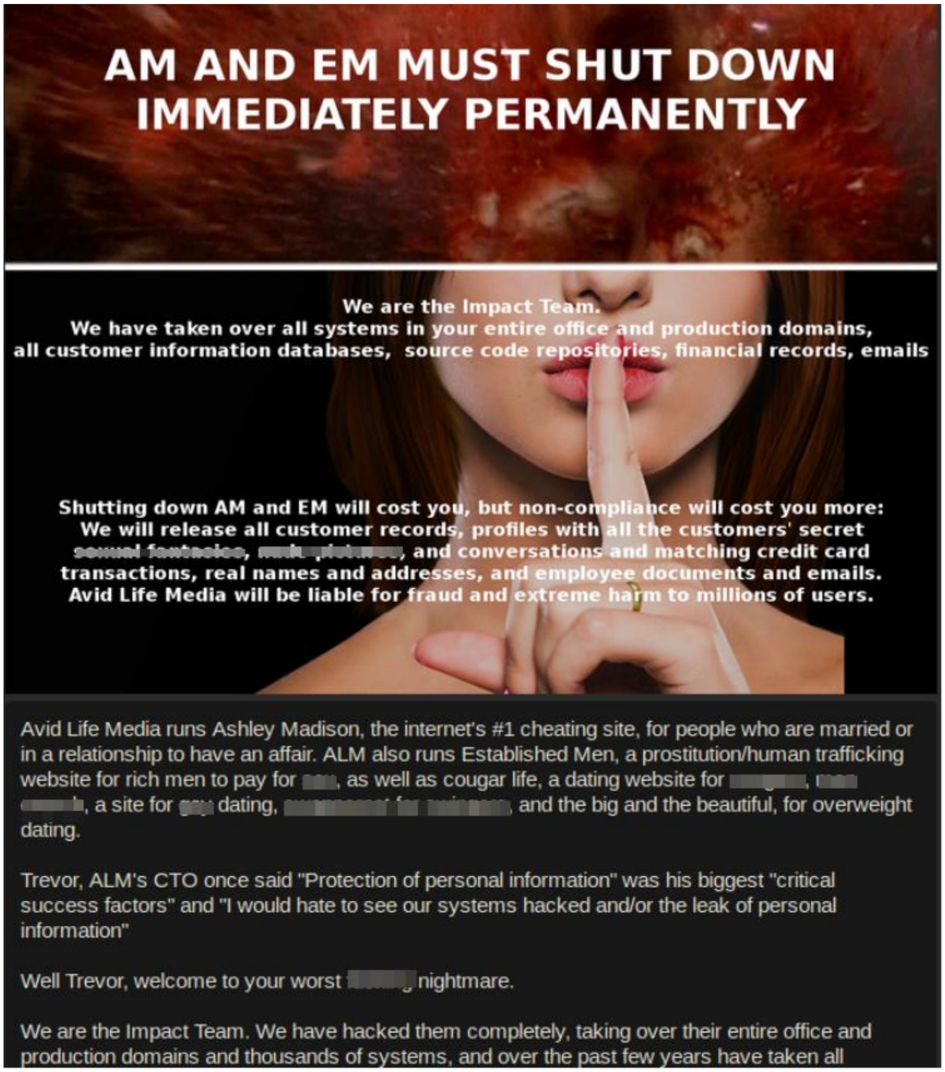
2.1. Role of The Impact Team

The main perpetrator of the Ashley Madison data breach calls itself 'The Impact Team'. It is unclear whether it is a group of hackers or a single hacker that carried out the attack. It appears the group was made with the sole purpose of hacking the infidelity website as no other previous hacks could be traced to this group. The group also didn't seem to directly have any financial motives as their main demand was to shut down the infidelity sites being run by Ashley Madison's then parent company, Avid Life Media (Ward & BBC, 2015). The hackers say that "there was no one watching" and they were inside the company's system for a long time without anyone noticing. The hackers seemed to have a disdain for infidelity as they called the company and the users both "Stupid". Whoever was behind this attack is still not found with some speculations going on here and there but no hard evidence against anyone (Reuters; The Indian Express, 2015).



