LONDON
METROPOLITAN
UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

CC5051NI Databases

50% Individual Coursework

Autumn 2023

Student Name: Sulav Neupane

London Met ID: 22085653

Assignment Submission Date: Sunday, May 5, 2024

Word Count: 4000

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

1. INTRODUCTION:

"Life is short, Have an affair." The main marketing tagline for the website AshleyMadison.com is "Have an affair." With 12 million US members and 18 million global, the website provides a platform to look for extramarital encounters. (Anderson, 2014). Ashley Madison promised consumers will have an affair within three months of signing up. Although using the website was free, users had to buy credits to communicate with other users. Ashley Madison would also clean a user's profile, erasing any data pertaining to their interactions on the website, for $19. Ashley Madison's business was so great that it contemplated a $200 million London initial public offering. (http://harbert.auburn.edu, 2022).

Figure 1 Ashley madison.com (Moscaritolo, 2015)

That was prior to the Ashley Madison website being widely hacked and user emails, names, addresses, sexual desires, credit card transactions, and account information being publicly disclosed online. Ashley Madison stated that the company had roughly 40 million registered users at the time of the hacking incident. Reputational harm, family disputes, divorces, suicides, a $578 million lawsuit brought against the business, and the departure of Noel Biderman, the founder and CEO of Avid Life, were among the ramifications that followed. Customers learned a vital lesson from the hacking scandal: there is always a risk of hacking when using the Internet. As a result, nothing on the Internet can be totally untraceable and anonymous. Even individuals who had paid $19 to have their data removed discovered that certain transaction data remained on. (Basu, 2015)

2. Background of the Scandal:

The scandal begins when a group of hackers going by the name "Impact Team" broke through Ashley Madison's security measures and obtained illegal access to the internal data of the website. Millions of users' private information, including names, email addresses, physical addresses, and credit card numbers, was compromised because of this hack. (Blasiola, 2016)

The Impact Team demanded that Ashley Madison and its sibling website, Established Men, be taken offline permanently or else they would reveal this wealth of information. The Impact Team threatened to make the stolen data publicly available on the internet, but the owners of the website refused to comply with their requests. The people involved suffered significant repercussions because of the Ashley Madison data leak. Many people experienced negative effects on their personal and professional lives because of having their private behaviors made public. A few went through broken relationships, divorce, lost their jobs, and even faced blackmail and harassment. (Boyd, 2011)
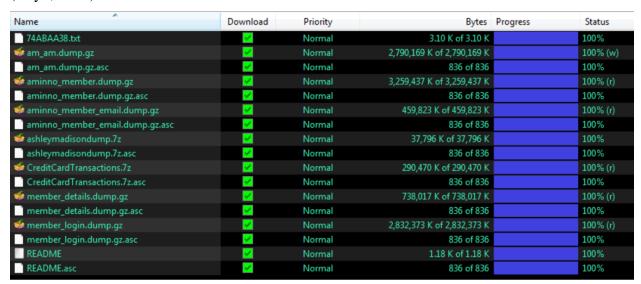
Name	Download	Priority	Bytes	Progress	Status
74ABAA38.txt	✅	Normal	3.10 K of 3.10 K		100%
am_am.dump.gz	✅	Normal	2,790,169 K of 2,790,169 K		100% (w)
am_am.dump.gz.asc	✅	Normal	836 of 836		100%
aminno_member.dump.gz	✅	Normal	3,259,437 K of 3,259,437 K		100% (r)
aminno_member.dump.gz.asc	✅	Normal	836 of 836		100%
aminno_member_email.dump.gz	✅	Normal	459,823 K of 459,823 K		100% (r)
aminno_member_email.dump.gz.asc	✅	Normal	836 of 836		100%
ashleymadisondump.7z	✅	Normal	37,796 K of 37,796 K		100%
ashleymadisondump.7z.asc	✅	Normal	836 of 836		100%
CreditCardTransactions.7z	✅	Normal	290,470 K of 290,470 K		100% (r)
CreditCardTransactions.7z.asc	✅	Normal	836 of 836		100%
member_details.dump.gz	✅	Normal	738,017 K of 738,017 K		100% (r)
member_details.dump.gz.asc	✅	Normal	836 of 836		100%
member_login.dump.gz	✅	Normal	2,832,373 K of 2,832,373 K		100% (r)
member_login.dump.gz.asc	✅	Normal	836 of 836		100%
README	✅	Normal	1.18 K of 1.18 K		100%
README.asc	✅	Normal	836 of 836		100%

