The Impact of Data Breaches on Marketing Performance Maritime

عمرو محي الدين قناوي

باحث دكتوراه في إدارة الاعمال كلية الدراسات العليا للأعمال بالاكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

تحت إشراف

أ.د/منى قدري

عميد كلية الدراسات العليا بالاكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

أ.د/ هشام دنانة

أستاذ دكتور التسويق الاستراتيجيبالاكاديمية والجامعة الامريكية في مصر

Abstract:

This research, focusing on the healthcare industry, explores how data breaches in various companies affect their marketing effectiveness. It also aims to investigate the impact of data breaches on differences in customer trust, attitude, behavior, and loyalty due to the moderating effects of industry type, organizational nature, firm size, and data characteristics. What is important and unique about this research is that, against a growing volume of research, this one focuses on how a data breach has complex impacts on many areas of marketing, rather than focusing on areas like cybersecurity and organizational effectiveness.

This research, therefore, employs a mixed-methods methodology, combining an online survey of Egyptian marketing professionals with semi-structured interviews with key informants. The results show that data breaches significantly destroy customer trust, leading to a series of destructive consumer behaviors in the form of propagating false information, negative word-of-mouth, and customer defection. The study also identifies organizational responses as crucial in curbing the erosion of trust. This study points out that for customer loyalty to be regained post-data breach, it is necessarily dependent on appropriate communication as well as corrective actions. Secondly, this research identifies the attitudes of consumers as key in causing an effect on behavioral intentions regarding post-data breaches. A good attitude facilitates customer loyalty while a bad experience discourages customers from returning. Importantly, the customers' perceptions of control over their data are of critical importance in shaping their loyalty intentions. A greater perception of control over data results in a decrease in perceived vulnerability.

The findings of this study are the foundation for further research needed in this area and provide potential indications of the strategies organizations might adopt to protect marketing performance in a data breach.

الملخص:

تستقصي هذه الدراسة تأثير خرق البيانات على أداء التسويق داخل المنظمات، مع التركيز بشكل خاص على قطاع الصحة. تهدف الدراسة إلى تحليل كيف تؤثر التغيرات في ثقة العملاء، ومواقفهم، وسلوكياتهم، وولائهم على معدل خرق البيانات. مع الأخذ في الاعتبار الأدوار المعدلة لنوع الصناعة، وطبيعة المنظمة،

وحجم الشركة، وخصائص البيانات. تكمن أهمية هذا البحث في نهجه الجديد؛ حيث يستكشف الطرق المعقدة التي تؤثر بها خروقات البيانات على أبعاد مختلفة من التسويق، متجاوزًا الاعتبارات التقليدية للأمن السيبراني ونجاح المنظمات.

من خلال استخدام منهجية مختلطة، تتضمن هذه الدراسة استبيانًا عبر الإنترنت لمتخصصي التسويق المصريين، بالإضافة إلى مقابلات شبه منظمة مع شخصيات بارزة في هذا المجال. تكشف النتائج أن خروقات البيانات تضعف بشكل كبير ثقة العملاء، مما يؤدي إلى سلوكيات استهلاكية ضارة، بما في ذلك نشر معلومات مضللة، والكلام السلبي، وانسحاب العملاء. علاوة على ذلك، تسلط الدراسة الضوء على الدور الحاسم لاستجابات المنظمات في التخفيف من تآكل الثقة. إن التواصل الفعال والإجراءات التصحيحية ضرورية لاستعادة ولاء العملاء بعد خرق البيانات. بالإضافة إلى ذلك، تؤكد هذه الدراسة على تأثير مواقف المستهلكين على نواياهم السلوكية في سياق ما بعد خرق البيانات. تعزز المواقف الإيجابية ولاء العملاء، في حين أن التجارب السلبية تثبط العودة. والأهم من ذلك، أن تصورات العملاء حول السيطرة على بياناتهم تلعب دورًا محوريًا في تشكيل نوايا ولائهم؛ حيث يرتبط الشعور الأكبر بالسيطرة بانخفاض الإحساس بالهشاشة.

تشكل نتائج هذه الدراسة الأساس للبحوث المستقبلية في هذا المجال الحيوي وتوفر رؤى قيمة حول الاستراتيجيات التي يمكن أن تتبناها المنظمات لحماية أدائها التسويقي في مواجهة خروقات البيانات.

Keywords: Data Breach, Consumer Trust, Marketing Performance, Customer Behavior, Cybersecurity.

Introduction:

Today's data-driven landscape finds businesses understanding how vital marketing data has become and forms ways to strategize toward such end customers. The explosion of data from all directions is converting a somewhat traditional approach to marketing into an astute, analytical discipline. (Cognism, 2022). This paper seeks to identify the complex interrelationship between data breaches and marketing performance, especially in the healthcare industry. While businesses are increasingly relying on consumer data to target their marketing, data breaches could serve as a severe threat to consumer trust and loyalty in general marketing effectiveness.

The study investigates how data breach incidents affect different dimensions of marketing performance, such as consumer behavior, customer loyalty, and consumer attitude. These would, in turn, yield valuable insights into the wider ramifications of data security on marketing strategies and organizational reputation. This paper also identifies key cybersecurity measures that, if implemented effectively, can reduce the negative consequences of a data breach and improve marketing performance by engendering greater consumer trust.