dmps/	9.7 GiB	54.55%	
74ABAA38.txt	3.0 KiB	100.00%	Normal Priority
ashleymadisondump.7z	36.0 MiB	55.61%	Normal Priority
README.asc	0.8 KiB	100.00%	Normal Priority
aminno_member_email.dump.gz.asc	0.8 KiB	100.00%	Normal Priority
aminno_member_email.dump.gz	438.5 MiB	68.83%	Normal Priority
member_details.dump.gz.asc	0.8 KiB	100.00%	Normal Priority
am_am.dump.gz	2.6 GiB	62.99%	Normal Priority
README	1.2 KiB	100.00%	Highest Priority
member_login.dump.gz	2.6 GiB	48.44%	Highest Priority
member_details.dump.gz	703.8 MiB	36.54%	Normal Priority
CreditCardTransactions.7z.asc	0.8 KiB	100.00%	Normal Priority
member_login.dump.gz.asc	0.8 KiB	100.00%	Normal Priority
am_am.dump.gz.asc	0.8 KiB	100.00%	Normal Priority
ashleymadisondump.7z.asc	0.8 KiB	100.00%	Normal Priority
aminno_member.dump.gz.asc	0.8 KiB	100.00%	Normal Priority
CreditCardTransactions.7z	277.0 MiB	0.37%	Do Not Download
aminno_member.dump.gz	3.0 GiB	59.51%	Normal Priority

Figure 7: Data dumped by The Impact Team, (Graham Robert).



AM AND EM MUST SHUT DOWN
IMMEDIATELY PERMANENTLY

We are the Impact Team.
We have taken over all systems in your entire office and production domains,
all customer information databases, source code repositories, financial records, emails

Shutting down AM and EM will cost you, but non-compliance will cost you more:
We will release all customer records, profiles with all the customers' secret
[redacted], [redacted], and conversations and matching credit card
transactions, real names and addresses, and employee documents and emails.
Avid Life Media will be liable for fraud and extreme harm to millions of users.

Avid Life Media runs Ashley Madison, the internet's #1 cheating site, for people who are married or in a relationship to have an affair. ALM also runs Established Men, a prostitution/human trafficking website for rich men to pay for [redacted], as well as cougar life, a dating website for [redacted], [redacted], a site for [redacted] dating, [redacted], and the big and the beautiful, for overweight dating.

Trevor, ALM's CTO once said "Protection of personal information" was his biggest "critical success factors" and "I would hate to see our systems hacked and/or the leak of personal information"

Well Trevor, welcome to your worst [redacted] nightmare.

We are the Impact Team. We have hacked them completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all

Figure 8: Snippet of the message released by The Impact Team, (Kerbs, 2015).

2.2. Problem Statement

The Ashley Madison data breach posed a significant risk to all the users affected because the amount of Personally Identifiable Information (PII) was very high. The information leaked ranged from user's name, address, their sexual preferences, to even their financial information (KerbsOnSecurity, 2022). This report aims to analyse and provide insights to the scandal from a multi-faced perspective. It will discuss the legal, social, ethical, and professional issues concerning the data breach, talk about the fallout effect this data breach has created and its overall impact on the users the users that were directly affected.

