DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105
ISSN - 1983-716X

DATA SECURITY AND ITS IMPACT ON VALUE CREATION: ANALYZING CONSUMER PERCEPTIONS IN THE UNITED STATES

SEGURANÇA DE DADOS E SEU IMPACTO NA CRIAÇÃO DE VALOR: ANALISANDO AS PERCEPÇÕES DO CONSUMIDOR NOS ESTADOS UNIDOS

LA SEGURIDAD DE LOS DATOS Y SU IMPACTO EN LA CREACIÓN DE VALOR: ANÁLISIS DE LAS PERCEPCIONES DE LOS CONSUMIDORES EN ESTADOS UNIDOS

ABSTRACT

Purpose: Data security has become an essential concern for businesses as it directly influences the trust between consumers and businesses. Data breaches and cyberattacks are becoming more frequent, highlighting the need for strong security measures as the consequences of a data breach can be devastating, leading to financial losses, reputational damage and stakeholder distrust. In this sense, our purpose is to analyze data security practices that create value for consumers.

Design/methodology/approach: To explore big data practices, an exploratory descriptive approach was applied. Initially, we use the JUST Capital 2020 database with 922 companies divided into six industries and identified those most recognized by which ones consumers for their perceive data security actions. In a second step, we analyzed annual reports to understand which actions related to the topic the companies adopt.

Findings: We analyzed data from 922 U.S.-listed companies and found that the information technology sector had the highest scores in data security, whereas the manufacturing sector ranked the lowest. Nearly 48% of firms had weak security measures, highlighting widespread vulnerabilities. We found a pattern of companies' best practices that create more value to consumers regarding data security, such as following regulatory policies, having risk management programs, promoting internal and external audits and inspections, and allocating staff focused on data security.

Originality: The originality of our study lies in the analysis of consumer value perception related to data security variables while validating the use of a new and promising database in stakeholder management research. In addition, our findings emphasize the growing need for stronger data protection, especially in industries where it is not yet a priority.

Ana Helena Freitas Kuznetzow
Postgraduate
Universidade de São Paulo – Brazil
anahfkw@gmail.com

Helna Almeida de Araujo Goes
PhD student
Universidade de São Paulo - Brazil
helna@usp.br

Mariana Uchoa
PhD student
Universidade de São Paulo – Brazil
marianauchoa@outlook.com

João Mauricio Gama Boaventura
PhD
Universidade de São Paulo - Brazil
jboaventura@usp.br

Submitted on: 09/22/2024
Approved on: 05/28/2025

How to cite: Kuznetzow, A. H. F., Goes, H. A. de A., Uchoa, M., & Boaventura, J. M. G. (2025). Data Security And Its Impact On Value Creation: Analyzing Consumer Perceptions In The United States. *Alcance (online)*, 32(1), 86-105. https://doi.org/10.14210/alcance.v32n1(Jan/Abr).p86-105

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

Research limitations/implications: Our study contributes to the stakeholder management literature on value creation by investigating the consumer value perception regarding data security, exposing both the degree of importance that consumers attach to this issue and the consequences affecting the behavior of companies.

Practical implications: We identified the best data security practices adopted by companies and analyzed patterns influencing managerial decisions, such as concerns over financial sanctions and potential damage to brand reputation in the event of a data breach. In sum, our findings suggest that to meet consumer demands and create value, companies should implement a security strategy with strong authentication, encryption, and risk management.

Keywords: Data security. Stakeholder management. Value Creation. Big data. JUST Capital.

RESUMO

Objetivo: A segurança de dados se tornou uma preocupação essencial para as empresas, pois influencia diretamente a confiança entre consumidores e empresas. Violações de dados e ataques cibernéticos estão se tornando mais frequentes, destacando a necessidade de fortes medidas de segurança, pois as consequências de uma violação de dados podem ser devastadoras, levando a perdas financeiras, danos à reputação e desconfiança das partes interessadas. Nesse sentido, nosso propósito é analisar práticas de segurança de dados que criam valor para os consumidores.

Design/metodologia/abordagem: Para explorar as práticas de segurança da informação, foi aplicada uma abordagem descritiva exploratória. Inicialmente, exploramos o banco de dados JUST Capital 2020 com 922 empresas divididas em seis setores e identificamos aquelas mais reconhecidas pelos consumidores por suas ações de segurança de dados. Em um segundo momento, analisamos relatórios anuais para entender quais ações relacionadas ao tema as empresas adotam.

Principais resultados: Analisamos dados de 922 empresas listadas nos EUA e descobrimos que o setor de tecnologia da informação teve as maiores pontuações em segurança de dados, enquanto o setor de manufatura teve a menor classificação. Quase 48% das empresas tinham medidas de segurança fracas, destacando vulnerabilidades generalizadas. Encontramos um padrão de melhores práticas das empresas que promovem mais valor aos consumidores em relação à segurança de dados, como seguir políticas regulatórias, ter programas de gerenciamento de risco, promover auditorias e inspeções internas e externas e alocar pessoal focado na segurança de dados.

Originalidade: A originalidade do nosso estudo está na análise da percepção de valor do consumidor relacionada às variáveis de segurança de dados ao validar o uso de um novo e promissor banco de dados na pesquisa de gerenciamento de stakeholders. Além disso, nossas descobertas destacam a crescente necessidade de maior proteção de dados, especialmente em setores onde isso ainda não é uma prioridade.

Limitações/implicações da pesquisa: Nosso estudo contribui para a literatura de gerenciamento de stakeholders sobre criação de valor ao investigar a percepção de valor do consumidor em relação à segurança de dados, expondo tanto o grau de importância que os consumidores atribuem a essa questão quanto às consequências que afetam o comportamento das empresas.

Implicações práticas: Identificamos as melhores práticas de segurança de dados adotadas por empresas e analisamos padrões que influenciam decisões gerenciais, como preocupações com sanções financeiras e danos potenciais à reputação da marca no caso de uma violação de dados. Em suma, nossas descobertas sugerem que, para atender às demandas do consumidor e criar valor, as empresas devem implementar uma estratégia de segurança com autenticação forte, criptografia e gerenciamento de risco.

Palavras-chave: Segurança de dados. Gestão de stakeholders. Criação de valor. Big data. JUST Capital.

RESUMEN

Propósito: La seguridad de los datos se ha convertido en una preocupación esencial para las empresas, ya que influye directamente en la

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

confianza entre consumidores y empresas. Las violaciones de datos y los ataques cibernéticos son cada vez más frecuentes, lo que pone de relieve la necesidad de medidas de seguridad sólidas, ya que las consecuencias de una violación de datos pueden ser devastadoras y provocar pérdidas financieras, daños a la reputación y desconfianza de las partes interesadas. En este sentido, nuestro propósito es analizar prácticas de seguridad de datos que creen valor para los consumidores.

Diseño/metodología/enfoque: Para explorar las prácticas de seguridad de la información, se aplicó un enfoque descriptivo exploratorio. Inicialmente, exploramos la base de datos de JUST Capital 2020 con 922 empresas divididas en seis sectores e identificamos aquellas más reconocidas por los consumidores por sus acciones de seguridad de datos. En segundo lugar, analizamos los informes anuales para entender qué acciones relacionadas con el tema adoptan las empresas.

Hallazgos: Analizamos datos de 922 empresas que cotizan en bolsa en Estados Unidos y descubrimos que el sector de tecnología de la información obtuvo las puntuaciones más altas en seguridad de datos, mientras que el sector manufacturero obtuvo las puntuaciones más bajas. Casi el 48% de las empresas tenían medidas de seguridad débiles, lo que pone de relieve vulnerabilidades generalizadas. Encontramos un patrón de mejores prácticas de las empresas que promueven más valor para los consumidores con respecto a la seguridad de los datos, como seguir políticas regulatorias, tener programas de gestión de riesgos, promover auditorías e inspecciones internas y externas y asignar personal enfocado en la seguridad de los datos.

