REPORT ON

EXAMING DATA BREACH AND ETHICAL CHALLENGES IN EXPEDIA'S DATA PRACTICES

DATA 5120 01 24SQ

DATA SCIENCE, LAW AND ETHICS

Submitted by

LAVANYA BUNADRI

ABSTRACT

This report devolves significant data security challenges occurred by Expedia. Where Expedia, is a major travel sector, faced notable data security obstacles after experiencing a data breach in November 2020. The breach occurred due to a misconfiguration of AWS S3 bucket, resulting in the exposing the millions of personal records. Furthermore, there were claims of unauthorized sharing of data, such as the misappropriation of marketing data from competitors, Reservation Counter. These events exposed significant ethical and security deficiencies in the organization.

INTRODUCTION

Expedia Group provides travel services like hotel reservations, flight bookings, rental cars, and vacation bundles. Over time, Expedia has experienced substantial growth, solidifying its position as a top player in the travel sector. Its goal is to provide a range of creative travel choices to ensure that global travel is within reach for all. Expedia have many popular brands such as Hotels.com, Orbitz, Travelocity, and Hotwire, catering to millions of customers globally.

However, the company encountered significant data security issues in November 2020 after a misconfigured Amazon S3 bucket led to a data breach exposing millions of personal records. Furthermore, claims of unauthorized data sharing with an affiliate, Reservation Counter, brought attention to significant ethical and security concerns. These occurrences highlight the significance of strong data protection measures to uphold customer confidence and meet legal requirements. This report examines these issues, emphasizing the importance of tackling these weaknesses to protect Expedia's image and customer information.

ISSSUES IDENTIFIED

DATA BREACH INCIDENT

A data breach incident at Expedia in November 2020 exposed tens of millions of personal records due to a misconfigured AWS S3 bucket. This breach allowed unauthorized access to sensitive customer information like names, addresses, and possibly payment details. The reason for this was weak security settings and poor monitoring, which didn't stop unauthorized access to the cloud-stored data. The breach led to potential legal fines under laws like the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR), damaged customer trust, and hit Expedia's reputation.

Because of this compromise, Expedia had to review and update its data security practices, including strengthening security settings. The incident underlined the importance of strong data security procedures and persistent attention in protecting sensitive consumer information. Fixing these flaws is critical for avoiding future breaches and recovering customer and stakeholder trust.

UNAUTHORIZED DATA SHARING

Unauthorized data sharing involves the improper or illegal distribution of data to individuals or entities without the right to access it. In the case of Expedia, the company was accused of stealing marketing data from its affiliate, Reservation Counter, and sharing it with a competitor. This is a serious breach of business ethics and confidentiality agreements, showing major weaknesses in how Expedia controls data access and usage. Unauthorized data sharing can lead to big legal problems, like lawsuits and fines under data protection laws.

Unauthorized data sharing impacted the company's brand and ethical standards, in addition to the legal penalties. Such activities threaten the relationship between the corporation and its affiliates, customers, and the public. This loss of trust might make it more difficult for Expedia to compete, as individuals may be unwilling to deal with or buy from a firm that is perceived as untrustworthy. The negative publicity from these unethical tactics might have a long-term impact on Expedia's reputation, impacting consumer loyalty and market position. To address these vulnerabilities, Expedia must thoroughly review and reinforce its internal policies and controls, preventing future improper data sharing and restoring faith in its ethical processes.

RECOMMENDATIONS

OPERATIONAL RESPONSE

Implement a Comprehensive Data Governance Framework

Expedia should implement a robust data governance structure to efficiently manage and protect data throughout the firm. This framework will solve internal control shortcomings while also ensuring compliance with legal and ethical norms. A data governance framework should define specific data management policies, procedures, and responsibilities. It should guarantee that data handling processes are consistent with legislative requirements and ethical standards, notably those outlined in US data privacy regulations such as the California Consumer Privacy Act (CCPA).