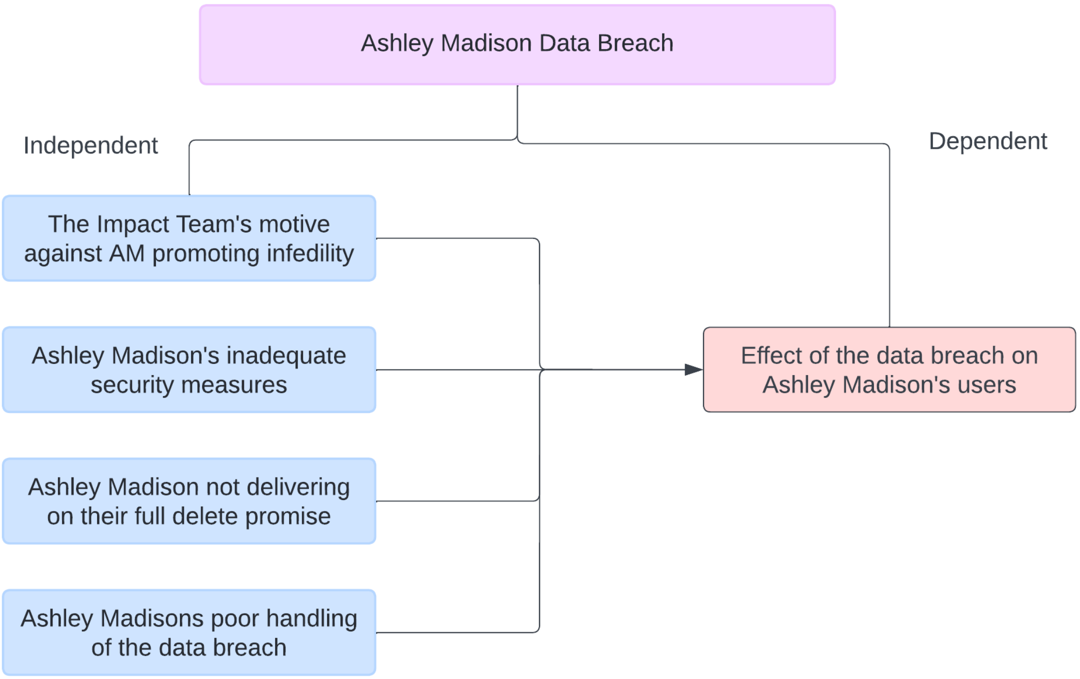

Ashley Madison Data Breach
Independent
Dependent
The Impact Team's motive against AM promoting infedility
Ashley Madison's inadequate security measures
Ashley Madison not delivering on their full delete promise
Ashley Madisons poor handling of the data breach
Effect of the data breach on Ashley Madison's users

Figure 9: Theoretical Framework

2.3. Legal Issues

The protection of the user's data lies in the hands of the organization collecting them. The US law states that "In a cloud environment, Under US law, the data owner faces liability for losses resulting from a data breach" (AuroraWDC, 2020). The hackers also face criminal charges for unauthorized access of private information. They can also be sued by Ashley Madison on criminal grounds (Strom, 2023). In case of Ashley Madison, the following legal issues were faced.

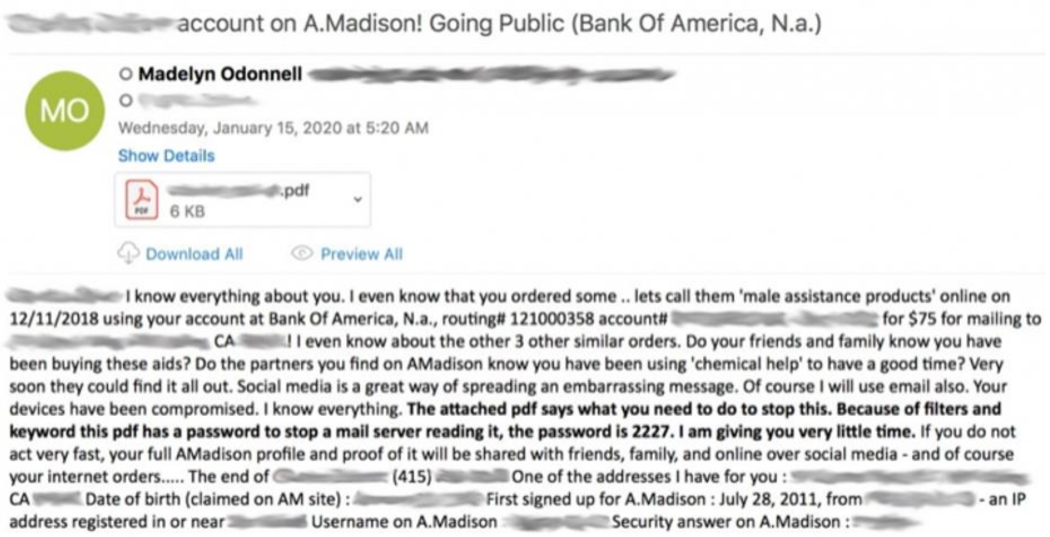
- Ashley Madison faced a $578 Million lawsuit in the Canadian court. The case was filed by Canadian law firms on behalf of Canadian Ashley Madison users (Noronha, 2015).
- A $5 Million lawsuit filed in the U.S. District on behalf of a female candidate who pointed out how Ashley Madison charged $19 for a full delete that didn't work as promised (Noronha, 2015).
- The FTC (Federal Trade Commission) of the US was settled $1.6 million by Ashley Madison. FTC fined Ashley Madison for having lax security, engaging in deceptive practices (the full delete service) and more (Bisson, 2016) (Federal Trade Commission, 2016).
- The Office of the Privacy Commissioner of Canada issued an investigation on the data breach and published a report with all its findings. In which it created guidelines for other organisations to follow to avoid any future data breached (Privacy Commission of Canada, 2016).
- US judge okayed a $11.2 million settlement for hacked Ashley Madison Users (Salter, 2017)