Originalidad: La originalidad de nuestro estudio radica en el análisis de la percepción de valor del consumidor relacionada con las variables de seguridad de datos al tiempo que valida el uso de una base de datos nueva y prometedora en la investigación de gestión de las partes interesadas. Además, nuestros hallazgos enfatizan la creciente necesidad de una mayor protección de datos, especialmente en industrias donde todavía no es una prioridad.

Limitaciones/implicaciones de la investigación: Nuestro estudio contribuye a la literatura de gestión de las partes interesadas sobre la creación de valor al investigar la percepción de valor del consumidor con respecto a la seguridad de los datos, exponiendo tanto el grado de importancia que los consumidores le otorgan a este tema como las consecuencias que afectan el comportamiento de las empresas.

Implicaciones prácticas: La principal se refiere a verificar las mejores prácticas adoptadas por las empresas en materia de seguridad de datos y no duda en colocar este aspecto como uno de los pilares de su gestión. Este estudio también fue importante para comprender patrones que llevan a decisiones gerenciales, como el miedo de las empresas a sufrir sanciones financieras y perder la reputación de su marca en casos de fuga de datos. Identificamos las mejores prácticas de seguridad de datos adoptadas por las empresas y analizamos los patrones que influyen en las decisiones de gestión, como las preocupaciones sobre sanciones financieras y el posible daño a la reputación de la marca en caso de una filtración de datos. En resumen, nuestros hallazgos sugieren que, para satisfacer las demandas de los consumidores y crear valor, las empresas deben implementar una estrategia de seguridad con autenticación sólida, cifrado y gestión de riesgos.

Palabras clave: Seguridad de datos. Gestión de grupos de interés. Creación de valor. Big data. JUST Capital.

INTRODUCTION

Value creation is the fundamental premise of a business's purpose. This principle is a key argument of stakeholder theory, shaping business strategy in both academic research and managerial applications (Freeman, 1984; Barney & Harrison, 2020; Bridoux & Stoelhorst, 2016). Stakeholder theory derives from the premise that capitalism works better when actors (stakeholders) are engaged in (joint) value creation (Bridoux & Stoelhorst, 2022). We understand value as the combination of tangible and intangible assets that a company provides to its stakeholders, fulfilling their needs and sustaining the relationship between the company and its stakeholders (Soares et al., 2014; Boaventura et al., 2020).

In parallel, data security has become a critical concern for businesses as it directly influen-

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

ces the trust between consumers and businesses. Data breaches and cyberattacks are becoming more frequent, highlighting the need for strong security measures as the consequences of a data breach can be devastating, leading to financial losses, reputational damage and stakeholder distrust (Liu & Barbar, 2024; Shankar, & Mohammed, 2020). For instance, we can examine the 2014 Target data breach, one of the largest in U.S. retail history, where over 40 million customers' personally identifiable information (PII) and credit card details were compromised. Similarly, the Yahoo breach in 2013 resulted in two major data breaches, affecting over a billion user accounts (Shankar & Mohammed, 2020). This issue is not exclusive to the United States, highlighting the global challenge of data security and the urgent need for stronger protective measures across industries and regions (Liu & Barbar, 2024).

Although the literature on data privacy has expanded in recent years (Martin et al., 2017; Farhad, 2024), few management studies examine how corporate data security practices impact consumer-perceived value creation. Most existing studies focus on debates about the relevance of ethical issues in big data analytics and how consumers perceive their data security as a tangible value. According to Someh et al. (2019), the non-reciprocal character of the interaction between organizations, individuals, and society highlights ethical concerns or dilemmas for different stakeholders in a context that have the asymmetrical power from collecting to the sale of the individuals' data without their consent or awareness (Barocas & Nissenbaum, 2014; Solove, 2013).

Although data security has been widely studied from a technical and regulatory perspective, there is still a significant gap in understanding how consumers perceive these practices and their impact on stakeholder management and value creation. Stakeholder theory (Freeman et al., 2010) suggests that companies should consider consumer expectations, yet few studies address data security as a strategic factor in this context. Furthermore, research by Acquisti, Brandimarte, and Loewenstein (2015) indicates that information asymmetry regarding privacy can affect how consumers evaluate these practices. Thus, exploring the relationship between data security, consumer perception, and competitive advantage contributes to significant advances in stakeholder theory.

Furthermore, robust databases, such as Just Capital 2020, have not yet been widely validated in the stakeholder management literature, reinforcing the need for studies that advance the measurement of these practices. This is possible because Just Capital considers the perspective of consumers and other stakeholders when measuring business practices that influence the trust and reputation of organizations, with data security being one of the pillars analyzed (Just Capital, 2020). By using this database, the study is anchored in a data set recognized in the market, using the most prominent and leading companies on the US Stock Exchange, many of which are leaders in their sectors, contributing to the validity of the findings and strengthening their applicability, both academically and practically. This way, we provide an updated and comparable cross-section between different companies and sectors, allowing a descriptive analysis of the relationship between information security and value creation.

We founded two existing studies in the literature using Just Capital; the first one analyzed the value potential of companies considered "fair" that adopt responsible and ethical business practices and how they can positively influence the financial performance and trust of companies (Ahmad, 2020), the second one sought to understand the differences in value perceptions for different groups of stakeholders, considering the value created and distributed by public companies in the United States (Santos et al., 2024).

In this sense, our purpose is to analyze data security practices that create value for consumers by answering the research question: What are the best practices of data security that create value for consumers? To this end, we use the JUST Capital 2020 database as a source to analyze American companies' behaviors regarding data security, i.e., we use it to analyze what practices related to data security are perceived as the best to create value for consumers, generating evidence of the relevance of this topic amidst a context in which data sharing is becoming increasingly frequent.

We analyzed data from 922 U.S.-listed companies, and we found evidence that the Infor-

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

mation Technology sector presented the highest score on data security whilst the Manufacturing sector presented the lowest score. While tech and finance firms prioritize security due to its business relevance, Commerce and Services present opportunities for improvement, especially post-COVID-19. In addition, alarmingly, 48% of firms underscored, highlighting widespread weaknesses regarding data security.

Lastly, we identified top-performing companies in each industry and their data security practices, emphasizing the growing need for stronger data protection across industries. In other words, these findings highlight the growing importance of data security across industries and the need for improvements, particularly in sectors where it is not yet a core business priority. Thus, we contribute to the literature by identifying which data security practices are perceived as valuable by consumers, expanding the understanding of the relationship between data security and value creation in the context of stakeholder management.

This article is structured as follows. First, we present the theoretical background, outlining key concepts related to stakeholder theory and value creation. Next, we highlight the context of data security. Following, the research methodology is detailed, including data collection and analysis procedures. The subsequent section discusses the findings, highlighting their implications for both academic and managerial practice. Finally, the conclusion summarizes the main insights and contributions, acknowledges limitations, and suggests directions for future research.

STAKEHOLDER MANAGEMENT

"Stakeholder theory is a tool to better describe the world and foster better action" (Parmar et al., 2010, p. 409). In agreement with these lines, it came to address three interconnected problems relating to business:(1) the problem of value creation and trade, (2) the problem of ethics of capitalism, and (3) the problem of managerial mindset. Stakeholder theory suggests the unity of analysis between a business and the groups and individuals who can affect or be affected by the organization (Freeman, 1984). In this research, we focus on customers, a primary stakeholder group — "groups and individuals who have a stake in the success or failure of a business" (Valentinov & Chia, 2022, p.762).