Figure 2: Links to the data dump. (McNeil, 2015)

The controversy brought attention to wider societal concerns about privacy and the morality of accessing and sharing sensitive information, in addition to online platforms' susceptibility to data breaches. It sparked discussions on the obligations placed on businesses to protect user data, the ramifications of internet anonymity, and the morality of infidelity and private behavior. (A.Acquisti, 2006)

The Ashley Madison controversy highlighted the intricate relationship between technology, privacy, and social norms in the digital era and served as a sobering warning of the possible dangers of providing private information to websites. (vitak, 2015)

Figure 3:The statement released by Impact Team (McNeil, 2015)

3. Legal Issues:

The Ashley Madison scandal prompted various legal repercussions, including class-action lawsuits and allegations of fraud. Questions arose regarding the site's practices, such as the alleged creation of fake profiles to lure users and questionable data scrubbing services. Additionally, the breach highlighted the importance of stringent data protection measures and the potential liabilities faced by companies failing to safeguard user information adequately.

Figure 4:A snippet of the message left behind by the Impact Team. (krebsonsecurity.com, 2022)

3.1 Data Breach Lawsuits:

In response to a data breach impacting 37 million members, Ashley Madison's owner, Ruby Corp, will pay $11.2 million in a settlement, subject to court approval. The corporation denies wrongdoing while acknowledging the impact on users. The settlement permits customers to recover up to $3,500 based on verifiable losses. Previously, Ruby paid $1.66 million to resolve an FTC investigation. Lawyers may receive one-third of the settlement as fees. The case is now pending in the Eastern District of Missouri. (Stempel, 2017)

3.2 Privacy Violations: (4th amendment violation)

Invasions of privacy can have major effects on your home life, to your reputation, to your profession. The Ashley Madison privacy breach is particularly concerning given the nature of the website and the kinds of user information it carries. On most social media networks, members may delete their accounts. This does not necessarily mean that user's data gets erased. In most circumstances, the data remains on the website's systems. Ashley Madison offered to permanently remove user information in exchange for money. This is called a "hard delete", "paid delete" or "full delete". User's true names, addresses and communication history were meant to be erased. Numerous consumers have called Charney Lawyers claiming to have paid for the "full delete" option, only to find that their data was never destroyed and later revealed in this privacy breach. In any event, various experts criticized the paid delete option as unethical. Following the hacking scandal, the Toronto star reported that Ashley Madison has now promised to delete user information for free. (Macri A. , 2022)

3.3 Consumer Protection: (Federal act violation)

'Life is short have an affair' the slogan of Ashley Madison scandal highlighted issues related to consumer protection and promised to provide secure services to protect users from harm but AshleyMadison.com deceptively promoted itself as "100% secure and anonymous," engaging consumers with fake profiles and luring them into premium subscriptions. Despite claims of privacy, the site's $19

The "Full Delete" option failed to remove all user information, including critical details such as names, preferences, and financial information. This breach of privacy had serious consequences for people seeking confidentiality in their online activity. (Schifferle, 2016)

3.4 Cybersecurity Regulation:

The Ashley Madison breach sparked debate over the necessity for stricter cybersecurity legislation to protect users' sensitive information from illegal access and misuse. Lawmakers and policymakers investigated how to improve cybersecurity standards, promote transparency, and hold businesses accountable for breaches and data mismanagement. (Orji, 2012)

4. Social Issues:

The scandal had profound social implications, leading to ruptured relationships, family conflicts, and even suicides among affected individuals. The revelation of high-profile users further intensified public scrutiny and condemnation. Moreover, concerns emerged regarding the broader societal attitudes towards infidelity and the erosion of trust in online platforms promising anonymity and discretion.

4.1 Impact on Relationships:

The Ashley Madison breach exposed people's extramarital affairs, which had far-reaching ramifications for personal relationships. University of Central Florida psychologists discovered that infidelity-related disclosures, such as those originating from the Ashley Madison breach, might cause mental discomfort, relationship conflict, and even divorce (Amato, 2003). Furthermore, a study published in the Journal of Marriage and Family highlighted the emotional toll of infidelity on betrayed spouses, with common reactions including betrayal, rage, and mistrust (Allen, 2005). The breach highlighted the delicate dynamics of trust and intimacy in relationships, as well as the terrible impact breaches have on people's personal lives.