The study adopts a mixed-methods approach, both in quantitative surveys and qualitative interviews, and thereby contributes to the literature by highlighting the multi-faceted outcomes of data breaches on marketing performance. The findings will also be useful for organizations, researchers, and practitioners to further press the importance of data protection strategies in an increasingly digital marketplace.

2. Literature Review

2.1 Impact of Data Breaches on Customer Behavior

Data breaches have a significant effect on customer behavior, trust, and buying intentions for the concerned firm. On one side, various studies have shown that even though a breach can hurt consumer confidence, it often does not result in increased security behaviors among customers. On the other hand, consumers feel a lack of control over their security, which creates a paradox whereby consumers do not change their security practices after a breach has occurred. (Curtis, Carre, & Jones, 2018).

This finding indicates that the reputation of a company is a stronger determinant in customer trust persistence after a breach than the quality of security statements. In this regard, companies providing monitoring services after a data breach reduce the negative connotations and facilitate revisits by consumers for subsequent purchases despite heightened perceptions of risk. In contrast, consumers notified of breaches through media reports are least likely to continue transactions with the affected company, revealing a strong media effect on consumer behavior. (Aivazpour, Valecha, & Chakraborty, 2019).

Furthermore, research has shown that consumers more often blame their security habits than the organization that was breached, which shows that there is a lack of awareness about data security. Although customer defections following breaches are low, many consumers wish for swifter notifications and accountability by businesses, meaning effective communication can be a retention tool for customer loyalty. (Janakiraman, Lim, & Rishika, 2018), (Mayer, Zou, Schaub, & Aviv, 2021).

Moreover, emotional reactions to breaches, such as fear and anger, may differentially influence consumer intentions. While fear increases sensitivity to the scope of the breach, thereby increasing the likelihood of avoidance of the business where the breach occurred, anger may lead to insensitivity to the scope of the breach. (Chatterjee, 2019).

Overall, though data breaches tend to immediately impact consumer trust and behavior, businesses that do respond well through communication and remediation can mitigate most long-term damage and protect customer relationships. Figure 1 shows the proposed research model used in this study.

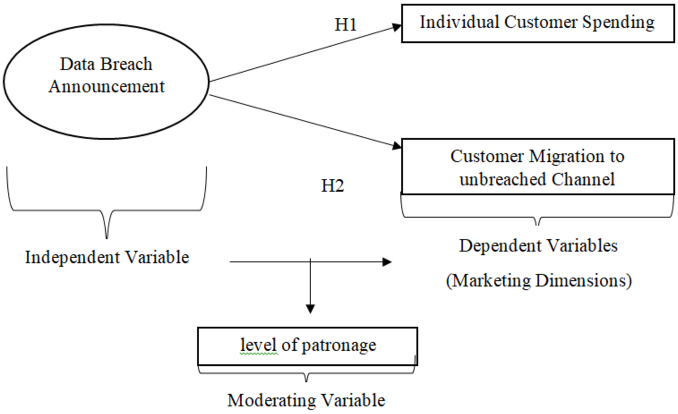


Figure 1: Proposed Research model used by (Janakiraman, Lim, & Rishika, 2018)

2.2 Impact of Data Breaches on Customer Loyalty

Data breaches have a huge impact on customer loyalty, though the influence may vary depending on the context and the breach itself. Studies show that online data privacy is not a major driver of customer loyalty, but data breaches can result in a loss of trust among customers, especially those enrolled in loyalty programs. Loyal customers are more likely to react negatively to a data breach, as their level of trust decreases more than that of non-users of loyalty programs. Second, trust rebuilding after a breach will require effective crisis management and communication. (Hugosson & Dahlén, 2021).

Other studies also show that consumers tend to view data breaches as a result of factors other than their actions, further indicating that perceptions are important in assessing blame. The controllability of the breach-that is, whether the customer perceives the organization could have prevented it predicts loyalty intentions. If customers think that a company is in control of the breach, their loyalty will likely decrease. (Chen & Jai, 2021), (Nsibande, 2020).

Besides, the magnitude of the breach does not impact uniformly on customer loyalty; it is revealed that perceived cause and controllability are more important than the magnitude of the breach itself (Monroe & Lane, 2019). On the whole, organizations must understand these dynamics to manage effectively customer relationships in a post-breach situation and minimize the long-term effects on loyalty. Therefore, the authors proposed that (Figure 2):

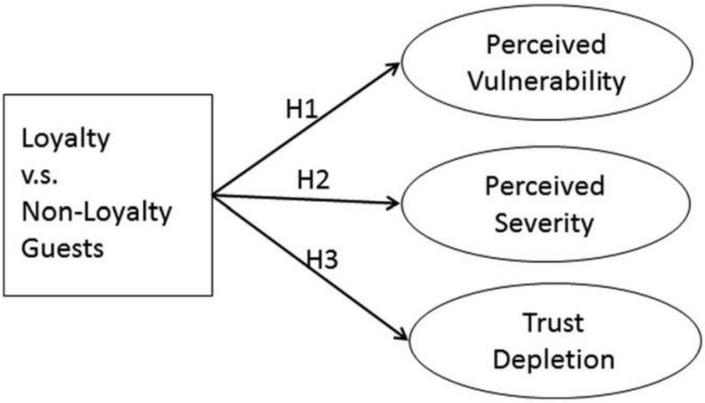


Figure 2: Proposed Framework used by (Chen & Jai, 2021).