Implementation Steps:

- Form a cross-functional Data Governance Committee with representatives from IT, legal, compliance, and business areas. Assign specific roles and duties for data management and protection.
- Develop data policies and procedures. Developing comprehensive data management policies that address data classification, access control, retention, and sharing. Then it confirms that these rules are compliant with applicable legal and regulatory obligations, such as the CCPA and GDPR.
- Implement data stewardship. Designate data stewards in each department to oversee data handling methods and guarantee compliance with data policy. This includes delegating tasks to specific individuals or teams to ensure data quality, integrity, security, and regulatory compliance.
- Conducting regular data audits. Conduct periodic audits to ensure compliance with data policies and identify areas for improvement. Use audit findings to update policies and address any gaps in data protection
- By developing and conducting training programs to educate staff on data governance, security, and their role in data protection. Include training on how to identify and respond to data breaches and illegal data access attempts.
- Monitor and report on data governance: Use monitoring technologies to track data access and usage throughout the organization. Create frequent reports for senior management and the data governance committee to assess performance and compliance.

A comprehensive data governance framework ensures that data is managed securely and ethically, reducing the risk of data breaches and unauthorized data sharing. By establishing clear policies and responsibilities, Expedia can create a culture of accountability and compliance, protecting both customer data and the company's reputation.

TECHNICAL MECHANISM

Advanced Data Encryption and Access Controls

Expedia should implement advanced data encryption and strict access controls to secure sensitive data and prevent unauthorized access. Data encryption and access controls are essential technical mechanisms that protect sensitive data from unauthorized access and potential breaches. By encrypting data both at rest and in transit, and by implementing robust access control measures, Expedia can ensure that only authorized users can access.

Implementation Steps:

- Data Encryption: Use Advanced Encryption Standard (AES) to encrypt all sensitive data stored in databases, file systems, and cloud storage. Encryption in Transit Implement Transport Layer Security (TLS) to encrypt data transmitted between systems, ensuring that data remains secure during transfer.
- Access Controls: Role-Based Access Control defines and enforces access policies based on user roles within the organization. Limit access to sensitive data to only those employees who need it to perform their job functions.
- Multi-Factor Authentication: Require MFA for accessing sensitive systems and data. This adds an additional layer of security by requiring users to provide two or more verification factors.
- Secure Key Management: Implement a secure key management system to generate, distribute, rotate, and store encryption keys. Use hardware security modules (HSMs) to protect keys from unauthorized access.
- Audit and Monitoring: Audit Logs enable detailed logging of all access to sensitive data, including successful and failed access attempts, changes to access controls, and key management activities. Real-Time Monitoring: Implement real-time monitoring tools to detect and respond to unauthorized access attempts and suspicious activities promptly.

Implementing advanced encryption and access controls ensures that sensitive data remains protected, even if it is accessed or intercepted by unauthorized individuals. Encryption safeguards the confidentiality and integrity of data, while access controls and monitoring provide robust security measures to prevent and detect unauthorized access. By employing these technical mechanisms, Expedia can significantly reduce the risk of data breaches and unauthorized data sharing, ensuring compliance with regulatory requirements and maintaining customer trust.

COST AND EFFORT CONSIDERATION:

- To achieve the recommendation Expedia should follow some terms and conditions where Expedia is a large, well-established online travel company with significant resources and technical expertise. The implementation of advanced data encryption and access controls is well within the capabilities of such an organization.
- Annual Revenue with substantial annual revenue, Expedia should associate with cost implementing these technical measures are justified by the need to protect sensitive customer data and comply with regulatory requirements.
- Expedia should manage the number of employees, i.e., thousands of people, including IT and security professionals with the expertise required to manage and implement complex security systems. The presence of skilled personnel ensures that the proposed technical measures can be effectively deployed and maintained.
- Technical knowledge of Expedia's workforce, the implementation of advanced encryption and access control mechanisms is realistic. Training programs can be developed to ensure all employees understand and adhere to new security protocols.
- Size and Location of Expedia serves millions of customers globally, making data protection is a critical priority. Implementing these technical measures will help safeguard sensitive information across all regions, ensuring compliance with various international data protection laws, such as GDPR and CCPA.