4.2 Privacy and Data security concerns:

The Ashley Madison data hack highlighted the critical need for stronger privacy and data security protections in the digital era. Users give sensitive personal information to internet platforms, expecting it to be secure from unauthorized access. However, hacks like this underscore the susceptibility of such data, as well as the risks connected with revealing personal information online. According to (Ponemon Institute., 2020), the average cost of a data breach in 2020 was $3.86 million, highlighting the substantial financial ramifications for businesses and the significance of strong security measures. Furthermore, a study published in the Journal of Consumer Research found that data breaches might reduce consumer trust and loyalty to affected organizations, emphasizing the long-term influence on company reputation and consumer interactions (Guo, 2017)

4.3 Legal Ramifications:

The Ashley Madison leak sparked a flurry of class-action lawsuits, raising critical legal concerns regarding data security and business responsibility. Legal academics have questioned the scope of firms' responsibility to protect user data and the potential consequences of failing to do so. Harvard Law Review research examined the legal landscape around data breaches and concluded that firms may be held accountable for negligence if proper security measures are not implemented to secure user data (Bamberger, 2010). Furthermore, the hack sparked debate on the necessity for regulatory reforms to enhance data protection laws and make companies accountable for data breaches (Richards, 2015)

4.4 Ethical Considerations:

The Ashley Madison leak prompted ethical concerns about organizations' responsibilities to protect user privacy and the cultural stigma connected with adultery. Ethicists have questioned the ethical implications of internet platforms that allow for extramarital affairs, as well as the possible harm caused by user confidentiality breaches. Research published in the Journal of Business Ethics looked at the ethical implications of data breaches and concluded that businesses have a moral imperative to prioritize customer privacy and security (Gupta, 2019). Furthermore, the hack sparked debate regarding the ethics of data use in academic research and the significance of protecting people's privacy rights (Salter, 2018)

4.5 Broader Implications for Online security: Digital trust

The Ashley Madison incident underscored the larger issues of maintaining privacy and security in an increasingly linked and data-driven world. Cybersecurity experts have stressed the importance of preemptive measures to reduce the risk of data breaches and secure user information from bad actors. World Economic Forum research listed cybersecurity as one of the most serious global concerns, emphasizing the importance of joint efforts to combat cyber threats (World Economic Forum. , 2020). Furthermore, the incident served as a wake-up call to businesses across industries about the need to invest in strong security measures and applying best practices to protect customer data (Symantec, 2021)

5. Ethical Issues:

Ashley Madison's ethical discussions revolved around the morality of advertising extramarital affairs, as well as the site's alleged deceptive methods. While some supported users' privacy and individuality, others criticized the platform as exploitative and damaging to relationships. The hacking incident generated ethical problems about the perpetrators' goals and methods, balancing desires for justice with the illegality of their conduct. (2015)

5.1 Virtue Theory:

The Ashley Madison data hack raises serious questions about the company's moral integrity and commitment to virtuous action. Virtue ethics emphasizes the necessity of instilling moral values like honesty, integrity, and accountability. Ashley Madison's promotion of extramarital affairs goes against ideals like honesty and fidelity, and their failure to appropriately safeguard user data reveals a lack of integrity and accountability for their clients' privacy. As a result, the company's acts are considered unethical under virtue ethics since they disrespect fundamental moral ideals. (Tomlinson, 2012)

5.2 Deontological ethics:

Deontological ethics, which emphasizes duties, regulations, and obligations, also condemns Ashley Madison's actions in the data breach issue. According to deontological principles, the corporation owed a fundamental duty to protect the privacy and confidentiality of its users' information, regardless of the repercussions. The violation not only broke this responsibility, but it also violated consumers' trust, resulting in a breach of ethical obligations regardless of any advantages or costs. (Prichard, 2024)

5.3 Utilitarianism:

Utilitarianism, is a consequentialist ethical philosophy that assesses actions based on their overall implications, further condemns Ashley Madison's behavior. While the site may have been enjoyable for some users seeking extramarital affairs, the hack resulted in considerable harm to millions of customers whose privacy was violated. From a utilitarian standpoint, the harm inflicted

by the breach considerably surpasses any potential gains from the service, making Ashley Madison's actions unethical under utilitarian grounds. (Mill, 2001)

5.4 Rights:

Finally, rights ethics, which focuses on the protection of individual rights and freedoms, strongly criticizes the Ashley Madison breach. Users of the site had a reasonable expectation that their personal information would be kept secret, and the breach infringed this basic right to privacy and confidentiality without their knowledge. Under rights ethics, the breach is considered unethical because it violated users' fundamental rights, emphasizing the company's failure to respect its rights. (Kapoor,2019)

6. Professional Issues:

From a professional standpoint, the Ashley Madison scandal underscored the importance of ethical conduct and transparency in business operations. Criticisms against the company's business model and security protocols highlighted the need for responsible corporate governance and accountability. The fallout from the breach tarnished the reputation of Ashley Madison and served as a cautionary tale for organizations operating in sensitive industries.