Another research paper's objective is to explore the effect that data breaches of varied degrees of severity have on the loyalty of customers. (Nsibande, 2020). The authors postulated four hypotheses which are shown in Figure 2-3.

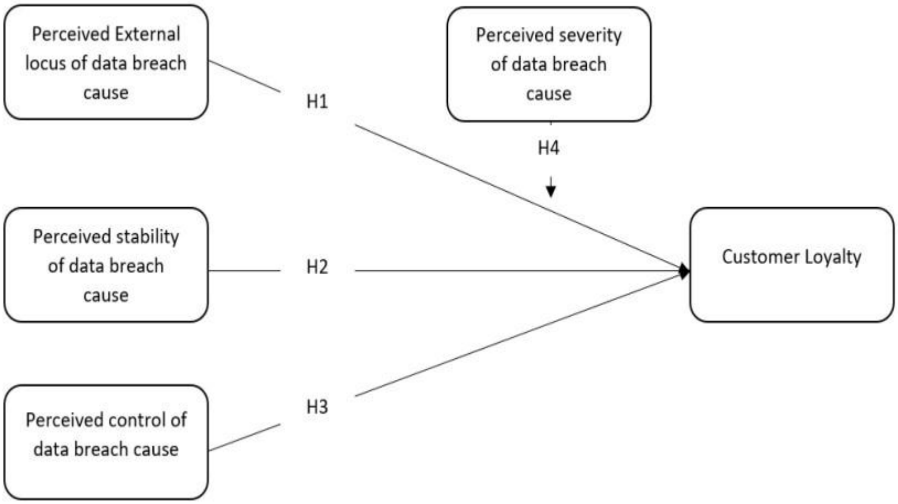
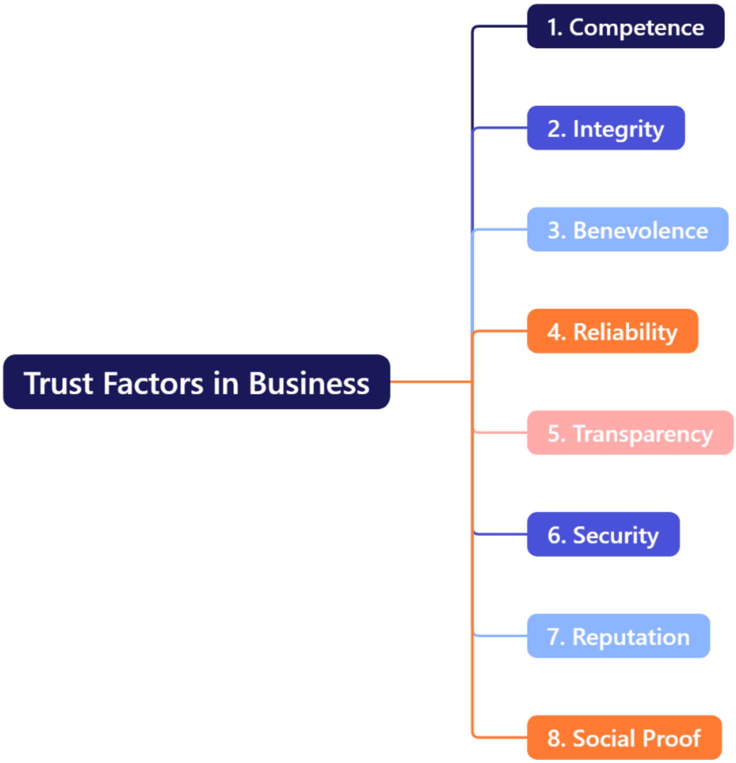

Perceived External locus of data breach cause
Perceived severity of data breach cause
H1
H4
Perceived stability of data breach cause
H2
Customer Loyalty
H3
Perceived control of data breach cause

Figure 3: Proposed Framework used by (Nsibande, 2020).

2.3 Impact of Data Breaches on Consumer Trust

Trust can be understood as the firm belief in the truth and ability of an organization concerning the security of private information and safety in service delivery. Trust is essential to ensure consumer loyalty, repeat purchasing, and positive word-of-mouth. (Curtis, Carre, & Jones, 2018).

Key dimensions of consumer trust include:



The given dimensions are essential to ensure the trust of the consumer in general, and more especially for a consumerist culture that was rapidly thrust into electronic commerce. The impact of the breach undermines consumer trust: as soon as that trust is violated, online transactions and loyalty fall. Cases of data breaches, like Capital One (2019) and Marriott International (2020), point to lost consumer trust due to inadequate security measures. In these events, trust can be regained through enhanced security, openness, and an immediate one. (Kumari, Sinha, & Priya, 2014).

