ISSN 2303-4521
Original Research
Periodicals of Engineering and Natural Sciences
Vol. 12, No. 2, July 2024, pp.331-342

A big data approach to risk management and control: Cybersecurity in accounting

Petar Halachev
Department of Informatics, University of Chemical Technology and Metallurgy, Sofia, Bulgaria, https://orcid.org/0009-0008-2159-406X

ABSTRACT

This research reviews into the critical interplay between big data applications and cybersecurity risks within the accounting sector. Aimed at understanding how big data can mitigate these risks, the study develops a novel theoretical model using differential equations. This model, rooted in a thorough empirical approach, undergoes validation through logistic regression analysis of responses from 200 participants. The analysis particularly focuses on how demographic and socio-economic factors influence cybersecurity perceptions. Data Breach Consistency emerges as a key factor, evidenced by a coefficient of 1.204 and an odds ratio of 3.331, indicating a substantial link between the recognition of data breaches and increased cybersecurity concerns. Malware and Ransomware concerns demonstrate a notable impact, with a coefficient of 0.907 and an odds ratio of 2.477, underscoring the gravity of these threats. Results further highlight the mitigating influence of Big Data Mitigation on cybersecurity risks, marked by a coefficient of 0.491. The robustness of the model is affirmed by an Area Under the Curve (AUC) score of 0.843, attesting to its efficacy in predicting cybersecurity concerns. The findings highlight the vital role of big data in formulating effective cybersecurity strategies. This study not only contributes to the academic discourse on the intersection of big data and cybersecurity in accounting but also offers practical insights for enhanced decision-making and policy formulation in the evolving digital business environment.

Keywords: Cybersecurity, Big Data, Risk Assessment, Financial Security.

Corresponding Author:

Petar Halachev, PhD in Computer Science and Engineering, Associate Professor, Departement Informatics, University of Chemical Technology and Metallurgy, Sofia, Bulgaria, https://orcid.org/0009-0008-2159-406X
Corresponding author: (e-mail: x3m@mail.orbitel.bg)

1. Introduction

An increasingly pressing issue in this age of digital transformation is the potential overlap between accounting and cybersecurity. This study delves into the ever-changing landscape of cybersecurity risks in the accounting industry, a field where the exposure of financial data has been greatly amplified by the spread of digital technologies. Despite the many benefits to efficiency and accessibility brought about by the digital revolution in accounting practices, organizations are now vulnerable to complex cybersecurity threats. In a world where protecting private financial data is of the utmost importance, these dangers pose serious problems for corporate leadership and management. This research seeks to answer the scientific question of how accountants perceive cybersecurity in the context of big data. Innovative methods of risk management and data protection are required due to the ever-changing risk landscape caused by the growing interconnection of financial data. The pressing necessity for strong security protocols and cutting-edge analytical tools is brought to light by high-profile cybersecurity incidents in the corporate sector, which serve to emphasize this problem. The study aims to contribute to this field by investigating how big data is changing cybersecurity strategies in accounting. This will provide new ways of looking at digital risks in this important industry.

Accounting and cybersecurity have both been profoundly affected by the advent of the digital age. How quickly accounting and cybersecurity are becoming interdependent [1]. While financial data digitization has made many things easier and more efficient, it has also made institutions more vulnerable to cyberattacks.

Conventional accounting methods, which have mostly depended on tried-and-true auditing procedures, are facing new competition in this dynamic marketplace. The pressing need for innovative and flexible accounting methods to counteract new forms of cybercrime, such as the ransomware attack on the Colonial Pipeline in 2021, is highlighted by the devastating societal and economic effects of such crimes [2].

In their study, Wiguna et al. [3] investigate how e-government influences user behavior in relation to cybersecurity. In order to counter cyber threats, their research shows that e-government systems are widely adopted based on how useful they are perceived to be. The significance of user-centric approaches in developing and implementing digital governance solutions is emphasized by this perspective. In addition, there needs to be a lot of attention given to the part that big data analytics plays in improving cybersecurity risk management [4,5]. To further improve organizations' preparedness and responsiveness, big data analytics can be used to examine massive datasets in order to identify possible cyber threats early on. One key advantage of these technologies in detecting and reducing cyber risks is their capacity to process and analyze massive amounts of data in real-time.

One notable example of the ever-changing cyber threat landscape is the Notpetya ransomware attack [7]. In response to the points made by Calderon and Gao [8], our research clarifies how socioeconomic variables like income and education influence cybersecurity worries. Extra evidence of the cyberattack on the University of California, San Francisco [9]. The advent of such sophisticated cyberattacks is a watershed moment. Incidents like these show how cyber threats are getting more sophisticated and powerful, threatening not only specific companies but entire industries and even world trade.

This is an area where the work of Danko et al. [10] shines brightest. It explores Generation Z's points of view, illuminating how their geographical backgrounds impact their perceptions of cybersecurity risks. Various age groups may display different levels of concern regarding online privacy, according to Dinev and Hart [11]. Future research could delve further into the age-related dynamics of cybersecurity concerns, as this divergence suggests. One of the most important factors that contributes to increased cybersecurity concerns is data breach consistency, according to our findings [12–14]. Data breaches have a major effect on public opinion and anxiety, as shown by incidents like the Equifax data leak [15]. Accrual accounting is an essential part of modern financial management, and researchers are interested in how company culture influences its adoption. The capacity of an organization to adapt and react to the difficulties brought about by the digitalization of financial systems is heavily influenced by its internal culture [16].