2.4. Social Issues

The Ashley Madison data breach had a significant social impact. Because the site itself was promoting infidelity, most if not all its users were people already in a committed relationship. The following social issues were faced because of the Ashley Madison hack.

- Many partners found out they were being cheated on through the data breach. This caused many marriages to end in divorce. Business Insider reported that a marriage counselling firm in the UK started to receive calls from distressed users who found their partners information on the data breach (Slater-Robins, 2015).

- Two individuals who were associated with the data breach are reported to have committed suicide as reported by the BBC News. The guilt and shame of their infidelity being publicly disclosed is bound to have negative effects on the user’s mental health (Baraniuk, 2015).
- In 2020, scammers were still using the leaked data to run an extortion scam on the victims. They sent emails with highly personal information to the victims to get money from them (Doffman, Zak; Forbes, 2021). A sample of the email is shown below:



[redacted] account on A.Madison! Going Public (Bank Of America, N.a.)

○ Madelyn Odonnell [redacted]
○ [redacted]
Wednesday, January 15, 2020 at 5:20 AM

[redacted].pdf
6 KB

[redacted] I know everything about you. I even know that you ordered some .. lets call them 'male assistance products' online on 12/11/2018 using your account at Bank Of America, N.a., routing# 121000358 account# [redacted] for $75 for mailing to [redacted] CA [redacted]! I even know about the other 3 other similar orders. Do your friends and family know you have been buying these aids? Do the partners you find on AMadison know you have been using 'chemical help' to have a good time? Very soon they could find it all out. Social media is a great way of spreading an embarrassing message. Of course I will use email also. Your devices have been compromised. I know everything. **The attached pdf says what you need to do to stop this. Because of filters and keyword this pdf has a password to stop a mail server reading it, the password is 2227. I am giving you very little time.** If you do not act very fast, your full AMadison profile and proof of it will be shared with friends, family, and online over social media - and of course your internet orders..... The end of [redacted] (415) [redacted] One of the addresses I have for you : [redacted] CA [redacted] Date of birth (claimed on AM site) : [redacted] First signed up for A.Madison : July 28, 2011, from [redacted] - an IP address registered in or near [redacted] Username on A.Madison [redacted] Security answer on A.Madison : [redacted]

Figure 10: Extortion Mail Sent to AM Data Breach Victims (Forbes).

- The trust in corporations declined even more as Ashley Madison promised but never delivered on the £19 “Full Delete” option that they claimed removed all user data permanently (KerbsOnSecurity, 2022).

2.5. Ethical Issues

The ethical analysis of the Ashley Madison data breach is a very complex topic. Ashley Madison facilitated infidelity and cheating among its users which might be considered unethical by several people. We need to look at this data breach from all available perspectives and draw out our own conclusion.