2.4 Impact of Data Breaches on Consumer Attitude

Consumer attitude depicts a manner of feeling, beliefs of man, and intention to undertake an action toward a firm, product, or service. Marketing, social influences, cultural backgrounds, and individual experiences form a set of beliefs. The way consumers show their reactions toward data breaches depicts their worries about their sensitive personal information being safe and how much they believe in corporations. (Ablon L. , Heaton, Lavery, & Romanosky, 2016). Key findings by Ablon et al. in consumer attitudes towards notifications of data breaches include the following:

- Consequences for Trust: Data breaches incur severe losses in public confidence in the capabilities of different entities to protect personal information, thus reducing consumer trust in data security measures.
- Reaction to Notifications: Consumer reactions to breach notifications are all over the place, with many unhappy concerning how companies handle notifications and subsequent actions taken. Satisfaction varies depending on the type of data lost and corporate response.
- Importance of Remediation Offers: Remediation-free credit monitoring offer, for instance- indicates a company is taking responsibility for protecting consumer information.

- Perceived Personal Costs: It shows that consumers are increasingly worried about the financial and personal security implications of data breaches.
- Recommendations for Improvement: Companies should improve communication and post-breach response strategies as means of building consumer confidence and satisfaction, emphasizing openness and effective remediation options.

3. Methodology:

The primary concern of this study is to look into how data breaches affect businesses' marketing, specifically how they deal with customers and how loyal they are. Some factors that act as mediators in this relationship are trust, attitude, and level of control. The relationships between these variables could be shown in the proposed research model that is depicted in Figure 4.

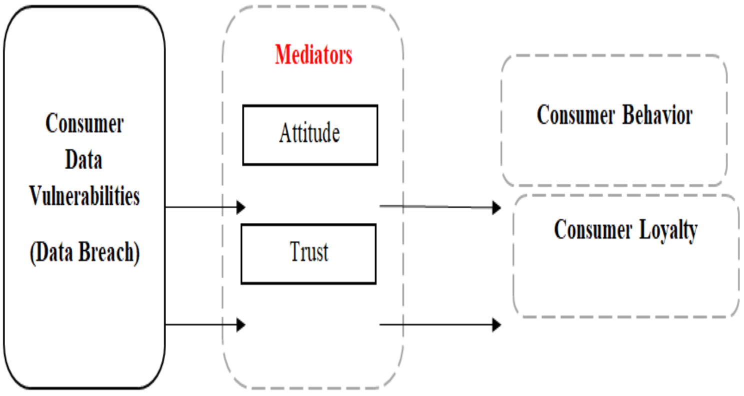


Figure 4: Proposed research model.

3.1 Research hypothesis

Hypothesis	
H1	There is a statistically significant relationship between Dealing with data breaches and consumer behavior.
H2	There is a statistically significant relationship between Dealing with data breaches and consumer loyalty.
H3	There is a statistically significant relationship between Dealing with data breaches and consumer attitude.
H4	There is a statistically significant relationship between consumer attitude and consumer behavior.
H5	There is a statistically significant relationship between Dealing with data breaches and consumer trust.
H6	There is a statistically significant relationship between consumer trust and consumer loyalty.
H7	There is a statistically significant relationship between consumer trust and consumer behavior.
H8	There is a statistically significant relationship between consumer attitude and consumer loyalty.

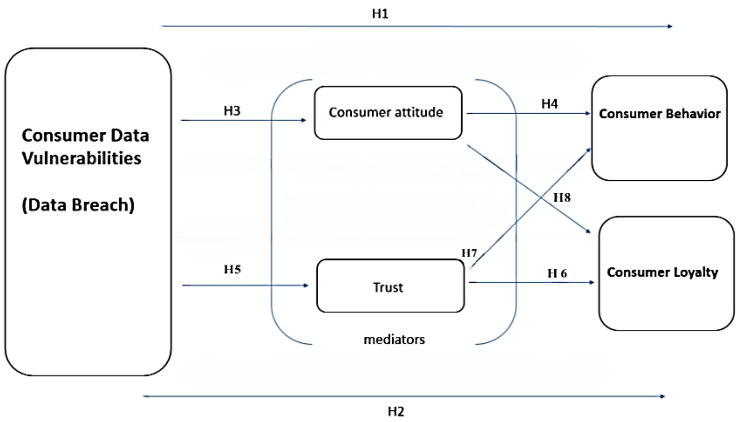


Figure 5: Proposed research model

The descriptive research design will be used in this study, based on a web survey to ascertain the attitudes of consumers regarding data breaches and the consequent effects on marketing performance. In this respect, the methodology covers the following: a statement of problem and research objectives; review of related literature on the impact of data breaches on marketing indicators; and a structured questionnaire with the following 2 sections:

- Section One: Demographic Variables (e.g., sex, age, employment position, experience).
- Section Two: Attitudinal Measures using a 5-point Likert scale for measuring perceptions about data breaches.

The target population involves managers, department heads, and marketers in various companies in Egypt; a sample size of approximately 100 responses was calculated using the specified formula. Data collection will be done through emails and social media platforms, followed by a thorough data analysis using descriptive and inferential statistical methods, including reliability testing and hypothesis testing by two-way ANOVA and Structural Equation Modeling (SEM). Moreover, qualitative interviews with experts will be carried out to grasp what each of them feels about data breaches. This is aimed at providing useful insights into future marketing and cybersecurity strategies.