On the one hand, there's the viewpoint of the users whose data was compromised. From this standpoint, the breach raises serious legal and ethical problems about privacy rights, data protection, and organizations' obligations to preserve sensitive information. Users trusted Ashley Madison with their personal information in the expectation of privacy, and the breach violated that trust. The legal measures launched against Ashley Madison underscore firms' potential responsibility for failing to sufficiently protect consumer data, as well as the need of regulatory compliance in resolving data security concerns. (Buchanan, 2021)

On the other hand, there is Ashley Madison, the company's point of view, which is dealing with legal, financial, and reputational issues because of the breach. Ashley Madison's handling of the incident, including communication with affected individuals and response to claims of deceptive statements, has been questioned. The corporation must traverse a complex legal landscape, which includes class action lawsuits and regulatory inquiries, as well as deal with reputational harm and restore customer trust. The breach emphasizes the necessity of transparency, responsibility, and ethical behavior when managing data security incidents and limiting their impact on stakeholders. (Schwartz, 2016)

6.1 Company perspective

1. Honest and fair:

The well-known internet dating site Ashley Madison rose to prominence with the tagline "Life is short, have an affair," portraying itself as a covert channel for people looking for extramarital affairs. With twelve million users in the United States and eighteen million worldwide, the website promoted communication between users via a credit-based system. But the "Impact Team," a gang of hackers, broke through its security system and exposed private user information, including names, email addresses, and payment information, shattering the company's assurance of

anonymity. A series of negative events, such as court disputes, public outcry, and significant societal ramifications, followed this breach. The Ashley Madison controversy acted as a clear warning about the weaknesses present in internet platforms. (Anderson L. , 2014)

2. Respect and protect personal privacy:

An essential ethical precept is protecting and preserving one's personal privacy, especially in the age of internet sites like Ashley Madison. Users of these sites have faith that the security and confidentiality of their personal data will be maintained. Ensuring that users have control over their data and that it is only used for the purposes for which they have given consent is essential to respecting their privacy. Furthermore, putting strong security measures in place to stop illegal access and data breaches is another aspect of privacy protection. This principle was broken in the Ashley Madison case, which had serious repercussions for the involved parties due to the invasion of user privacy. Organizations that handle sensitive user data must be committed to openness, responsibility, and moral conduct to protect individual privacy. (Macri L. , 2022)

3. Thorough Planning and Scheduling:

From a business standpoint, thorough planning and scheduling entails creating specific plans and deadlines for efficiently managing activities, resources, and projects. This method guarantees that objectives are well-defined, due dates are fulfilled, and resources are distributed effectively. Businesses that put a high priority on careful planning and scheduling are better able to manage challenging projects, reduce risks, and adjust to shifting market conditions. (Conway, 2021)

6.2 Hacker perspective

1. Respect property rights:

Preserving the privacy and security of user data is necessary to honor property rights on Ashley Madison. With the expectation of privacy and discretion, users entrust the platform with sensitive information, such as personal details and conversation history. A violation of property rights occurs when someone betrays this trust by improperly managing or revealing user data without authorization. In addition, if Ashley Madison's promised "full delete" option which allegedly erased user information for a fee isn't carried out as promised, it creates ethical questions. Users are entitled to control over the information about them, and any illegal use or distribution of that information is a violation of their property rights. Therefore, upholding strong data security

protocols, being open about data practices, and considering user preferences for data management are crucial to protecting property rights on Ashley Madison. (Manley, 2016)

2. Understand relevant law:

From the viewpoint of a hacker, comprehending pertinent legislation entails looking at the legal structures and guidelines controlling digital privacy, computer crimes, and cybersecurity. This viewpoint entails being aware of regulations pertaining to data protection, intellectual property, and electronic communications, as well as others like the Computer Fraud and Abuse Act (CFAA), which forbids illegal access to computer systems. Hackers may evaluate the legal risks and ramifications of their activities by considering variables such jurisdictional distinctions, tactics used by law enforcement, and possible fines for online crimes. Comprehending case law and legal precedents can also offer valuable perspectives on how courts construe and implement cybersecurity and hacking-related legislation. Hackers can reduce the possibility of legal consequences and make wise decisions about their actions by being aware of the legal environment. (Zetter, 2015)