Previous literature has discussed how managerial actions have the potential to affect a broad range of people all over the world (Clement, 2005) and how managers must be concerned about the responsibilities of the firm, as it affects not only the firm but also its stakeholders (Parmar et al., 2010). Freeman (1984) also draws attention to the fact that companies must align social and ethical issues with the company's business model and that any change in the management direction should consider the impact that will be caused on stakeholders (Freeman, 1984).

For that matter, stakeholder management requires long term commitment by firms. According to Tantalo (2014), it can be divided into four steps: first, it is essential to identify the relevant stakeholder groups; second, it is necessary to ponder the relevance of each stakeholder, then understand how the expectations of each group are being met and finally, modify corporate policies if necessary, considering the stakeholders' priorities (Freeman, 1984). In this way, the company can more deeply understand the needs and get closer to the variables that make up the value creation of its main stakeholders (Harrison et al., 2010).

Therefore, the stakeholders' perception of value must be examined carefully. To bring benefits to the company and society (in)directly, it must follow a process in which the stakeholder is placed at the center of management decisions. Next, we address the topic of value creation in this context and how it relates to the variables that we analyze in this paper.

Value Creation

Freeman (2010) argues that "The primary responsibility of the executive is to create as much value as possible for stakeholders" (Freeman, 2011, p. 2). The importance of value creation generated by companies for their stakeholders is not limited to Freeman's research; it has repercussions in several research in the stakeholder literature. For example, Verbeke, Osiyevskyy, and

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

Backman (2017, p. 685) argue that value creation is a fundamental prerequisite for the very survival of any company.

This statement requires a profound understanding of the definition of value creation. However, there are several articles in the literature with different definitions of value — see Table 1.

We use the definition of value creation with a focus on the customer's perspective, focusing on values such as safety, respect, business reputation, accessibility and considering that customers represent, within the universe of primary stakeholders, those who have greater strategic importance, greater value and power over the company (Boaventura et al., 2020). Therefore, as much as the other definitions complement the understanding of value creation, the most relevant definition for this study is the one from Boaventura et al. (2020). In their research, different terms related to all the primary stakeholders' perceptions of value performed by companies were compiled and categorized into tangible and intangible values.

Table 1

Different Value Definitions

Type of value	Definition
Value in Exchange	The idea that value is based on how much a given item is within a marketplace exchange. Value is negotiated and inter-subjective.
Intrinsic vs. Extrinsic Value	One way to think about value is whether it is intrinsic, or an inherent feature, of an item or whether it is simply a vehicle or means to some other good (i.e., extrinsic). Most goods in the marketplace are extrinsic. However, some things are good in and of themselves. Kant calls a good will an inherent good; virtues also would qualify as inherent goods
Subjective vs. Objective Value	Subjective typically refers to the assessment of an individual and what they like, while objective typically refers to a norm that operates across individuals or at a higher level of analysis (e.g., a universal moral norm; a social value; a human right).
Customer Value – Tangible vs. Intangible	- Products with Quality and Functionality, Product's Price, Perceived Quality, Service, Safety, Value for Money, Accessibility - time required to purchase the product and time required to master using the new product (Harrison and Wicks, 2013; Tantalo and Priem, 2016: 322; Clarke, 1998). - Business Reputation, Respect, Environmental Corporate Responsibility and "Eco Friendly" Product (Harrison and Wicks, 2013; Tantalo and Priem, 2016: 322; Clarke, 1998).

Source: Adapted from Boaventura et al. (2009; 2020) and Harrison & Wicks (2013).

Applying this value categorization, it is possible to understand how the data security metrics relate to consumers' perception of value. Thus, this study contributes both to future research and to greater assertiveness in the stakeholder management of companies since, according to Priem (2007), when a value has been created, the consumer (1) will be willing to pay for a novel benefit, (2) will be willing to pay more for something perceived to be better, or (3) will choose to receive a previously available benefit at a lower unit cost, which often results in a greater volume purchased. Therefore, from the consumers' perspective, value creation involves increasing use-value or decreasing exchange value (Priem, 2007).

To balance the creation of value aimed at consumers, one of the possible practices concerns ethics in data management, based, for example, on regulatory compliance, resulting in a balance in value creation. Due to the exponential advance in the maturity of technologies and innovations, many benefits are achieved, such as improving operational efficiency and optimizing processes; however, many risks arise, such as cybersecurity, data privacy, and regulatory compliance (Campos & dos Reis Carneiro, 2024). Regulatory compliance avoids legal penalties and reinforces stakeholders' trust in the organization (Soares de Souza & Tomei, 2024).

The interaction between data security and ethical information management offers a comprehensive perspective for stakeholder management (Freeman et al., 2010). By protecting data and respecting the privacy of individuals, companies strengthen the trust and loyalty of customers, partners, and other stakeholders, creating a virtuous cycle of shared value. In the next section, we will discuss data security in detail.

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

Big Data and Data Security

The term "Big Data" was first introduced in 2005 by Roger Magoulas to define a significant amount of data that traditional data management techniques could not process due to its complexity and size (Chaorasiya & Shrivastava, 2014). For MIKE 2.0, a methodology that provides a framework for information management, Big Data is defined by its size, comprising a large, complex, and independent collection of data sets with the potential to interact.

Given the complexity of big data, both in literature and in practice, the study of algorithms has intensified in search of a faster and more assertive use of data (Madsen, 2015). According to Gunther (2017), "algorithmic processing generally follows fixed, pre-programmed procedures" (Günther et al., 2017, p. 196), and it can provide patterns and insights that had not been considered before and can therefore change the course of management decisions.

Big data has its advantages, such as enhancing customer satisfaction by using information from call centers and getting a pattern, improving services and products by knowing the potential consumers and their preferences. This advantage is only possible because algorithms are increasingly capable of predicting human behavior. The impacts encompass both the individual consumer, who can have the service and products adjusted according to their preferences and also the organization that, knowing the preferences of its consumers, can focus its efforts more assertively and efficiently, being able to create and distribute value to its consumers more accurately (Boaventura et al., 2020; Günther et al., 2017).

On the other hand, there are debates in the literature about data management, especially regarding consumers' data, which generates, in fact, only positive externalities for society and individuals. For example, Zwitter (2014) highlights cases of privacy breaches, extensive individual profiling, and discrimination against customers. In line with this idea, "ethical issues arise when organizations collect, analyze, share, and/or sell individuals' data without individuals' genuine consent or awareness" (Someh et al., 2019, p. 720). In these cases, the proportion of the damage affects consumers and institutions unequally, being the consumers the most affected since they are the owners of the data.

The internet and digital technologies have played a key role in business decisions, turning the ability to manage data into a core capability. Gunther (2017) draws attention to two cases, Netflix, which offers media streaming and builds a dynamic of recommendations based on consumers' patterns, and The New York Times, which uses data to engage readers in its digital environment. According to his research, those two cases are examples of the movement of monetization of personal data, which has consequences for the company, for being inside its business model while transforming the customer experience.

The implications of these dynamics go beyond economic gains, but they can directly impact consumers' data autonomy and privacy (Orbik & Zozul'aková, 2019). According to BBC, this impact was felt by nearly 339 million customers, who had their personal data, such as name, phone, email, passport, and even credit cards, exposed to a group of hackers who invaded Marriott International. This company, which has international operations, had the breach was identified in 2018 and, as a result, the company was fined €18.4 million for the violation by the UK's privacy control and has become one of the most emblematic cases of data leakage. EasyJet also suffered from a cyber-attack that exposed the personal and payment information of nearly 9 million users in May 2020 (NSFOCUS, 2019).

In 2018, C&A, a Brazilian clothing retail company, also suffered from cyber-attacks conducted by hackers. Although names, credit cards, personal codes, and emails of 2 million consumers were exposed on this occasion, this case clarifies that the issue of cybersecurity is global and should be looked at carefully by all countries and companies that deal with data management.