4. Results and Discussion

A total of 490 individuals participated in answering the questionnaire and after the exclusion of responses containing missing data, a total of 465 valid responses were considered eligible for analysis.

Table 1: Demographic characteristics. Source: prepared by the researcher.

Total	Age							
465	Less than 20		20:30		30:40		Over 40	
	79	17.0%	229	49.2%	146	31.4%	11	2.4%
	Gender							
	Male				Female			
	286		61.5		179		38.5%	
	Education							
	High School Diploma		Bachelor's Degree		Graduate Degree (Masters, Ph.D.)		Other	
	45	9.7%	334	71.8%	69	14.8%	17	3.7%

As for descriptive statistics, respondents generally view the management of the data breach of this company positively; mean scores on all items exceed 3.91. They show a positive attitude toward the firm: they intend to continue using the website and recommend it to friends. At the same time, they had relatively fewer responses such as negative word-of-mouth dissemination or competition migration. They also have resisted falsifying information and doing other forms of shopping.

Table 2: Descriptive statistics. Source: prepared by the researcher

Construct	Mean	Std. Deviation	Skewness	Kurtosis
Dealing with Data Breaches	04.04	0.67	-0.047	-0.818
Attitude	4.00	0.66	-0.041	-0.555
Trust	3.83	0.66	0.19	-0.783
Consumer Behavior	1.82	0.64	0.141	-0.717
Consumer Behavior	1.93	0.70	0.109	-1.148
Consumer Loyalty	1.99	0.67	-0.056	-0.895
Consumer Loyalty	1.96	0.66	0.047	-0.818

4.1Construct validity:

Construct validity describes the degree to which the measure represents what it is theoretically set to measure. Construct validity measures in this research were checked within a multi-staged procedure using the processes recommended by Gerbing et al., 1996. The EFA was done initially. This analysis allowed for the identification of items that did not fit well with the underlying construct and were thus removed to refine the measurement model. The revised model was tested for its fit using confirmatory factor analysis. This approach gave a strong test of the capability of the measurement instrument to reflect the theoretical construct it was intended to measure.

4.2 Exploratory Factor Analysis (EFA)

This was done using SPSS V25 by EFA through Hotelling's Principal Components extraction and Varimax rotation for the interpretation of the factors, retaining items with minimum factor loading on 0.3 for substantial loadings on the underlying factors. Of course, no item was excluded in the analysis, and the least related to its factor was DB8, with a loading value of 0.544. Results of exploratory Factor Analysis are summarized in Table NO.3

The Kaiser-Meyer-Olkin measure of sampling adequacy was 0.942, which falls within the criteria by Kaiser and Rice, 1974, of a meritorious level of sampling. This was further supported by the significance of Bartlett's test of sphericity, with a χ^2 of 16490.548, at p = 0.00.

Table 3: Exploratory Factor Analysis. Source: prepared by the researcher

Variable	Items	Loading	Variable	Dimension	Items	Loading
Dealing with Data Breaches	**DB1**	**0.676**	**Consumer Behavior**	**Falsifying Information**	**CBF1**	**0.754**
	DB2	**0.77**			**CBF2**	**0.664**
	DB3	**0.688**			**CBF3**	**0.642**
	DB4	**0.763**			**CBF4**	**0.684**
	DB5	**0.634**		**Shopping Alternatives**	**CBS1**	**0.659**
	DB6	**0.663**			**CBS2**	**0.789**
	DB7	**0.615**			**CBS3**	**0.722**
	DB8	**0.544**			**CBS4**	**0.637**
Attitude	**AT1**	**0.599**	**Consumer Loyalty**	**Negative Word of Mouth**	**CLN1**	**0.752**
	AT2	**0.739**			**CLN2**	**0.726**
	AT3	**0.632**			**CLN3**	**0.692**
	AT4	**0.633**		**Switching Behavior**	**CLS1**	**0.742**
	AT5	**0.715**			**CLS2**	**0.805**
Trust	**TR1**	**0.806**			**CLS3**	**0.756**
	TR2	**0.838**	**Trust**		**TR4**	**0.873**
	TR3	**0.778**			**TR5**	**0.852**

4.4 Confirmatory Factor Analysis (CFA)

A confirmatory factor analysis (CFA) was conducted using AMOS v26 to evaluate and refine the measurement model in an iterative process.

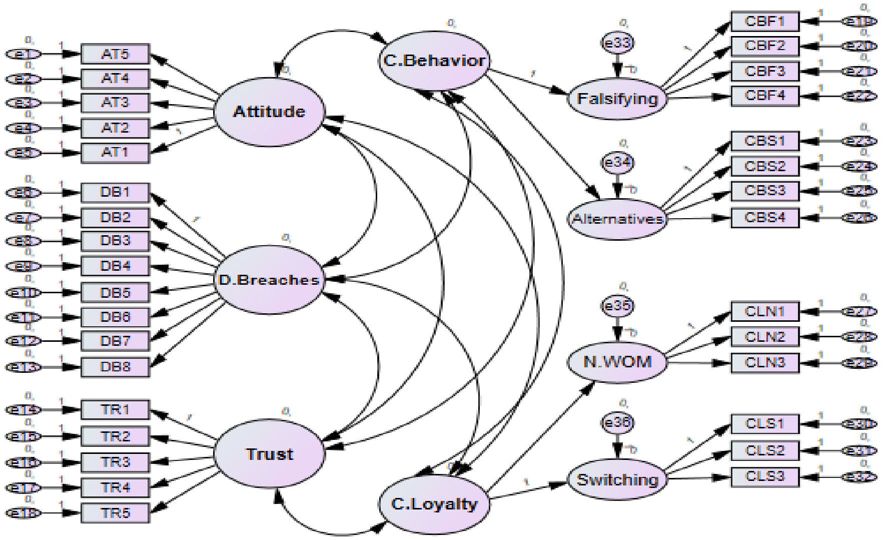


Figure 6: Confirmatory factor analysis (Start). Source: prepared by the researcher