3. Respect confidentiality:

From the standpoint of a hacker, maintaining confidentiality requires knowing and abiding by ethical guidelines when managing sensitive data that is obtained through hacking activities. Hackers must think about the moral ramifications of their activities and the possible harm that could arise from revealing sensitive information, even though they may use vulnerabilities to obtain illegal access to systems or data. (Daniel, 2019)

7. Conclusion:

In conclusion, the Ashley Madison scandal serves as a cautionary tale about the potential consequences of inadequate data security measures and ethical lapses in online platforms. The breach not only exposed millions of users' private information but also led to widespread legal, social, and professional repercussions. From a legal standpoint, the incident sparked numerous lawsuits and regulatory inquiries, highlighting the need for stronger data protection laws and enforcement mechanisms. Socially, the breach caused ruptured relationships, emotional distress, and erosion of trust in online privacy. Professionally, it underscored the importance of responsible corporate governance, transparency, and ethical conduct in safeguarding user data and maintaining business sustainability. Moving forward, the Ashley Madison scandal should serve as a wake-up call for businesses to prioritize data security, ethical behavior, and customer trust to prevent similar incidents and mitigate their impact on stakeholders. (Hudson, 2024)

7.1 Brainstorming:

1. Reputation Management:

    - Strategic planning: Develop a proactive reputation management plan to rebuild trust and credibility. (Fombrun, 2020)
    - Media strategy: Craft a strategic approach to manage media coverage and public perception effectively. (Dozier, 2021)

2. Customer Relations:

    - Compensation and restitution: Offer appropriate compensation and restitution to affected users to address grievances. (Smith, 2018)
    - Customer support: Establish a dedicated customer support team to address inquiries and concerns promptly. (Anderson J. , 2019)

3. Long-Term Strategy:

    - Collaboration with cybersecurity firms: Forge partnerships with cybersecurity experts and industry associations to strengthen security measures.
    - Continuous evaluation: Implement mechanisms for ongoing assessment and improvement of security practices.

7.2 Analysis:

1. Reputation Management:

    - Media monitoring: Monitor media coverage and public sentiment to gauge the effectiveness of reputation management efforts. (Lee, 2019)

    - Crisis response evaluation: Assess the organization's response to the crisis and identify lessons learned for future incidents.

2. Customer Relations:

    - Satisfaction measurement: Measure customer satisfaction with the compensation and support provided and address any unresolved issues promptly.

    - Trust rebuilding: Track progress in rebuilding trust among users and implement strategies to strengthen customer relationships.

3. Long-Term Strategy:

    - Performance metrics: Establish key performance indicators (KPIs) to measure the effectiveness of long-term security initiatives and track progress over time.

    - Adaptation and flexibility: Remain adaptable to evolving cybersecurity threats and regulatory changes, adjusting strategies as needed to ensure ongoing compliance and protection.

8. References

(2015, july). Retrieved from https://theguardian.com/commentisfree/2015/jul/21/it-hurts-but-im-going-to-defend-ashley-madison-and-37-million-cheaters

(2022). Retrieved from krebsonsecurity.com: https://krebsonsecurity.com/2022/07/a-retrospective-on-the-2015-ashley-madison-breach/

A.Acquisti. (2006). Awareness, information sharing and privacy.

Allen, E. S. (2005). *Journal of Marriage and Family*.

Amato, P. &. (2003). People's reasons for divorcing: Gender, social class, the life course, and adjustment. . *Journal of Family Issues*.

Anderson. (2014). Retrieved from https://adg-qa-assets.s3-ap-southeast-2.amazonaws.com/images/6minutes/AM_2014_Anderson_Study_-77505.PDF

Anderson, J. (2019). Effective Strategies for Building Customer Support Teams. *Customer Relationship Management Journal*.

Anderson, L. (2014). *Inside Ashley Madison*. Retrieved from Forbes: https://www.forbes.com/sites/kashmirhill/2014/12/10/inside-ashley-madison-calls-from-crying-spouses-fake-profiles-and-the-hack-that-changed-everything/ [Accessed on 28th April 2024].

Bamberger, K. A. (2010). *Privacy on the books and on the ground*.

Basu, T. (2015, August 23). Retrieved from https://time.com/4007374/ashley-madison578-million-lawsuit-canada/

Blasiola, S. (2016, october 8). Retrieved from file:///C:/Users/user/Desktop/ojsAdmin,+Blasiola.pdf

Boyd, D. (2011). social privacy in networked publics. 29.