Understanding the growing relevance of data in recent years, The Economist argues in its 2017 edition that the world's most valuable resource was no longer oil but data. ISO (The International Organization for Standardization) and IEC (International Electrotechnical Commission) saw this growing importance. Therefore, in 1995, a group of standards was created to govern the

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

guidelines related to the scope of information security, represented by the ISO 27000 series. This group includes ISO/IEC 27002, an international standard that establishes guidelines to support organizations' implementation and control of the Information Security Management System (SGSI) (ISO/IEC, 2013). This standard contains 14 security control clauses, including technical measures such as cryptography or communication security (ISO/IEC, 2013).

The standard established by ISO ensures that companies and their stakeholders are assured of safety and protected against harm, generating value for the business (ISO/IEC, 2013). To analyze the best practices, the 14 clauses were segmented into four main pillars of actions that companies should pay attention to: Establishment of Privacy Policies and documentation, Monitoring of suppliers, Data Management, and Operation Security — see Table II.

Table 2
Four Pillars of Data Security

Four pillars of Data security	14 Control Clauses of ISO 27002	Definition of the Clauses
Establishment of Privacy Policies and documentation	Information Security Policies	Information security should be directed from the top of the organization, and policies should be communicated clearly to all employees.
	Organization of Information Security	A management framework should support the organization's information security operations, both on- and off-site.
	Information security aspects of business continuity management	Information security continuity should be embedded in the organization's business continuity management practices.
	Compliance	Information should be protected to meet legal, statutory, regulatory, and contractual obligations and comply with the organization's policies and procedures.
Data Management	Human resource Security	Employees and contractors should be aware of their role in safeguarding the organization's information before and during employment. The organization's information should also be protected.
	Asset Management	Organizations should identify their physical and information assets and determine the appropriate level of security necessary for each.
	Information security incident management	Information security incidents should be handled consistently and effectively.
Operation Security	Access Control	Access to information and information processing facilities should be limited to prevent unauthorized user access. Users should be responsible for safeguarding their authentication information, such as passwords.
	Cryptography	Policies on cryptography and the use of cryptographic keys should be developed and implemented to protect the confidentiality, integrity, and/or availability of information.
	Physical and environmental security	Controls should be introduced to prevent unauthorized physical access, damage, and interference to information processing facilities.
	Operation Security	Procedures and responsibilities, Security from malware, Backup, Logging and monitoring, Control of operational software, Technical vulnerability management and Information systems audit coordination
	Communication security	Information should be protected in networks and as it is transferred, both within the organization and externally.
	System acquisition, development and maintenance	Information security should be designed and implemented throughout information systems' lifecycle. Test data should also be protected.
Monitoring of suppliers	Supplier relationships	Any of the organization's information assets that are accessible by suppliers should be appropriately protected.

Source: The authors (2025).

In addition to ISO 27002 certification, there is another vital driver when it comes to data security, The EU General Data Security Regulation (GDPR), which states that organizations must adopt specific policies, procedures, and processes to protect the personal data they own (Lopes et al., 2019).

Based on the concept of privacy as a fundamental human right, it has seven main privacy principles (fairness and lawfulness; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality; accountability) and is considered one of the forerunners of uniform legislation regarding data security breaches (Tankard, 2016). Having great relevance, GDPR has impacts worldwide and is considered by many companies, even if they are not European, as a guide in terms of data security, as will be shown later. In the USA, the primary data security law is the California Consumer Privacy Act, CCPA, which provides several user rights, such as the right to delete personal information and opt-out of sales. Therefore, it is considered the law reference for the USA.

From the points mentioned above, it is clear the importance of approaching the topic of data se-

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

curity and relating it to the value attributed to the consumer. In addition to being a current issue and one that has become more and more essential each year, it is an issue that inevitably affects the lives of all consumers. Because the capture and use of data have advantages and disadvantages, this paper seeks to understand the primary practices that allow companies to stand out in data security. Furthermore, considering the significant impact of data management, this study aims to elucidate which measures create the most value to consumers.

METHOD

Context and Data

The U.S. is one of the countries that most causes and suffers from cyberattacks in the world. According to a survey by SurfShark, a Dutch digital privacy and security company, in 2024, the USA ranked third with the highest number of breached accounts. Given this scenario and the economic and political importance of the country and the companies that are part of this context, we selected the JUST Capital database for this study. JUST Capital aims to research the American population's perception of companies and understand the most important attributes that they should have (JUST Capital). The result of this research is a ranking of the companies considered the fairest in the USA according to the public's priorities, based on how each stakeholder is affected by the company: Workers, Communities, Shareholders and Governance, Customers, and Environment.

For each stakeholder, JUST Capital provides the attributes that were measured. The community has four measurement attributes: shareholders and governance, 3 attributes; environment, 4 attributes; workers, 5 attributes; and customers, 4 attributes. The Customer stakeholder measures a company across four Issues: Customer Privacy, Customer Treatment, Transparent Communication, and Beneficial Products. Therefore, one of the attributes provided by the database is data privacy, which allowed us to use this database as an essential tool.

The 2020 JUST Capital ranking was used as our database, with research carried out in 2019 with 922 companies listed on the stock exchange. This year was chosen because in 2020, with the COVID-19 pandemic, many companies were affected and had to reconsider their priorities, and consumer perception may have been affected by this event, which is not the focus of the study.

Assignment of Variables

The Customers measure whether a company (1) protects the privacy of customers; (2) treats customers with respect and provides a positive customer experience; (3) makes products or offers services that do no harm to society; and (4) is transparent in communications about its products and services. In this paper, the focus is on the first one, an enabler to analyze the perceived value of the data privacy issue from the customers' point of view, considering some imperative variables that consumers appreciate, such as service rating, transparency, honesty, privacy, data oversight, quality, and product (JUST Capital, 2020).

Data Privacy (CUST.PRIV) is divided into two, which is the grouping of variables (1) Controversies in Customer Privacy as Reported in the Media (CUST.PRIV.CONT) and (2) Privacy Policies, Security, and User Information (CUST.PRIV.MGMT). In order to have a more assertive result, and without prejudice, only the variable Privacy Policies, Security, and User Information (CUST.PRIV.MGMT) was used in a context where all metrics mentioned in Appendix 1 were included in this variable.

To verify the reliability of the database and ensure that data security variables were measured, the first step of the research was to analyze and classify JUST Capital's variables according to the principles established by ISO 27002. Table 3 presents the initial comparison with JUST Capital's metric, the concept, and which ISO principle is met. Four principles stood out: confidentiality, integrity, authenticity, and availability. The first concerns the exclusivity of access to specific data, while the second advocates that the stored data remains complete and resistant to failures. Authenticity is about the authorship of a given piece of data, though it is possible to guarantee that a particular individual sent a piece of information. Lastly, availability guarantees that information is available to everyone who needs it.

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

Table 3
Metrics of Data Privacy from JUST Capital database

Metrics	Definitions
Customer Data Selling	It is an assessment of whether the company states that it does not sell users' data, this metric was selected considering confidentiality and integrity principles.
Tracking of User Activity	It is an assessment of whether the company explicitly states that it does not track users' behavior or complies with "do not track" requests. This metric was selected considering mainly the integrity principle.
User Control over Data Retention	It is an assessment of whether the company gives users full control over their own data. This metric was selected considering availability principles.
User Data Security Breaches	It is an assessment of whether the company clearly discloses its process for notifying users whose data might be affected by a data breach. This metric was selected considering integrity and confidentiality principles.
Data privacy controversies	It is the total number of cases occurring globally that pertain to privacy violations, as reported by influential and highly influential news sources over the past three years. This metric was selected as it exposes the importance of the data security issue. This metric was selected considering integrity and confidentiality principles.

Source: Adapted from JUST Capital database (2020).

