Avinash Bunga

Information Systems and Business Analytics, Park University

CIS611HOS1P2024 - Introduction to Business Analytics

Professor: Timur Rakhimov

February 22, 2024

Unit 7: Discussion

Navigating the Intersection of Data Privacy and Security in Analytics and Technology Roles

Introduction

In the dynamic landscape of analytics and technology, specific professional roles stand out for their significant contributions to data privacy and security. In today's dynamic organizational landscapes, certain roles are pivotal due to their direct involvement in overcoming many challenges and duties. These professionals are at the forefront of adhering to continuously changing regulations and maintaining the ethical handling of information, thereby establishing a foundation of trust and integrity within the framework of digital operations. In our discussion, we will investigate the distinct contributions each of these roles makes to data protection and cybersecurity, thus defining the contours of contemporary data management and security strategies. This examination is essential to grasp the comprehensive responsibilities involved in managing data within the technological domains prevalent in our current era (Correll, 2019; Cote, 2021; Pınarbaşı, 2022; Vidgen, Hindle, & Randolph, 2020).

My Definition of Data Security (Informed by Practical Application in Business Analytics): Based on my experiences as a fraud analyst and insights from the (Vidgen et al., 2020) study, I define data security as the comprehensive strategies and actions implemented to protect digital information from unauthorized access, disclosure, alteration, or destruction. This concept includes technical measures like encryption and secure network architectures and organizational practices such as access controls and frequent security audits to guarantee the integrity and confidentiality of data against threats and vulnerabilities (Correll, 2019; Cote, 2021; Pınarbaşı, 2022; Vidgen et al., 2020).

Example: Enhancing Data Security at Uber

- **Background and Context:** Uber has faced multiple data breaches over the years, necessitating a revamp of their data security protocols. This example is informed by the comprehensive measures required by past incidents and legal settlements (Insider Lab, 2022; Pınarbaşı, 2022).
- **Implementing End-to-End Encryption:** Uber has enhanced its app's security by incorporating comprehensive encryption for all user interactions. By doing so, the company aims to safeguard the confidentiality of conversations and data shared between passengers and drivers, ensuring that such information remains inaccessible to external threats (Insider Lab, 2022; Uber, 2022).
- **Upgrading Access Management Systems:** The company introduces stringent access management protocols. These include biometric authentication and role-based access controls, limiting data access to authorized personnel only (Insider Lab, 2022; Uber, 2023).

- **Regular Security Assessments:** Uber commits to continuous security evaluations, involving third-party cybersecurity experts to conduct penetration tests and identify potential system vulnerabilities (Insider Lab, 2022; Tata & Mitsunari, 2020).
- **Response to Historical Breaches:** These enhancements are part of Uber's ongoing efforts to address security flaws exposed by previous breaches and to meet regulatory requirements imposed following legal actions (Insider Lab, 2022; Uber Team, 2022).
- **Objective and Expected Outcomes:** The aim is to fortify Uber's data security framework, preventing future unauthorized access and building trust with users and stakeholders (Insider Lab, 2022).

My Definition of Data Privacy (Derived from Cote, 2021): In line with Cote's insights, data privacy means a person has control over their personal details. It highlights the importance of being open, getting permission, and treating people's information with care. From my time analyzing fraud, this means we must always ask customers clearly if we can use their information, making sure we respect their privacy (Buckbee, 2023; Cote, 2021).

Example: Data Privacy Enhancements at Uber

- **Situation**: In response to past privacy concerns and breaches, Uber overhauls its data privacy approach to regain user trust and comply with global data protection regulations (Insider Lab, 2022; Uber Team, 2022; Wu, 2018).

- **Action**: Uber initiates a comprehensive data privacy program that includes clearer communication with users about how their data is used. They introduced a new section in the app that allows users to review and manage the data Uber has on them, such as trip history and account information. This feature is designed to increase transparency and give users control over their personal data, aligning with recommendations to improve transparency and restrict employee access to user data (Insider Lab, 2022; Wu, 2018).
- **Result**: Users now have a clearer understanding of what data Uber collects and why. The new privacy controls allow users to opt out of certain data collection practices, enhancing their autonomy over personal information. This results in improved user trust and satisfaction, reducing privacy-related complaints and aligning Uber more closely considering privacy laws like GDPR and CCPA (mosaic, n.d.; Uber, n.d.).
- **Future Steps**: Uber continues to evaluate and update its privacy practices in response to evolving data protection standards and user feedback. They also plan regular privacy training for employees to ensure ongoing compliance and awareness (mosaic, n.d.; Uber, n.d.; Wu, 2018).