- Deontology is guided by rules to distinguish what is right and what is wrong. A deontologist will always follow the law and keep their promises (Chonko, 2012). Ashley madison is clearly unethical when looked at from a deontological perspective, as they failed to keep their promise of deleting the user's data after receiving a fee. The impact team however delivered on their promise to leak data if their demands were not fulfilled.
- Utilitarianism is guided by the consequences of one's actions. Act utilitarianism tells us to perform acts that benefit the most people regardless of the rules whereas Rule utilitarianism takes rules and fairness into consideration. Were Ashley Madisons services and intentions acts that benefited the most people? Not at all, infidelity, and adultery benefits only a small group of people and instead causes harm to most. Even the impact team's decision to leak user data caused harm to most people instead of doing them any good. On top of that, their decision to hack is also illegal (Chonko, 2012).
- Rights based ethics protects and gives priority to rights established by the society. Rights are valid and ethically correct because a large population endorses them. In case of Ashley Madison, people had the right to have their data deleted after paying a fee because it was promised to them, and they also had the right to have their data protected from any potential leaks. The hackers in the other hand had no right to breach into a company's database no matter their intentions (Chonko, 2012).
- Virtue based ethics judges a person by their character rather than by their action. We can say that the impact team had relatively good intentions in their mind when they decided to release the data. They were against infidelity and wanted one of the biggest infidelity endorsing site to shut down.

2.6. Professional Issues

Professional ethics are code of conducts that govern the behaviour of a professional. They are set of rules and conducts one must follow in a professional environment (Immigration Advisers Authority, 2018).

- As an organization with highly sensitive user data, Ashley Madison had the responsibility of making sure that their security was robust and fool proof. They failed to protect their user's data.

- A professional is also deemed to be honest, but it was revealed that Ashley Madison was lying about the £19 full delete feature and the user's data were still stored in their database.
- When the hackers gave Ashley Madison one month to shut down their website and showed proof that they were indeed inside the system, AM should have handled the situation better and kept their users at the topmost priority.
- The FTC found that the security of Ashley Madison was lax and fined them, further bringing their professional reputation down.

2.7. Ashley Madison Now

After the data breach, the parent company of Ashley Madison Avid Life Media has rebranded itself as Ruby Life ltd. And has continued the Ashley Madison site. The company claims to have brought in new cyber security experts and put up a new cyber security model in place (Michael Kerner, 2018). Ashley Madison now has more than 70 million users and is one of the largest dating sites in the world. Ashley Madison reports that they are gaining 21,000 new members a day and predict that if everything goes as per plan, they will be gaining more than 30,000 new members a day. They claim that this shows how viable their business model is and how they have managed to bounce back even after suffering from a massive data breach in 2015. Users will most probably continue to sign up and use the services provided by Ashley Madison. As per data security, Ashley Madison has said to put up entirely new data protection measures and is doing everything it can to prevent another data breach from happening (Takahashi, 2021).

Data breach and data leak will continue to happen for as long as there is data being stored in the cloud. Companies that store data need to be vigilant about potential data leaks and make sure there are proper security measures in place to prevent any data leak from occurring.

3. Conclusion

The 2015 Ashley Madison data breach was a big fiasco that caused a lot of drama and had several negative consequences. This data breach highlights how fragile digital privacy can be if it is not taken seriously and handled properly. Ashley Madison in a way deceived their users by making them pay £19 pounds for a full delete service while not removing the user data as promised. On top of that, encouraging infidelity is unethical from a utilitarianism perspective because how their service benefits a very small group of people and harms the rest. The service they provide is considered socially unacceptable and is looked down upon. Does that justify the user's data being hacked? Not at all, no matter how socially looked down upon, Ashley Madison's users had their right to privacy and data protection. Even if the hackers were guided by a strong sense of morality of ending infidelity, they still breached the user's right to privacy.

When we analyze the entire situation properly, we realize that all the parties involved were equally guilty of something. Ashley Madison was promoting infidelity and taking money for a service who's promise they never fulfilled. The hackers were breaching user privacy, which is unacceptable no matter how morally guided they were. The users of Ashley Madison were looking for affairs outside their current marriage/relationship which is a big disgrace as considered by the society. What we can learn from all of this is that companies need to ensure that there are robust data security measures being implemented to prevent data breach. Companies must also deliver on their promise of privacy and data security. Overall, this data breach served as a lesson on what precautionary measures both the users and the organizations must take, and how we can try to prevent data breaches from happening.