Measurement of variables and Data Analysis

The scores provided by JUST Capital were used to measure consumers' perceptions of the importance of data privacy. According to the methodology provided by JUST Capital (2020), the variables are collected on a gross scale, then normalized and compared with the overall weighted average score of each company. The data analysis was then performed in two stages: first, using the JUST Capital database, an analysis was performed by sector to understand its influence on the variables used, with basic descriptive statistics such as mean, median, mode and standard deviation.

When performing this analysis, we intend to summarize and describe the data used, thus not requiring robustness or control tests. However, statistical precautions were taken, such as identifying and treating outliers and verifying asymmetric distributions using medians. The decision to analyze, classify, and group companies by sector is made because each industry deals with specific types of data, risks, and regulatory requirements, so challenges and vulnerabilities vary depending on the sector. Understanding how the sector works may not differentiate internal companies, but it provides relevant insights for organizations in the sector. Grouping companies into broad categories makes it easier to identify patterns and trends. However, this simplification may fail to capture important nuances between companies within the same sector, especially in relation to characteristics such as strategy, innovation, and performance. To address this issue, we performed a second qualitative analysis, described below.

Then, in the second stage, the companies with the highest scores were selected, and the public reports were analyzed to understand what actions these companies actually take. To this end, the five best-rated companies in each sector and their 2019 annual report were ranked and collected, considering the Investor Relations reports available on the companies' websites. The year 2019 was chosen so that when analyzing the reports from the same reference year from the JUST Capital database, the result obtained would be more reliable. The 2019 reports were analyzed with a focus on the data privacy sector and the companies' actions in relation to this issue. After observing the saturation of the data contained in these reports, it was found that the qualitative analysis of 3 main companies in each sector would be sufficient to reach a satisfactory result for the research since the actions were repeated in the other reports. After this stage, the research consolidates the results in a single table, which brings together all the companies analyzed and which actions they practice most, according to the grouping indicated by JUST Capital. The analyzed companies are presented in Appendix 2.

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

RESULTS

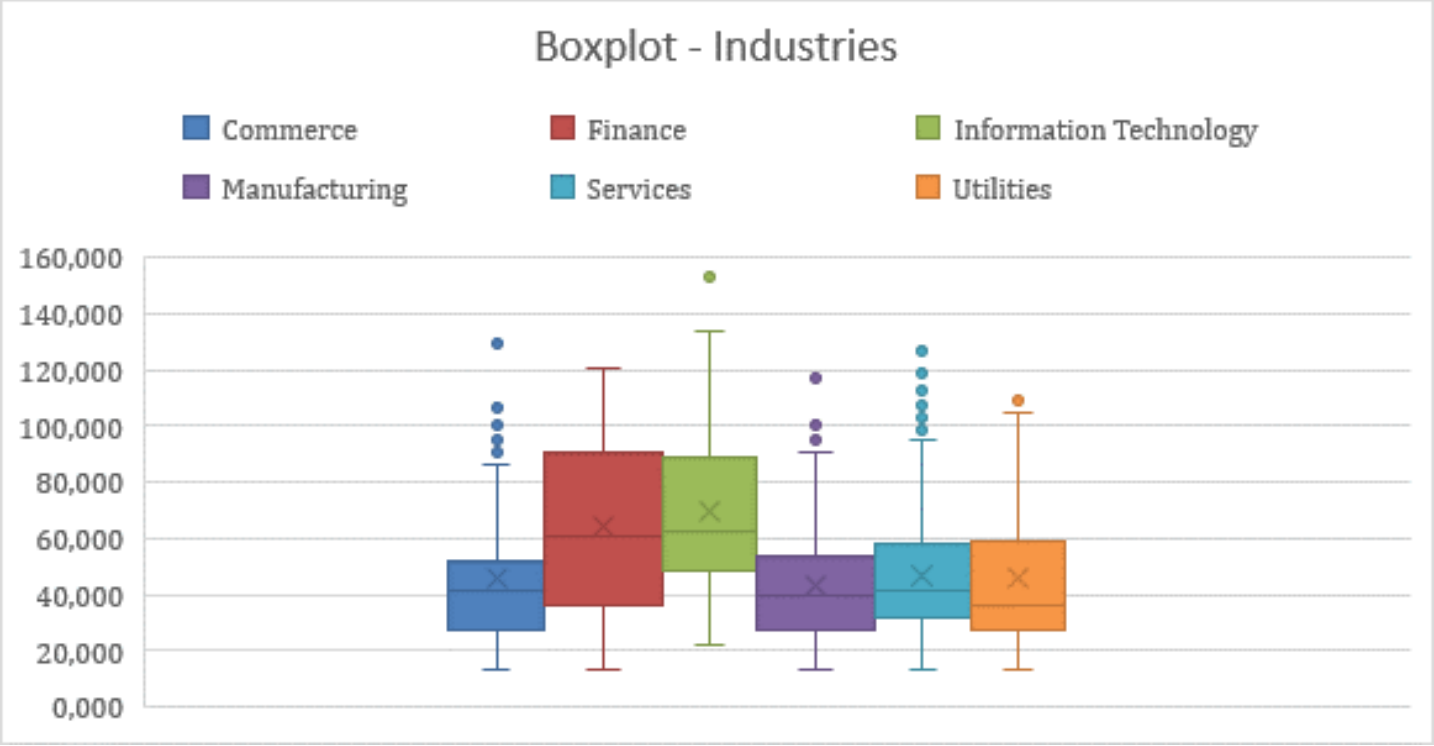
The following results were collected in 2019 and published in 2020 of 922 companies listed on the US stock exchange. First, to determine the value of the data security from a consumer perspective, we analyzed the scores for the CUST.PRIV.MGMT metric, collecting the average, mode, variance, and standard deviation of the companies grouped into the six industries. After that, the companies that had the best results were explored.

Considering the mean results of the CUST.PRIV.MGMT metric, the sector with the highest score is the Information Technology industry, with 68.71. This value is almost 7% higher than Finance, ranking second in the results, with a score of 63.71. When the other industries are observed, Commerce, Manufacturing, Services, and Utilities have very similar results, between 43.62 and 47.25 – see Figure 1. These statistical differences demonstrate that challenges and vulnerabilities are not homogeneous across sectors, as each industry has specific operational characteristics, data sensitivity levels, and regulatory requirements.

Technology companies tend to have better results in data security, as this is a core area of their business. However, these companies occupy a paradoxical position: while they develop solutions to strengthen cybersecurity, they are also among the most targeted by attacks due to their interconnectivity and the high value of the data they store. Despite rapid technological advances, many information security problems arise from human factors. Therefore, in addition to security policies and risk mitigation strategies, it is essential to invest in user education and training, promoting digital literacy (Nikiforova, 2022).

As a result, technology companies, such as cloud service providers, social networks, and software platforms, need to constantly innovate to protect their systems and customers' systems, making data security a strategic factor for their competitiveness. Protecting data management systems is crucial to maintaining the integrity and confidentiality of information (Nikiforova, 2022). Therefore, the company's reputation is compromised if there is no security in this sense.

Figure 1
Boxplot Industries



Source: The authors (2022).

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

On the other hand, financial institutions also have data security as a market requirement. Based on the X-Force Threat Intelligence Index (2023) report, the finance and insurance sector has ranked second among the sectors most targeted by cybercriminals since 2018. Intrusion attempts are recurrent because they carry sensitive consumer data, such as banking details, financial routines, and economic power. Due to the responsibility for data security, these companies needed to improve their actions and evolve quickly in data security.