The initial unadjusted confirmatory factor analysis (CFA) of the measurement model resulted in a significant chi-square statistic (CMIN/DF = 2.971, DF = 450, p = 0.00). However, several fit indices (NFI, RFI, TLI) fell below the commonly accepted thresholds for adequate model fit, as outlined by Hu and Bentler (1999) and Browne and Cudeck (1992).

Table 4: CFA Model Modifications and fit measures. Source: prepared by the researcher

Model Modifications	PCMIN/D	NFI	RFI	IF	TLI	CFI	RMSEA
	< 3	≥ 0.9	≥ 0.9	≥ 0.9	≥ 0.9	≥ 0.9	< 0.08
NO modifications	2.971	0.86	0.845	0.902	0.892	0.902	0.065
Eliminating (CLN1, DB5, TR1)	2.496	0.89	0.877	0.931	0.922	0.93	0.057
+ eliminating	2.332	0.907	0.893	0.944	0.936	0.944	0.054

(AT1, CBS1, CBS3)							
+ eliminating (AT5,DB1,DB3)	2.174	0.923	0.91	0.957	0.949	0.957	0.050

To improve model fit, modification indices were consulted, and a series of adjustments were implemented. These modifications primarily involved removing specific items. Following these refinements, the revised model achieved satisfactory fit indices (CMIN/DF = 2.174, CFI = 0.957, IFI = 0.957, NFI = 0.923, TLI = 0.949, RFI = 0.91, and RMSEA = 0.05).

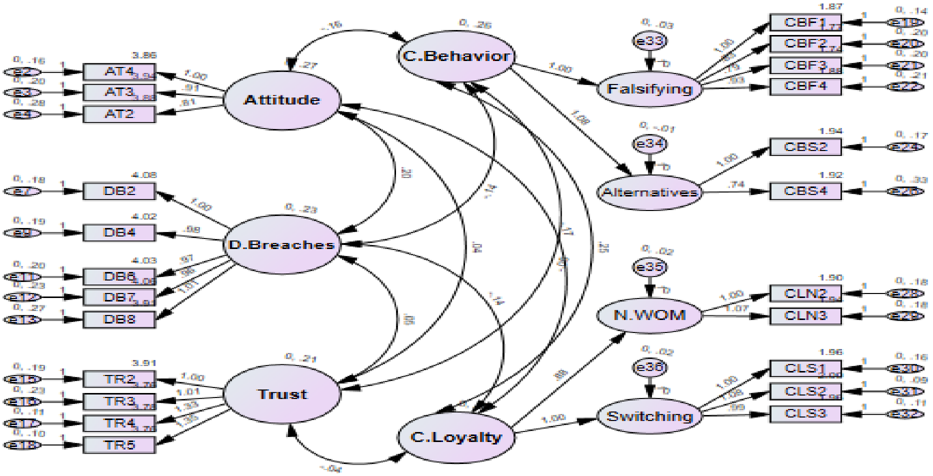


Figure 7 : confirmatory factor analysis (End). Source: prepared by the researcher

4.5 Reliability Analysis:

Table 5: Cronbach's Alpha Source: prepared by the researcher

Variable\ Dimension	Number of items	Cronbach's alpha (α)
Dealing with Data Breaches	٨	0.886
Attitude	٥	0.85
Trust	٥	0.894
Consumer Behavior	٨	0.892
Falsifying Information	٤	0.831
Shopping Alternatives	٤	0.808
Consumer Loyalty	٦	0.902
Negative Word of Mouth	٣	0.794
Switching Behavior	٣	0.887

Cronbach's alpha (α) was employed to evaluate the internal consistency of the scale using SPSS V25 software. All Variables and dimensions demonstrated both satisfactory reliability (α > 0.5) according to Nunnally (1978) and strong reliability (α > 0.7) based on the criteria established by Ketchen et al. (2006)

4.6 Hypothesis testing

The latent variables were computed, and path analysis was conducted to test the 3 relationships hypothesized. All analyses were done using AMOS v26. Path analysis was used because it is a statistically efficient way to comprehensively evaluate complex relationships.