4. Research Questions

1. Ashley Madison Data breach.
2. Ashley Madison Data breach statistics.
3. Investigation on the Ashley madison data breach.
4. What legal actions were faced by Ashley Madison for the data breach?
5. What was the FTC settlement by Ashley Madison based on?
6. What was leaked in the Ashley Madison Data breach?
7. Who was the main perpetrator behind the Ashley Madison Hack?
8. What were the demands by the impact team?
9. What was the manifesto of The Impact Team?
10. What were the security measures in place in Ashley Madison?
11. What is the number of divorces caused by the Ashley Madison Data breach?
12. When did the Ashley madison Data breach take place?
13. How did the Ashley madison data breach affect its users?
14. What was the motive behind the Ashley Madison data breach?

5. References

- Immigration Advisers Authority, 2018. *Professional ethics and codes of conduct.* [Online] Available at: https://www.iaa.govt.nz/for-advisers/adviser-tools/ethics-toolkit/professional-ethics-and-codes-of-conduct/
  [Accessed 27 April 2024].
- AuroraWDC, 2020. *Who is liable when a data breach occurs?.* [Online] Available at: https://aurorawdc.com/who-is-liable-when-a-data-breach-occurs/
  [Accessed 27 April 2024].
- Baraniuk, C., 2015. *Ashley Madison: 'Suicides' over website hack.* [Online] Available at: https://www.bbc.com/news/technology-34044506
  [Accessed 27 April 2024].
- Bisson, D., 2016. *Ashley Madison slammed with $1.6 million fine for devastating data breach.* [Online]
  Available at: https://grahamcluley.com/ashley-madison-slammed-with-1-6m-fine-for-data-breach/
  [Accessed 27 April 2024].
- Business Insider, 2015. *Cheating website Ashley Madison has been hacked and data from its members has leaked online.* [Online]
  Available at: https://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7
  [Accessed 21 April 2024].
- Chonko, L., 2012. *Ethical Theories.* [Online] Available at: https://dsef.org/wp-content/uploads/2012/07/EthicalTheories.pdf
  [Accessed 27 April 2024].
- Doffman, Zak; Forbes, 2021. *Ashley Madison Hack Returns To 'Haunt' Its Victims: 32 Million Users Now Watch And Wait.* [Online]
  Available at: https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait/?sh=67f657e55677
  [Accessed 27 April 2024].

- Ellingwood, J., 2017. *User Data Collection: Balancing Business Needs and User Privacy.* [Online]
  Available at: https://www.digitalocean.com/community/tutorials/user-data-collection-balancing-business-needs-and-user-privacy
  [Accessed 21 April 2024].
- Federal Trade Commission, 2016. *Ashley Madison settles with FTC over data security.* [Online]
  Available at: https://www.ftc.gov/business-guidance/blog/2016/12/ashley-madison-settles-ftc-over-data-security
  [Accessed 27 April 2024].
- Fortune Busniess Insights, 2024. *Big Data Analytics Market.* [Online]
  Available at: https://www.fortunebusinessinsights.com/big-data-analytics-market-106179
  [Accessed 4 April 2024].
- Gibbons-Nef, T., 2015. *Thousands of .mil addresses potentially leaked in Ashley Madison hack.* [Online]
  Available at: https://www.washingtonpost.com/news/checkpoint/wp/2015/08/19/thousands-of-mil-addresses-potentially-leaked-in-ashley-madison-hack/
  [Accessed 21 April 2024].
- Goodin, D., 2015. *Once seen as bulletproof, 11 million+ Ashley Madison passwords already cracked.* [Online]
  Available at: https://arstechnica.com/information-technology/2015/09/once-seen-as-bulletproof-11-million-ashley-madison-passwords-already-cracked/
  [Accessed 21 April 2024].
- Harvard Business Review, 2024. *Why Data Breaches Spiked in 2023.* [Online]
  Available at: https://hbr.org/2024/02/why-data-breaches-spiked-in-2023
  [Accessed 27 April 2024].
- internetsociety.org, 2023. *A Brief History of the Internet - Internet Society.* [Online]
  Available at: https://www.internetsociety.org/internet/history-internet/brief-history-internet/
  [Accessed 20 April 2024].