Thus, the results found are in line with the report presented by IBM, X-Force Threat Intelligence Index (2023), which identified that the number of cyberattacks has decreased since 2018 as companies in the sector are more advanced in digital transformations and, therefore, for an attack to happen, more work is required to be successful against these organizations. As the technology and financial sectors began to improve, other sectors began to gain attention to the vulnerability. They identified it as an opportunity for hackers to access it (IBM, 2023), so it is seen as an excellent management opportunity, especially for sectors that deal with the end consumer, such as commerce and services. However, unlike the Information Technology and Finance industries, data security is not profoundly linked to the core of these businesses.

According to the histogram, of 992 companies analyzed in the study, 48% have a score lower than 42, which is considered unsatisfactory for the analyzed variable. The worst result among the industries was manufacturing, with 43.79 points. If, on the one hand, JUST Capital extracts results from many companies, different from each other and which have distinct realities, on the other hand, user data security is a highly relevant topic. It has been gaining strength every time. Therefore, it is worrying that almost 50% of the companies analyzed have unsatisfactory results in a metric that can directly affect consumers.

The worst result among the sectors was manufacturing, with 43.79 points. This makes it a point of attention, given the high protection of the technology and finance sectors; the manufacturing sector was the one that suffered the most attacks (IBM, 2023), with challenges related to the protection of industrial data, intellectual property, and cybersecurity in automation systems. Attacks on these systems can compromise the supply chain and production efficiency. Since companies in this sector cannot stop their operations when facing problems with data privacy, attacks focus on extortion, which is a profitable strategy for attackers (IBM, 2023). Finally, the graph alerts us to the point of attention in the industrial manufacturing sector. In addition to having the worst average, it also has a low standard deviation level, showing consistency and homogeneity in the unsatisfactory result regarding data security.

Observing the graph makes it possible to infer that the Commerce and Services sectors demonstrate the presence of more outliers than the other sectors. This behavior indicates a departure from a solid grouping that respects a representative data standard. A point of attention is needed. In commerce, the main focus is on protecting customer data, including payment information and purchase history. With the increasing digitalization of retail and e-commerce, threats such as financial fraud and privacy breaches have become more frequent. The services sector includes a broad spectrum of activities (healthcare, finance, education, technology), where confidentiality and data integrity are essential. Finally, in the utilities sector, data security is directly linked to critical infrastructure, where cyberattacks can affect essential services for the population. The sector needs to balance operational resilience with protection against sophisticated threats.

Despite this, the evolution of data, especially after the COVID 19 pandemic, forced companies to use technological and digital means to continue with their activities in a context where face-to-face activities were being avoided, as the NSFOCUS report shows.

Based on the estimation of data security value created and searching for the mean of the data from CUST.PRIV.MGMT, a rank, was created looking for the most performing enterprises in which industry group. With this information, it was possible to verify in the public report of each one the importance given to the issue of data security. Below are the main actions and concerns of the three companies of each industry

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

that performed the most in the CUST.PRIV.MGMT variable and disclosed their results in public annuals reports. The report analyzed is from 2019 and was collected on the companies' websites. The section seeks to understand and descriptively translate what are the actions of companies in favor of data security so that it is possible to relate this to the consumer's perception of value — see Table 4.

Table 4

Best Data Privacy Practices Found in Each Company

Sector	Code of companies	Pillars of Security of Data			
		Establishment of Privacy Policies and documentation	Monitoring of suppliers	Data Management	Operation Security
Commerce	**URBN**	**X**	**X**		
Commerce	**ETSY**	**X**		**X**	**X**
Commerce	**P&G**	**X**	**X**	**X**	**X**
Manufacturing	**INTC**				
Manufacturing	**PRAH**	**X**			
Manufacturing	**NVDA**	**X**			
Services	**NLSN**	**X**		**X**	**X**
Services	**BAX**	**X**		**X**	
Services	**ANTM**	**X**	**X**	**X**	**X**
Utilities	**AT&T**	**X**			
Utilities	**Sprint**				
Utilities	**Zayo**	**X**			
Finance	**PNC**	**X**	**X**	**X**	**X**
Finance	**SPGI**				
Finance	**INFO**	**X**	**X**	**X**	**X**
Information Technology	**Apple**				**X**
Information Technology	**MSFT**	**X**			**X**
Information Technology	**AKAM**				

Source: The authors (2025).

Moreover, from the analysis of public reports from 2019 of the top 3 rank companies of each industry, considering the JUST Capital database, we could identify the companies' actions to best protect their data and systems as well as what companies consider risks related to non-security of data (see Table 5).

From the consumer's perspective, companies that implement multiple data security pillars offer stronger protection against breaches, even when shared with external vendors. In addition, companies that establish privacy policies and documentation provide greater transparency on how their data is managed. This clarity enhances consumer confidence, as they can better understand and trust the company's data handling practices. Such proactive approach enhances intangible relational value, as customers recognize the company's commitment to safeguarding their data, fostering trust, strengthening relationships, and ultimately translating into greater customer long-term loyalty.

Notably, companies must actively monitor their suppliers, as third-party data breaches remain a significant concern. Despite consumer concerns about IT companies, out of 3 companies observed and 4 possible actions, only 1 company describes 2 actions. While Apple and Microsoft are recognized for their strong security, they do not cover all of the best practices identified in this dataset, suggesting possible gaps in documentation or undisclosed security measures. Equally concerning, only a minority of the leading companies in our sample (3 out of 18) fully implement all identified best practices.

In contrast to the information technology sector, companies in the financial sector explicitly state the actions for the pillars analyzed. Of the three companies, 2 describe all of the actions,

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

while S&P Global Inc. does not have any related actions, as it tends to focus on financial performance, strategic initiatives, and market trends. This may be because data security policies and practices are addressed in dedicated documents, while annual reports have a broader and more strategic scope.

Companies in the utility and manufacturing sectors describe the Establishment of Privacy Policies and documentation in their reports, demonstrating little concern regarding data security. This aligns with the results found by JUST Capital data, where consumers barely notice actions taken by companies in the sector. The comparison between consumer perception and reports also shows that, despite the perception in relation to commerce and services, these companies have significant concerns about making the actions they take described and public.

On one hand, effective data security management requires companies to adopt a comprehensive approach that aligns with regulatory policies such as the GDPR and CCPA. Implementing strong authentication and encryption systems, along with robust risk management programs, is essential to safeguarding sensitive information. Regular internal and external audits and inspections help identify vulnerabilities and ensure compliance with security standards. Additionally, firms must continuously seek improvements in data security by staying ahead of emerging threats and act quickly in cases of cyber intrusion. Allocating dedicated security teams and providing employee training further strengthens protection measures, fostering a culture of security awareness across all levels of the company.

On the other hand, companies recognize several critical risks associated with data insecurity, which can have severe financial and operational consequences. Government fines and financial sanctions imposed for non-compliance with data protection regulations, such as the GDPR and CCPA, can lead to substantial monetary losses. Additionally, loss of brand reputation and consumer confidence is a significant concern, as data breaches can erode trust, impact customer loyalty, and harm long-term business relationships. Furthermore, organizations face an increase in operating costs due to the expenses required to mitigate damages, including legal fees, cybersecurity enhancements, and compensation for affected parties. As a result, businesses must proactively invest in robust data security measures to prevent these risks and ensure compliance with evolving regulatory standards.

Table 5

Sum of our results

Actions Taken by Companies for Data Security	What Companies Consider Risks Related to Non-Security of Data
To follow regulatory policies taken as reference, such as the GDPR and the CCPA	Government fines and financial sanctions
To have authentication, encryption systems and risk management programs	Loss of brand reputation and consumer confidence
Promote internal and external audits and inspections	
Constantly seek improvements in data security	Increase of operating costs caused by the mitigation of damage suffered
To allocate teams focused on data security and train all the employees	

Source: The authors (2025).

