Position Paper 2 Outline

Prompt: Regardless of industry, business organizations struggle trying to balance two seemingly opposing data-related considerations: data security vs. data usage. Quite commonly, organizational infrastructure managers (such as chief technology officers, etc.) charged with data security strive to limit access to data as a way of mitigating the possibility of data breaches, theft and related problems. Functional managers (such as chief marketing officers, etc.) tend to favor broader and easier access to organizational data, as a way of encouraging more fact-based planning and decision making. Is it possible for organizations to simultaneously accomplish both objectives, namely, making their data as secure as possible while also maximizing the usage and the utility of their data? Take a position, clearly describe and substantiate your reasoning; be specific.

Intro:

Background on Data Security/Privacy vs Usage/Accessibility – significance of this dilemma in modern organizations

Mention rapid growth of data in the digital age

Mention the increasing reliance on data in business operations

Highlight tension between data security and data usage

Importance of each

Safeguarding sensitive data, but needs to be accessible for use in decision making

Briefly mention the consequences of data breaches and misuse.

Which position I support = yes, but it will never be perfect

State that the essay will explore if it’s possible to balance data security and usage – The feasibility of balancing data security and data usage depends on a multitude of factors including industry, organizational culture, and risk tolerance.

P1: Data Security – the case for limiting access

Protecting privacy and sensitive information = critical

Robust data security measures protect individual privacy by ensuring that personal information remains confidential and is not misused or exposed without consent.

Data breaches and their consequences – include ethics

Regulatory compliance (HIPAA, etc)

Trust, reputation, and consumer confidence – individuals are more likely to engage with organizations and share data when they trust that their information will be secure (Morey et al., 2015).

Strategies for enhancing data security – restricted access controls (RBAC), encryption, data masking, regular security audits

As information is removed from datasets to protect privacy, the utility of the data is reduced (Mivule and Turner, 2013)

Example: Implantable medical devices equipped with wireless interfaces for easy access for timely medical interventions. However, can’t use typical security measures such as passwords and certificates due to frequent emergencies in medical settings

Makes IMDs susceptible to eavesdropping and unauthorized access and control

Researchers have demonstrated that it is possible to attack remotely - using cardiac defibrillators and insulin pumps (3,4)

Allowed them to modify the therapies being provided by the medical devices - shows capability to severly harm patients privacy and health. (Masoud et al., 2013).

P2: Data Usage – the case for broader access

The power of data in decision making – market insights, customer understanding, data-driven decision making

Data insights can provide a competitive advantage

Maybe add in some stats on how data driven decision making benefits businesses??

Data driven industries contribute significantly to economic growth – One study found that companies that use data-driven decision making have 5-6% higher productivity and output growth than other companies that don’t value a data-driven approach (Brynjolfsson, et al., 2011).

Fosters innovation and research

Examples: public health and safety – ie covid, tracking disease outbreaks for an efficient response

Paper to reference – Wacksman, 2021. Example of balancing access and privacy - contact tracing in the era of COVID-19.

P3: Balancing the two aspects

Risks of over-restriction – hindering innovation and growth, cause frustration

Risks of over-permissiveness – vulnerability to data breaches, legal and compliance challenges

Finding middle ground – establishing clear data usage policies (case for data governance frameworks!!), determining company values, collaborative decision making (organizational infrastructure managers and functional managers to devise strategies that optimize both security and usage), continuous monitoring and adjustment – striking a balance!!

Different industries may have unique data security and usage requirements (ie healthcare vs marketing - example)

Risk tolerance – organizations with high risk tolerance may lean towards maximizing data usage, while risk-averse organizations prioritize security

Approaches such as differential privacy can be used as a tool for organizations to balance data privacy and utility, particularly in situations where they need to share aggregate or statistical information while preserving the privacy of individual data contributors (cite DP paper!!)

Differential privacy provides a mathematical framework and techniques to add noise or perturbation to data in a controlled manner, making it difficult to reverse-engineer the individual data points while still allowing for meaningful analysis = privacy preserving analytics.

Even with the latest data privacy algorithms such as differential privacy, there is a major loss of data utility that comes with the increase in confidentiality (Mivule and Turner, 2013).

Conclusion:

Summarize main arguments, emphasize that achieving both objectives is possible

Recommendations – building a culture of data responsibility (and values data as a strategic asset), leveraging technology for security and usage (ie AI and ML, advanced security solutions), need for continuous adaptation and improvement

ML example:

Uses ML algorithms to check the balance between data anonymity and data utility to optimize the balance using the k-anonymity method (Esmeel et al., 2020).

AI evidence: Organizations that utilize security AI and automation in security measures save an average of $1.76 million compared to companies who don’t (IBM, 2023).

Closing remarks on the significance of the topic

Balancing data security and data usage is not a one size fits all approach

Organizations must assess their unique circumstances, industry, and risk tolerance to find the right balance

Evolving nature of data management in the digital age – should be agile in adapting to both evolving threats and opportunities to ensure that a balance is maintained.