Relationship between Data Privacy and Data Security:

Data privacy means a person's right to control their own information. This includes how this information is collected, used, and shared, making sure people's rights are looked after and their information is used in the right way. Data security comes into play because we need to keep this personal information safe to respect privacy. So, if we do not have good security, we cannot keep information private (Carmichael, 2023; Pınarbaşı, 2022).

Data security is about protecting personal details from being stolen or seen by people who should not have access to them. This means using tools like encryption and making sure only the right people can get to the data. While data security is about all kinds of data, not just personal info, it is important to keep personal information private (Carmichael, 2023; Pınarbaşı, 2022).

Distinction between Data Privacy and Data Security:

The main differences lies in their focus and scope. Data privacy is all about how personal information is handled in a way that's fair and legal. It is about making sure people agree to how their information is used and keeping them in the loop. On the other hand, data security is more about the technical side, like using tools and methods to keep all data types safe from hackers and accidents. While data privacy focuses on personal rights, data security is about protecting all data to keep that privacy intact (Carmichael, 2023; Pınarbaşı, 2022).

So, even though data privacy and data security are closely connected with security actions supporting the goal of privacy, they focus on different things. Having strong security is critical to keeping information private. However, following privacy rules is more than just having tight security; it is also about following ethical guidelines and laws (Carmichael, 2023; Pınarbaşı, 2022).

Key Roles in Analytics and Technology Impacting Data Privacy and Security

In the domain of analytics and technology, several roles significantly contribute to the areas of data privacy and data security:

- **Data Privacy Analysts**: These experts help set up systems that keep a company's data safe and private. They make sure all the rules about keeping information private are followed from when data is first collected until it is no longer needed. They work to prevent any leaks of private information (King, n.d.).
- **Chief Information Officers (CIOs)**: CIOs consider the big picture of keeping data safe and private. They develop strategies to handle these challenges and ensure these strategies are used in every part of the company. They help link data safety and privacy together (diVittorio, 2023).
- **Cybersecurity Professionals**: As laws about keeping data private keep changing, these tech experts need to know a lot about privacy rules. They make sure that when they protect the company from cyber threats, they also keep user data private as the law requires (Simplilearn, 2023).
- **Data Engineers and Data Analysts**: These techies manage and look at data while ensuring they follow privacy rules. Data Engineers build systems that keep data safe and organized, while Data Analysts use data carefully to respect privacy rules, often using specific computer languages and tools (Lin, 2023; Simplilearn, 2024).
- **Machine Learning Scientists and Data Scientists**: These folks use advanced computing to analyze data but must be careful not to break privacy rules. They must ensure their computer models and analyses do not misuse private information or accidentally share it (MagniMind, n.d.; SailPoint, 2023).

Each of these roles contributes differently but significantly to maintaining and enhancing data privacy and security within organizations. As data privacy and security become more connected, it's essential for experts in these areas to work

together and keep up with both fields. This collaboration helps ensure that both the company's and the customers' information stays safe (King, n.d.; diVittorio, 2023; Simplilearn, 2023; Lin, 2023; Simplilearn, 2024; MagniMind, n.d.; SailPoint, 2023).

In conclusion, the job roles within the analytics and tech sectors, especially when it comes to data privacy and security, are crucial and cover a wide range. From those who analyze data privacy issues to those in charge of information technology and from experts safeguarding against cyber threats to those crunching data numbers, every position has unique duties and chances to influence how we safeguard data. Working together, these professionals help build a strong, safe, and honest way of handling data that meets legal requirements and builds user trust. As our world becomes more digitized and data-driven, the need for these experts will increase, emphasizing the importance of continuous learning, flexibility, and teamwork to tackle ongoing data privacy and security challenges.