By considering these factors, the proposed technical mechanism of advanced data encryption and access controls is both realistic and achievable for Expedia. These measures will enhance the company's data security posture, mitigate risks, and ensure compliance with regulatory standards, ultimately protecting customer trust and maintaining business integrity**.**

LEGAL AND REGULATORY RECOMMENDATIONS

Legal and Regulatory requirements identified by group presentation

- **California Consumer Privacy Act (CCPA):**

The CCPA requires businesses to use proper security measures to protect consumer data and to quickly inform individuals if a data breach happens.

Current Practices and Gaps are:

- Data Protection: Expedia's weak security measures caused a data breach, showing they didn't protect data well enough.
- Breach Notification: Expedia did not inform affected individuals quickly about the breach, breaking the CCPA's rules for timely notification.

Recommendations Effectively Close the Gaps and Risks:

Operational Response: Implementing a comprehensive data governance framework will ensure robust data protection policies and regular audits, aligning with CCPA requirements.

Technical Mechanism: Deploying advanced encryption and strict access controls will protect sensitive data, ensuring it is securely stored and processed, meeting CCPA's data protection standards.

- **Payment Card Industry Data Security Standard:**

PCI DSS requires businesses to securely store and hash personal identifying information, including credit card security codes, to protect against data breaches.

Current Practices and Gaps are:

- Data Storage: Expedia did not store or hash personal identifying information, including credit card security codes, in compliance with PCI DSS, leading to a significant data breach.

Recommendations Effectively Close the Gaps and Risks:

Operational Response: Strengthening internal data governance policies to ensure secure data storage and hashing practices, regular compliance audits, and employee training on data security protocols will align with PCI DSS requirements.

Technical Mechanism: Implementing secure key management systems, regular key rotation policies, and advanced encryption techniques will protect sensitive data, ensuring it is stored and processed securely, meeting PCI DSS standards.

- **Ethical issue identified by the group is:**

Transparency and Accountability

Expedia failed to inform stakeholders promptly about the breach, learning from news reports instead.

Complement to Legal Issues:

Making sure to communicate quickly and clearly follows the CCPA's rules for notifying people about breaches. Being open and responsible meets legal requirements and builds trust with stakeholders.

By dealing with these ethical issues, Expedia can better follow the law, win back customer trust, and keep high ethical standards in managing data.

CONCLUSION

Effectively solving data privacy and security issues is vital for Expedia to keep its good reputation and customer trust. Implementing the recommended operational and technical measures will greatly improve Expedia's data privacy and security. By using a comprehensive data governance framework and advanced encryption and access controls, Expedia will fix current gaps and ensure strong data protection and compliance with CCPA and PCI DSS regulations. These steps will also support ethical standards, promoting transparency and accountability, which are essential for maintaining consumer trust.

Although these measures require time and effort, the long-term benefits include better legal compliance, stronger ethical practices, and an improved reputation. Ultimately, these actions will ensure that Expedia remains a trusted and responsible organization in the digital age, protecting customer data and rights.

REFERENCES

- https://www.expediagroup.com/home/default.aspx
- https://en.wikipedia.org/wiki/Expedia_Group
- https://www.independent.co.uk/travel/news-and-advice/expedia-data-breach-hotel-software-prestige-booking-b1720489.html
- https://topclassactions.com/lawsuit-settlements/privacy/data-breach/expedia-data-breach-amazon-infosec-accused-in-class-action-lawsuit/
- https://skift.com/2017/04/03/expedia-sued-by-affiliate-for-allegedly-stealing-data-and-handing-it-to-a-competitor/