Buchanan, J. (2021). The Ashley Madison Data Breach. *A Retrospective Analysis of Corporate Accountability and Privacy Law*.

Conway, T. J. (2021, march 2). Retrieved from Medium: https://medium.com/the-scarlett-letter/the-first-30-days-on-ashley-madison-a-male-perspective-887404e5dcf6

Daniel. (2019). Retrieved from QUT: https://eprints.qut.edu.au/119373/1/IRV_Ashley_Madison_FINAL.pdf

Dozier. (2021). *The Role of Media in Crisis Management.*

firestone, j. (2016, january 19). Retrieved from https://www.expertinstitute.com/resources/insights/ashley-madison-data-breach-lawsuits-consolidated-mdl/

Fombrun. (2020). *Reputation Management: The New Rules of Corporate Communication.*

Guo, L. Z. (2017). How do consumers react to data breaches in online stores? The role of brand reputation and e-trust. *Journal of Consumer Behaviour*.

Gupta, S. &. (2019). Ethical consideration of data breach: A literature review. Journal of Business Ethics.

http://harbert.auburn.edu. (2022). Retrieved from https://harbert.auburn.edu/binaries/documents/center-for-ethical-organizational-cultures/cases/ashley-madison.pdf

Hudson. (2024, march 4). *HR*. Retrieved from https://hudsonreporter.com/lifestyle/ashley-madison-review/

Kapoor, R. (2019, August 20). Retrieved from Sage journals: https://journals.sagepub.com/doi/full/10.1177/2277401719870004

Lee, J. &. (2019). Social Media Monitoring and Crisis Management: A Case Study Analysis. *Journal of Public Relations Research*.

Macri, A. (2022). STATEMENT FROM AVID LIFE MEDIA.

Macri, L. (2022). *Ashley Madison Changes Policy After Privacy Breach*. Retrieved from Charney Lawyers: https://charneylawyers.com/ashley-madison-class-action-lawsuit-privacy/

Manley, A. (2016, April 10). Retrieved from slide share: https://www.slideshare.net/AnnaManley/life-is-short-sue-everyone-legal-perspectives-on-the-ashley-madison-hack

McNeil, A. (2015). Retrieved from Malware bytes: https://www.malwarebytes.com/blog/news/2015/08/for-sign-off-times-up-ashley-madison-data-released

Mill, J. S. (2001). *Utilitarianism*. 52 Eby Street South kitchener: Batoche Books Limited.

Moscaritolo, A. (2015, August 19). Retrieved from https://www.pcmag.com/news/how-to-see-whos-in-the-ashley-madison-database

Orji, U. J. (2012, september). Retrieved from The Ashley Madison breach sparked debate over the necessity for stricter cybersecurity legislation to protect users' sensitive information from illegal access and misuse. Lawmakers and policymakers looked into how to improve cybersecurity standards, promo

Ponemon Institute. (2020). Retrieved from Cost of a Data Breach Report.: https://www.ibm.com/security/data-breach

Prichard, I. K. (2024, March 28). *deontological ethics*. Retrieved from www.britannica.com: https://www.britannica.com/topic/deontological-ethics

Richards, N. M. (2015). *The dangers of surveillance*. *Harvard Law Review*.

22085653

Salter, J. &. (2018). Research ethics and data breaches in qualitative inquiry: Protecting confidentiality and trust. Qualitative Psychology.

Schifferle, L. W. (2016, December 14). Retrieved from https://www.ftc.gov/business-guidance/blog/2016/12/ashley-madison-settles-ftc-over-data-security

Schwartz, P. M. (2016). The Ashley Madison Breach. *A Matter of Trust and Digital Vulnerability*.

Smith, A. &. (2018). Compensation Strategies for Data Breach Victims. *Journal of Information Privacy Law*.

Stempel, J. (2017, july 15). Retrieved from https://www.reuters.com/article/idUSKBN19Z2F3/

Symantec. (2021). *Internet Security Threat Report. Retrieved from* . Retrieved from https://www.broadcom.com/company/newsroom/press-releases/2021/symantec-releases-2021-internet-security-threat-report

Tomlinson, T. (2012, July). Retrieved from Research Gate: https://www.researchgate.net/publication/300201895_Virtue_Theory

vitak, j. (2015). balancing audience and privacy tensions on social network sites. *strategies of highly engaged users*.

(2020). *World Economic Forum*. .

Zetter, K. (2015, August 18). Retrieved from wired.com: https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/

22085653