References:

Buckbee, M. (2023, June 2). *Data Privacy Guide: Definitions, Explanations and Legislation*. Varonis. https://www.varonis.com/blog/data-privacy

Correll, M. (2019, May 2). *Ethical Dimensions of Visualization Research*. ACM Digital Library. https://dl.acm.org/doi/10.1145/3290605.3300418

Cote, C. (2021, March 16). *5 PRINCIPLES OF DATA ETHICS FOR BUSINESS*. Harvard Business School Online. https://online.hbs.edu/blog/post/data-ethics

Carmichael, M. (2023, February 28). *The Difference Between Data Privacy and Data Security*. Isaca. https://www.isaca.org/resources/news-and-trends/industry-news/2023/the-difference-between-data-privacy-and-data-security

DiVittorio, A. (2023, April 27). *Why CISOs Should Be Thinking About Data Privacy*. Datagrail. https://www.datagrail.io/blog/privacy-trends/why-cisos-should-be-thinking-about-data-privacy/

Edquist, A., Grennan, L., Griffiths, S., & Rowshankish, K. (2022, September 23). *Data ethics: What it means and what it takes*. Mckinsey. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes

Insider Lab (2022, December 9). *Insights from the Uber Breach: Ways to Prevent Similar Attacks*. Insidersecurity. https://insidersecurity.co/insights-from-the-uber-breach-ways-to-prevent-similar-attacks/

King, T. (n.d.). *A Data Privacy Analyst Job Description by Solutions Review*. Solutionsreview. https://solutionsreview.com/backup-disaster-recovery/data-privacy-analyst-job-description/

Knight, M. (2023, June 20). *What Is Data Governance? Definition, Types, Uses*. Dataversity. https://www.dataversity.net/what-is-data-governance/

MagniMind (n.d.). *The Role Of Data Science In Cybersecurity And In Protection Against Online Threats*. https://magnimindacademy.com/blog/the-role-of-data-science-in-cybersecurity-and-in-protection-against-online-threats/

mosaic (n.d.). *Why TrustArc Software?* https://mosaic.ee/trustarc/

Lavanchy, M. (2018, November 1). *Amazon's sexist hiring algorithm could still be better than a human*. Theconversation. https://theconversation.com/amazons-sexist-hiring-algorithm-could-still-be-better-than-a-human-105270

Lin, P. (2023, July 3). *Understanding the Crucial Role of Data Engineers in Data Security*. Linkedin. https://www.linkedin.com/pulse/understanding-crucial-role-data-engineers-security-polyd

Pınarbaşı, A. T. (2022, June 30). *Data Privacy vs. Data Security vs. Data Protection: In-Depth Look*. Termly. https://termly.io/resources/articles/data-privacy-vs-data-security-vs-data-protection/

SailPoint (2023, September 8). *Machine learning (ML) in cybersecurity*. https://www.sailpoint.com/identity-library/how-ai-and-machine-learning-are-improving-cybersecurity/

Simplilearn (2023, August 1). *Roles and Responsibilities of Cyber Security Professionals*. https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article#:~:text=evolving%20threat%20landscape.-,Roles%20of%20the%20Cyber%20Security%20Professional,monitoring%20and%20reacting%20to%20attacks.

Simplilearn (2024, January 29). *Data Analyst Job Description: Responsibilities, Skills Required*. https://www.simplilearn.com/data-analyst-job-description-article

Tata, S., & Mitsunari, A. (2020, November 17). *How Uber Manages Real-Time Risk Assessment*. Auditboard. https://www.auditboard.com/blog/how-uber-manages-real-time-risk-assessment/

Uber (n.d.). *Privacy Center*. https://privacy.uber.com/center

Uber (2022, March 10). *One Stone, Three Birds: Finer-Grained Encryption @ Apache Parquet™*. https://www.uber.com/en-IN/blog/one-stone-three-birds-finer-grained-encryption-apache-parquet/

Uber Team (2022, September 16). *Security update*. Uber. https://www.uber.com/newsroom/security-update/

Uber (2023, July 13). *Attribute-Based Access Control at Uber*. https://www.uber.com/en-IN/blog/attribute-based-access-control-at-uber/

Vidgen, R., Hindle, G., & Randolph, I. (2020). *Exploring the ethical implications of business analytics with a business ethics canvas.* European Journal of Operational Research, 281(3), 491–501. https://doi.org/10.1016/j.ejor.2019.04.036

Wu, S. (2018, September 27). *Uber and the Ongoing Battle Over Consumer Data Privacy*. Bloom.

https://bloom.co/blog/uber-and-the-ongoing-battle-over-consumer-data-privacy/