- Joris, T. & Yonego, 2014. *Data Is the New Oil of the Digital Economy.* [Online] Available at: https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ [Accessed 20 April 2024].
- Kerbs, B., 2015. *Online Cheating Site AshleyMadison Hacked.* [Online] Available at: https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/
  [Accessed 22 April 2024].
- KerbsOnSecurity, 2022. *A Retrospective on the 2015 Ashley Madison Breach.* [Online] Available at: https://krebsonsecurity.com/2022/07/a-retrospective-on-the-2015-ashley-madison-breach/
  [Accessed 21 April 2024].
- Lord, N., 2017. *A Timeline of the Ashley Madison Hack.* [Online] Available at: https://www.digitalguardian.com/blog/timeline-ashley-madison-hack [Accessed 22 April 2024].
- Maryland, U. o., 2016. *The Value of Data in Business.* [Online] Available at: https://onlinebusiness.umd.edu/blog/the-value-of-data-in-business/ [Accessed 20 April 2024].
- Michael Kerner, S., 2018. *Ashley Madison Takes Offensive Approach to Improve Breach Resilience.* [Online]
  Available at: https://www.eweek.com/security/how-ashley-madison-recovered-from-its-massive-data-breach/
  [Accessed 27 April 2024].
- Noronha, C., 2015. *Ashley Madison faces $578M Canadian class-action lawsuit.* [Online] Available at: https://apnews.com/general-news-86b58ff7b02c4f10a0d5f062cc7bff51 [Accessed 27 April 27 2024].
- Pearl, M., 2023. *Years later, the Ashley Madison hack remains an unsolved mystery.* [Online] Available at: https://mashable.com/article/ashley-madison-hack-retrospective [Accessed 22 April 2024].

- Privacy Commission of Canada, 2016. *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, Canada: Privacy Commission of Canada.
- Reed, B., 2015. *The most hilarious revelation about the Ashley Madison hack yet.* [Online] Available at: https://www.yahoo.com/tech/s/most-hilarious-revelation-ashley-madison-hack-yet-031557791.html
  [Accessed 21 April 2024].
- Reuters; The Indian Express, 2015. *Ashley Madison's hackers say there was no security to stop them from scouring data.* [Online] Available at: https://indianexpress.com/article/technology/tech-news-technology/cheating-website-ashley-madisons-hackers-say-nobody-was-watching/
  [Accessed 22 April 2024].
- Ruby Life Inc., 2024. *Affairs & Discreet Married Dating.* [Online] Available at: https://www.ashleymadison.com/
  [Accessed 21 April 2024].
- Salter, J., 2017. *Judge OKs $11.2M settlement for hacked Ashley Madison users.* [Online] Available at: https://apnews.com/general-news-d0dbb335a2b7492da7f7bd43049b4b6e
  [Accessed 27 April 2024].
- Slater-Robins, M., 2015. *First divorce case from the Ashley Madison leak.* [Online] Available at: https://www.businessinsider.com/first-divorce-case-from-the-ashley-madison-leak-2015-8
  [Accessed 27 April 2024].
- Strom, S., 2023. *Hacking Laws and Punishments.* [Online] Available at: https://www.findlaw.com/criminal/criminal-charges/hacking-laws-and-punishments.html
  [Accessed 27 April 2024].
- Surfshark, 2023. *Data breach statistics in 2023.* [Online] Available at: https://surfshark.com/research/study/data-breach-recap-2023
  [Accessed 27 April 2024].

- Takahashi, D., 2021. *Ashley Madison 'married dating' site grew to 70 million users in 2020.* [Online]
  Available at: https://venturebeat.com/consumer/ashley-madison-married-dating-site-grew-to-70-million-users-in-2020/
  [Accessed 28 April 2024].
- Victor, D., 2015. *The Ashley Madison Data Dump, Explained.* [Online]
  Available at: https://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html
  [Accessed 21 April 2024].
- Ward, M. & BBC, 2015. *Ashley Madison: Who are the hackers behind the attack?.* [Online]
  Available at: https://www.bbc.com/news/technology-34002053
  [Accessed 22 April 2024].