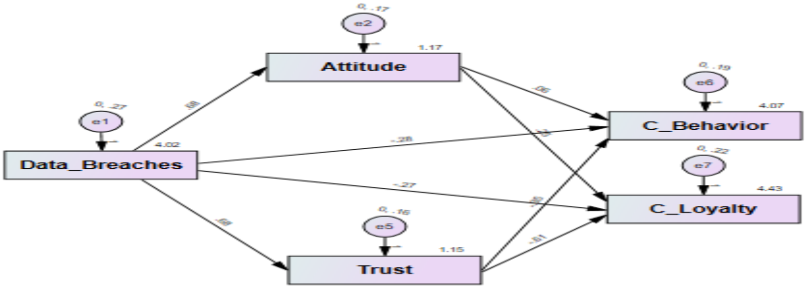


Figure 8: Path analysis. Source: prepared by the researcher

H1: There is a statistically significant relationship between Dealing with data breaches and consumer behavior (p ≤ 0.05).

Regression within the Path analysis framework revealed a statistically significant negative relationship between Dealing with data breaches and negative consumer behavior. The non-standardized regression coefficient (β) was -0.278 with a critical ratio (cr) of -4.551 exceeding the critical value (± 1.96) at a significance level (p) of 0.001 or less. This finding supports hypothesis H1, indicating a negative association between Dealing with data breaches and negative consumer behavior. The standardized weight of the regression is equal to -0.279, meaning that the higher the level of dealing with data breaches by 1, the lower the level of negative consumer behavior by 28%.

H2: There is a statistically significant relationship between Dealing with data breaches and consumer loyalty ($p \leq 0.05$).

Regression within a path analysis framework revealed a statistically significant negative association between Dealing with data breaches and negative consumer loyalty. The non-standardized regression coefficient (β) was -0.268 with a critical ratio (cr) of -4.037 exceeding the critical value (± 1.96) at a significance level (p) of 0.001 or less. This finding supports hypothesis H2, indicating a negative association between Dealing with data breaches and negative consumer loyalty. The standardized weight of the regression is equal to -0.231, meaning that the higher the level of dealing with data breaches by 1, the lower the level of negative consumer loyalty by 23%.

H3: There is a statistically significant relationship between Dealing with data breaches and consumer attitude ($p \leq 0.05$).

Regression within a path analysis framework revealed a statistically significant positive association ($\beta = 0.679$, $cr = 18.296 > 1.96$, $p \leq 0.001$) between Dealing with data breaches and positive consumer attitude, supporting hypothesis H3. The standardized weight of the regression is equal to 0.647, meaning that the higher the level of dealing with data breaches by 1, the higher the level of positive consumer attitude by 65%.

H4: There is a statistically significant relationship between consumer attitude and consumer behavior. ($p \leq 0.05$).

Path analysis did not yield a statistically significant association between positive consumer attitude and negative consumer behavior. The unstandardized regression coefficient was 0.062, with a critical ratio (CR) of 1.281. This CR value falls below the conventional threshold of 1.96, indicating a lack of statistical significance at the alpha level of 0.05. Further supporting this, the significance level of the test was 0.200, which is greater than the pre-established significance level (0.05). These findings suggest no significant relationship between positive consumer attitude and negative consumer behavior. Therefore, hypothesis H4 is not supported.

H5: consumer attitude mediates the relationship between dealing with data breaches and consumer trust ($p \leq 0.05$).

Regression within a path analysis framework revealed a statistically significant positive association ($\beta = 0.678$, $cr = 18.900 > 1.96$, $p \leq 0.001$) between Dealing with data breaches and positive consumer trust, supporting hypothesis H8. The standardized weight of the regression is equal to 0.660, meaning that the higher the level of dealing with data breaches by 1, the higher the level of positive consumer trust by 66%.

H6: There is a statistically significant relationship between consumer trust and consumer loyalty. ($p \leq 0.05$).

Regression within a path analysis framework revealed a statistically significant negative association between positive consumer trust and negative consumer loyalty. The non-standardized regression coefficient (β) was -0.609 with a critical ratio (cr) of -11.184 exceeding the critical value (± 1.96) at a significance level (p) of 0.001 or less. This finding supports hypothesis H2, indicating a negative association between positive consumer trust and negative consumer loyalty. The standardized weight of the regression is equal to -0.540, meaning that the higher the levels of positive consumer trust by 1, the lower the level of negative consumer loyalty by 54%.

H7: There is a statistically significant relationship between consumer trust and consumer behavior. ($p \leq 0.05$).

Regression within a path analysis framework revealed a statistically significant negative association between positive consumer trust and negative consumer behavior. The non-standardized regression coefficient (β) was -0.346 with a critical ratio (cr) of -6.907exceeding the critical value (± 1.96) at a significance level (p) of 0.001 or less. This finding supports hypothesis H2, indicating a negative association between positive consumer trust and negative consumer behavior. The standardized weight of the regression is equal to -0.357, meaning that the higher the levels of positive consumer trust by 1, the lower the level of negative consumer behavior by 36%.

H8: There is a statistically significant relationship between consumer attitude and consumer loyalty. (p ≤ 0.05).

Path analysis did not yield a statistically significant association between positive consumer attitude and negative consumer loyalty. The unstandardized regression coefficient was 0.247, with a critical ratio (CR) of 1.697. This CR value falls below the conventional threshold of 1.96, indicating a lack of statistical significance at the alpha level of 0.05. Further supporting this, the significance level of the test was 0.173, which is greater than the pre-established significance level (0.05). These findings suggest no significant relationship between positive consumer attitude and negative consumer loyalty. Therefore, hypothesis H6 is not supported.