Finally, not all companies view strict data security regulations favorably. Some argue that protecting users' cyber rights limits the effectiveness of certain advertising strategies, reducing their ability to collect and utilize consumer data. As a result, these restrictions may lead to lower profits by constraining communication channels and personalized marketing efforts.

Managerial Implication

Based on our findings, to strengthen data security management, companies should adopt a holistic security strategy that includes strong authentication protocols, encryption mechanisms,

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

and comprehensive risk management programs. Regular audits, vulnerability assessments, and penetration testing are essential to identify and address security gaps. Additionally, organizations must enhance transparency by establishing clear and accessible privacy policies and documentation, ensuring compliance with regulations such as GDPR and CCPA. Effectively communicating these policies helps build consumer trust by demonstrating a commitment to responsible data handling, and therefore, creating value for consumers.

Given that third-party breaches remain a significant concern, companies must actively monitor suppliers and external vendors by enforcing strict data protection contracts and conducting regular audits. Implementing a zero-trust framework can further mitigate external vulnerabilities. Internally, employee training and cybersecurity awareness programs are crucial in preventing security lapses, as human error remains a major risk factor. Regular training on phishing threats, secure password management, and data handling best practices fosters a culture of security awareness across all levels of the organization and it directly creates value for employees and indirectly to consumers.

To ensure regulatory compliance and avoid financial penalties, businesses should align with evolving data protection laws and dedicate resources to ongoing compliance monitoring, creating value for suppliers, employees and customers. Companies must also consider the long-term financial and reputational risks associated with data breaches. Investing in AI-driven threat detection, automated incident response systems, and secure cloud storage solutions enhances protection against cyber threats. Additionally, establishing a crisis response plan ensures rapid and effective mitigation in the event of a breach, minimizing damage and reinforcing customer confidence.

Finally, the finding that only 3 out of 18 leading companies fully implement the best practices highlights the need for industry collaboration. Companies should participate in cybersecurity forums, share threat intelligence, and align with recognized security frameworks such as ISO 27001 and NIST. By adopting these proactive strategies, companies can safeguard consumer data, build long-term trust, maintain regulatory compliance, and mitigate financial and reputational risks, ensuring sustainable success in an increasingly data-driven landscape. Companies that proactively act on it may develop a competitive advantage, resulting in converting intangible and relational value into performance.

CONCLUSION

Due to its increasing relevance in the business context, we analyzed data security practices that create value for consumers. To address our research question, we explored the JUST Capital 2020 database with 922 companies of six industries. Our findings indicated that there is an asymmetry between industries related to data privacy practices.

Our findings provide valuable contributions. In a context where data is considered one of the greatest assets in the corporate world, the acceleration of cyber-attack attempts is visible, ultimately affecting businesses and consumers. In this sense, the reports of companies excelling in data security metrics reveal recurring strategies across firms. Beyond preventive, control, and monitoring measures, some companies also adopt reactive strategies to mitigate damage. However, even with strong internal protections, data breaches can still occur through external vulnerabilities, such as supplier weaknesses or emerging attack technologies unknown to the company. This highlights the rapid evolution of information technology and the persistent exposure businesses face. Additionally, our research sheds light on the key factors that drive companies to invest in robust data security measures.

This study also clarified the opportunity for big data improvement in some sectors such as commerce, services, and manufacturing, bringing significant managerial contributions to the corporate environment. The main one refers to verifying the best practices adopted by companies concerned with data security and does not hesitate to place this aspect as one of the pillars of their management. Moreover, we provided valuable insights into the factors influencing managerial decisions, particularly companies' concerns about financial sanctions and reputational

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

damage resulting from data breaches. Additionally, it contributed to the literature by categorizing data security metrics within the JUST Capital database, offering a useful resource for future research seeking a deeper exploration of the topic.

This study has several limitations. It relies solely on JUST Capital's 2020 database, without examining potential changes in company metrics over time; future studies could benefit from analyzing longitudinal data. As a limitation, we highlight that intra-industry differences may impact the results, which could be mitigated by additional analyses considering variables such as company size and maturity level. Additionally, restricted access to JUST Capital's proprietary metrics prevented comparisons with companies in other regions, limiting the global scope of the analysis; future studies could benefit from analyzing cross-countries data, as the institutional context may influence data security. Another constraint is the exclusive focus on consumer perceptions of data security, overlooking insights from other stakeholders such as shareholders, employees, and government entities. Future research could explore these perspectives, conduct comparative studies using more recent JUST Capital data, identify value-destroying practices, and investigate the relationship between data security and financial performance. Our study represents an initial step towards understanding data security from perspectives not yet observed. As future studies, we suggest more robust statistical analyses to understand the influence of this variable on engagement, reputation, loyalty, trust or other aspects of stakeholder theory.

In conclusion, despite its limitations, our research offers a foundation for further refinement and future exploration. Potential directions for future studies include: i) how have companies' data security metrics evolved over time based on more recent JUST Capital databases?, ii) how do other stakeholders, such as shareholders, employees, and government entities, perceive the value of data security compared to consumers, iii) what are the differences in data security practices between companies in different countries, and how do they impact stakeholder trust?, iv) how has the COVID-19 pandemic influenced corporate data security measures and their effectiveness?, v) what specific practices contribute to value destruction in data security management? and vi) what is the relationship between a company's data security performance and its financial performance?

REFERÊNCIAS

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514.

Ahmad, H. I. (2020). Doing Better by Doing Good: Discussing the Value Potential of Selected "Just Companies". International Journal of Financial Research, 11(2), 40-50.

Anthem. (n.d.). Privacy & security standards. Anthem Corporate Responsibility. https://anthemcorporateresponsibility.com

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. Communications ofthe ACM, 57(11), 31–33. https://doi.org/10.1145/2668897

Barney, J. (2018). Editor's comments: Positioning a theory paper for publication. Academy of management review, 43(3), 345-348.

Boaventura, J. M. G., Bosse, D. A., Manuela Cunha de Mascena, K., &Sarturi, G. (2020). Value distribution to stakeholders: The influence of stakeholder power and strategic importance in public firms. Long Range Planning, 53(2), 101883. https://doi.org/10.1016/j.lrp.2019.05.003

Boaventura, J. M. G., Cardoso, F. R., da Silva, E. S., & da Silva, R. S. (2009). Teoria dos Stakeholders e Teoria da Firma: Un estudo sobre a hierarquização das funções-objetivo em empresas brasileiras. Revista Brasileira de Gestao de Negocios, 11(32), 289–307. https://doi.org/10.7819/rbgn.v11i32.378

Campos, D., & dos Reis Carreiro, F. (2024). Compliance e gestão de riscos em tempos de inovação e disrupção digital. Revista de Gestão e Secretariado, 15(4), e3743-e3743.

Chaorasiya, V., & SHRIVASTAVA, A. (2015). A survey on big data: techniques and technologies. International Journal of Research and Development in Applied Science and Engineering, 8(1), 1-4.

Donaldson, T., & Preston, L. E. (1995). The Stakeholder Theory of The Corporation: Con-

cepts, Evidence, And Implications and from the specific comments of many people, including Professors Aupperle. Academy of Management Review, 20(1), 65–91. https://doi.org/10.5465/amr.1995.9503271992

Farhad, M. A. (2024). Consumer data protection laws and their impact on business models in the tech industry. Telecommunications Policy, 48(9), 102836. https://doi.org/10.1016/j.telpol.2024.102836

Freeman, R. E. (1984). Strategic management: A stakeholder approach. In Strategic Management: A Stakeholder Approach. https://doi.org/10.1017/CBO9781139192675

Freeman, R. E., Harrison, J. S., Wicks, A. C., Parmar, B. L., & De Colle, S. (2010). Stakeholder theory: The state of the art.