Table 6: Results of Hypothesis testing. Source: prepared by the researcher

H. No	Path	Estimate	P	Remarks
H1	Dealing with data breaches → negative consumer behavior	-0.278	. ***	Supported
H2	Dealing with data breaches → negative consumer loyalty	-0.268	***	Supported
H3	Dealing with data breaches → positive consumer attitude	0.679	***	Supported
H4	positive consumer attitude → negative consumer behavior	0.062	0.200	Not supported
H5	Dealing with data breaches → positive consumer trust	0.678	***	Supported
H6	positive consumer trust → negative consumer loyalty	-0.609	***	Supported
H7	positive consumer trust → negative consumer behavior	-0.346	***	supported
H8	positive consumer attitude → negative consumer loyalty	0.247	0.173	Not supported

4.7 Qualitative data analysis

Following the interviews, the transcriptions were analyzed to assess the impact of data breaches on firms' marketing efforts concerning customer behavior and loyalty. The findings indicate that trust, attitude, and perceived control significantly influence this relationship. Section one discusses how consumer data vulnerabilities impact trust. It can be seen that while a data breach may initially strain trust, restoration depends upon the response of the company. The interviewees also highlighted transparency and pro-activity in communication as a key factor in rebuilding trust. Section two covers the impact of trust on consumer behavior: when trust is lost, consumers may engage in negative word-of-mouth and/or defect to competitors following a breach. The third aspect involves how consumer attitude leads to purchasing decisions, where positive attitudes generate loyalty, and negative ones, such as data breaches, will force customers to switch to other companies. Lastly, perceived control over data breaches: this is because consumers who are more in control over their information are less likely to react negatively. The interviewees have highlighted the fact that quick and effective responses in case of a breach are crucial to retaining consumer trust and loyalty; hence, there is a need for an effective incident response plan and clear communication.

5. Conclusion:

This paper tests how breaches of data in marketing immensely impact consumer trust and loyalty, more so within the health sector. The study adopts a mixed-methods approach in surveying and interviewing Egyptian marketing professionals and determined that data breaches can effectively weaken consumer confidence, leading to such negative behaviors as misinformation and customer defection. The findings accent how, even after a data breach incident, the organizational response has much to do along the lines of damage control-effective communication, transparency, and hence reinstallation of trust. Besides this, the consumer's control over their information shall be considered very relevant in commanding loyalty. While it points toward some very important clues, it is again limited by geographic boundaries, and cybersecurity or consumer behaviors are highly dynamic aspects. Future research might address the wider scope of data breaches within industries and regions, along with longitudinal studies to capture these events' long-term effects and in-depth qualitative inquiries into consumer attitudes regarding personal data protection. In general, the implication of this study for the difficult interrelation of data security and marketing effectiveness demands that every organization embrace effective cybersecurity measures to maintain brand integrity and restore consumer confidence in a progressively digital world.

References:

Ablon, L., Heaton, P., Lavery, D., & Romanosky, S. (2016). Consumer Attitudes Toward Data Breach Notifications and Loss of Personal

Information. Retrieved April 1, 2023, from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf

Aivazpour, Z., Valecha, R., & Chakraborty, R. (2019). Data Breaches: An Empirical Study of the Effect of Monitoring Services. The Data Base for Advances in Information Systems: In Press.

Chatterjee, S. G. (2019). Reacting to the scope of a data breach: The differential role of fear and anger. Journal of Business Research, 101, 183-193.

Chen, H., & Jai, T. (2021). Trust fall: data breach perceptions from loyalty and non-loyalty customers. The Service Industries Journal, 41(13-14), 947-963.

Cognism. (2022, 11 30). What is marketing data? Retrieved December 2, 2022, from What is marketing data?: https://www.cognism.com/what-is-marketing-data

Curtis, S., Carre, J., & Jones, D. (2018). Consumer security behaviors and trust following a data breach. Managerial Auditing Journal, 33(4), 425-435.

Hugosson, C., & Dahlén, V. (2021). Online data privacy as a driving factor for customer loyalty. Retrieved April 1, 2023, from https://www.diva-portal.org/smash/get/diva2:1725426/FULLTEXT01.pdf

Janakiraman, R., Lim, J., & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. Journal of Marketing, 82, 85-105.

Kumari, D., Sinha, P. C., & Priya, S. (2014). The impact of data breaches on consumer trust in e-commerce. International Journal of Current Science, 4(4), 1-9.

Mayer, P., Zou, Y., Schaub, F., & Aviv, A. (2021). Now I’m a bit angry:” Individuals’ Awareness, Perception, and Responses to Data Breaches that Affected Them. Retrieved April 1, 2023, from

https://www.ftc.gov/system/files/documents/public_events/1582978/now_i m_a_bit_angry_-
_individuals_awareness_perception_and_responses_to_data.pdf

Monroe, A., & Lane, J. (2019). People systematically update moral judgments of blame. Journal of Personality and Social Psychology, 116(2), 215-236.

Nsibande, S. (2020). The impact of Data Breaches of Varying severity on the customer loyalty of high net worth individuals in retail banking (Mini Dissertation (MBA) ed.). University of Pretoria.