Freeman, R. E. (2011). Managing for Stakeholders. SSRN Electronic Journal, 1–22. https://doi.org/10.2139/ssrn.1186402

Günther, W. A., Mehrizi, M. H. R., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. The Journal of Strategic Information Systems, 26(3), 191-209. https://doi.org/10.1016/j.jsis.2017.07.003

Harrison, J. S., Bosse, D. A., & Phillips, R. A. (2010). Managing for stakeholders, stakeholder utility functions, and competitive advantage. Strategic management journal, 31(1), 58-74. https://doi.org/10.1002/smj.801

Harrison, J. S., & Wicks, A. C. (2013). Stakeholder Theory, Value, and Firm Performance. Business Ethics Quarterly, 23(1), 97–124. https://doi.org/10.5840/beq20132314

IBM. (2023). IBM Security X-Force Threat Intelligence Index 2023. IBM. https://www.ibm.com/reports/threat-intelligence

International Organization for Standardization & International Electrotechnical Commission. (2013). ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls. ISO. https://www.iso.org

JUST Capital. (2020). Amidst Crisis, What Americans Want From Corporate America. October. Retrieved from: https://accounts.justcapital.com/download?file=8e34607577671197b1205f-745d0ab170

JUST Capital. (2020, October). Amidst crisis, what Americans want from corporate America. [Relatório]. JUST Capital. https://accounts.justcapital.com/download?file=8e34607577671197b1205f-745d0ab170

JUST Capital. (2023). JUST Capital's quarterly review of stakeholder performance: Q4 2023. JUST Capital. https://justcapital.com/reports/just-capitals-quarterly-review-of-stakeholder-performance-q4-2023/

JUST Capital. (n.d.). Mission & impact. JUST Capital. https://justcapital.com/mission-impact/

Liu, C., & Babar, M. A. (2024). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. Australian Journal of Management, 03128962241293658.

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. Iberian Conference on Information Systems and Technologies, CISTI, 2019-June(June), 1–6. https://doi.org/10.23919/CISTI.2019.8760937

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. Journal of Marketing, 81(1), 36-58. https://doi.org/10.1509/jm.15.0497

Madsen, A. K. (2015). Between technical features and analytic capabilities: Charting a relational affordance space for digital social analytics. Big Data and Society, 2(1), 1–15. https://doi.org/10.1177/2053951714568727

Nikiforova, A. (2022, April). Data security as a top priority in the digital world: preserve data value by being proactive and thinking security first. In The International Research & Innovation Forum (pp. 3-15). Cham: Springer International Publishing.

NSFOCUS, Inc. (2019a). Cybersecurity insights. In-Tech, 66(2).

NSFOCUS, Inc. (2019b). Vulnerability and threat trends research report 1-day. NSFOCUS.

Orbik, Z., & Zozuľaková, V. (2019). Corporate Social and Digital Responsibility. Management Systems in Production Engineering, 27(2), 79–83. https://doi.org/10.1515/mspe-2019-0013

Parmar, B. L., Freeman, R. E., Harrison, J. S., Wicks,

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

A. C., Purnell, L., & De Colle, S. (2010). Stakeholder theory: The state of the art. The academy of management annals, 4(1), 403-445. https://doi.org/10.1080/19416520.2010.495581

Priem, R. L. (2007). A consumer perspective on value creation. Academy of Management Review, 32(1), 219–235. https://doi.org/10.5465/AMR.2007.23464055

Santos, R. de O. S., Jr., Uchôa, M. T., Olar, A. I., & Boaventura, J. M. G. (2024). Value Distribution to Stakeholders: Insights from U.S. Publicly Traded Companies. Revista Ciências Administrativas, 30, 1-17. DOI: http://doi.org/10.5020/2318-0722.2024.30.e14322

Shankar, N., & Mohammed, Z. (2020). Surviving data breaches: A multiple case study analysis. Journal of Comparative International Management, 23(1), 35-54. https://doi.org/10.7202/1071508ar

Soares, C. S., Sarturi, G., & Boaventura, J. M. G. (2014). Afinal, o que é distribuir valor para os stakeholders? Engema, 17.

Soares de Souza, T., & Tomei, P. A. (2024). CULTURA ORGANIZACIONAL E LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Revista Pensamento Contemporâneo em Administração, 18(4).

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880–1903.

Someh, I., Davern, M., Breidbach, C. F., & Shanks, G. (2019). Ethical issues in big data analytics: A stakeholder perspective. Communications of the Association for Information Systems, 44(1), 718–747. https://doi.org/10.17705/1CAIS.04434

Surfshark. (2024). Data breach recap 2024. Surfshark. https://surfshark.com/research/study/data-breach-recap-2024

Tankard, C. (2016). What the GDPR means for businesses. Network Security, 2016(6), 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

Valentinov, V., & Chia, R. (2022). Stakeholder theory: A process-ontological perspective. Business Ethics, the Environment & Responsibility, 31(3), 762–776. https://doi.org/10.1111/beer.12441

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

APPENDIX

Appendix 1

Grouping Variables of JUST Capital

CUST.PRIV	CUST.PRIV. MGMT	CUST.PRIV.QUAL. CHANGES	CUST.PRIV.QUAL. CHANGESADV	Advanced Notice of Privacy Policy Changes
			CUST.PRIV.QUAL. CHANGESDISC	Disclosure of Privacy Policy Changes
		CUST.PRIV.QUAL. LANGUAGE	CUST.PRIV.QUAL.EN-GLISH	Privacy Policy in English
			CUST.PRIV.QUAL.SPA-NISH	Privacy Policy in Spanish
			CUST.PRIV.QUAL. OTHER	Privacy Policy in Other Languages
		CUST.PRIV.QUAL. POLICY	CUST.PRIV.QUAL.DISC	User Information Disclosure
			CUST.PRIV.QUAL.EASE	Accessible Privacy Policy
		CUST.PRIV.UI.DA-TAUSE	CUST.PRIV.UI.ADVERT	Customer Data Used in Advertising
			CUST.PRIV.UI.SELL	Customer Data Selling Practices
		CUST.PRIV.UI.TYPE	CUST.PRIV.UI.ONLY-NECC	Only Necessary User Information Collected
			CUST.PRIV.UI.DISC	User Information Disclosure
		CUST.PRIV.UI.DA-TACONTROL	CUST.PRIV.UI.TRA-CKING	Tracking of User Activity
			CUST.PRIV.QUAL.PO-LICYSCOPE	Broad Privacy Policy Scope
			CUST.PRIV.SECURITY. BREACHES	User Data Security Breaches
			CUST.PRIV.SECURITY. NOTIFY	Customer Security Notifications/User Security Notification
			CUST.PRIV.SECURITY. OVERSIGHT	User Data Security Oversight

Source: Adapted from JUST Capital database (2020).

DOI: https://doi.org/10.14210/alcance.v32n1(jan/abr).p86-105

APPENDIX
Appendix 2
Companies Analyzed

Code	Company	Sector
URBN	Urban Outfitters Inc	Commerce
ETSY	Etsy, Inc.	Commerce
P&G	The Procter & Gamble Company	Commerce
INTC	Intel Corp	Manufacturing
BAX	Baxter International Inc	Manufacturing
NVDA	NVIDIA Corp	Manufacturing
NLSN	Nielsen Holdings PLC	Services
PRAH	PRA Health Sciences, Inc.	Services
ANTM	Anthem, Inc	Services
AT&T	AT&T Inc	Utilities
Sprint	Sprint Corp	Utilities
Zayo	Zayo Group Holdings, Inc.	Utilities
PNC	PNC Financial Services Group Inc	Finance
SPGI	S&P Global Inc.	Finance
INFO	IHS Markit Ltd	Finance
Apple	Apple Inc	Information Technology
MSFT	Microsoft Corporation	Information Technology
AKAM	Akamai Technologies Inc	Information Technology