There is a wealth of evidence demonstrating the seriousness and breadth of data breaches in the modern digital age, with substantial studies highlighting the effects of these cyberattacks. By referencing Klein's [17] research, the Ponemon Institute highlights the far-reaching consequences of data breaches and the seriousness with which they can jeopardize sensitive financial and personal information. Cybersecurity is a complex issue, and new research has shed light on the influence of demographic, socioeconomic, and corporate variables. Understanding the specific cybersecurity challenges that occur in different geographic and social contexts requires an analysis that focuses on demographics [18]. The significance of adapting cybersecurity strategies to the perspectives and realities of various age groups, especially digital native youth, is emphasized by their research.

The SolarWinds intrusion and other high-profile incidents have brought greater attention to the vulnerabilities in software supply chains [19]. In their discussion of big data analytics for cybersecurity risk management, Rezaee et al. [20] provide some useful pointers. The use of big data analytics by leading financial institutions such as JPMorgan Chase to detect fraud is indicative of a trend toward real-time monitoring and anomaly detection [21]. A more proactive and technically advanced approach to protecting financial data and systems from cyber threats is indicated by this trend.

A thorough study has been carried out by Navia et al. [22] to expand the discussion to include the interaction between digital strategies and the performance of businesses. Their study focuses on small and medium-sized service businesses in Colombia and how their financial results are affected by their digital market orientation. The importance of digital adaptation in today's business landscape is highlighted by this study, which highlights its role in reducing cybersecurity risks and improving economic performance. In light of the ever-increasing variety of cyber threats, they stress the need of digital market orientation as a defensive strategy for companies, particularly SMEs [23].

Numerous influences and implications are shown by the accounting and technology research landscape. The use of fair value accounting by Vietnamese construction firms is thoroughly examined in the study by Thanh et al. [24]. Usefulness, reliability, and the cost-benefit ratio are some of the important variables that their research reveals affect this accounting method's adoption. To improve transparency and the quality of financial reporting, it provides practical advice for businesses that want to optimize their accounting procedures to meet global standards.

Additionally, research by [25, 26] investigates the effects of digital technology and AI development on society. They shed light on how this new paradigm of interaction is changing many parts of society, including decision-making, by investigating the developing dynamics between people and AI systems. Critical conversations about the ethical aspects of AI development are brought to the forefront by their research. The importance of strong ethical frameworks in guiding the development of AI systems cannot be overstated, especially as these systems acquire greater independence and decision-making capacity. Their research is especially pertinent to the accounting and financial industries, where the growing use of AI calls for extra attention to questions of fairness, accuracy, and ethics.

The Equifax data breach of 2017 is a prime illustration of this [27]. Large firms suffered heavy financial losses as a consequence of this incident, which also brought up important questions regarding their privacy and data protection policies. Forensic accounting and cyber threat analysis have emerged as critical areas where big data technologies have emerged as a response to these expanding cybersecurity challenges. When it comes to cyber threat forecasting in particular, Naseer et al. [28] outline the capabilities of machine learning algorithms in predictive modeling. Their findings show that sophisticated algorithms can foretell when cyberattacks may occur, bolstering the use of big data technologies for preventative cybersecurity. Predictive analytics and machine learning will play a crucial role in preventing and mitigating cyberattacks, rather than merely responding to them, as this development indicates a change in the cybersecurity paradigm [29].

A growing body of research has highlighted the importance of human factors in cybersecurity and the need for extensive cybersecurity education. Since technological fixes aren't enough to counteract cyber dangers, Viana et al. [30] stress the importance of learning how people act and how it affects cybersecurity. A more comprehensive strategy for cybersecurity is called for by their research, and part of that strategy is teaching people how to be safe online and avoid common cyberpitfalls. Developing robust cybersecurity strategies that can withstand both technological and behavioral challenges requires this viewpoint.

Similarly, Ovcharova [31] explores how digitization could revolutionize the world economy. The research shows that smart, efficient economies are the result of investments in education and digital technology. According to Ovcharova [31], digitization causes a sea change in the way economies function and compete on a global scale, rather than merely an improvement in technology. In order for people and companies to succeed in this new digital economy, it is crucial that everyone's digital literacy and skills are up to par.

Furthermore, the intricacies of safeguarding consumer rights in the context of online transactions are investigated by Sanetra-Półgrabi and Tetłaka [32]. Their research illuminates the difficulties customers confront in the online marketplace due to the interplay between fast technology advancements and shifting economic conditions. According to the research, companies should change their marketing approaches to put an emphasis on consumer safety and ethical concerns in light of these shifting circumstances. They call for a shift in emphasis toward consumers, with a focus on online ethics, to protect rights and build confidence in online marketplaces.

This review compiles findings from a wide range of studies to show that technological developments, demographic changes, and socioeconomic factors are just a few of the many factors that affect the dynamics and difficulties of cybersecurity in accounting. As the digital world is constantly changing, new risks are emerging, and strategies need to be adjusted accordingly. Therefore, it is clear that this area requires ongoing study. The research team behind this project hopes to learn more about the ever-changing cyber dangers facing forensic accountants and how well big data solutions work to keep them safe. The research presents two hypotheses that are in line with these goals,

Hypothesis 1: The efficacy of cybersecurity measures is significantly related to the degree of digital adaptation in accounting practices.

Hypothesis 2: When it comes to forensic accounting and cybersecurity, big data technologies significantly lessen potential dangers.

2. Research method

In our study, we employed a dual approach combining theoretical modelling and empirical analysis to understand the dynamics of cybersecurity concerns in the context of accounting. Initially, we develop a theoretical model using differential equations to depict the evolution of cybersecurity concerns over time. This model is represented by the differential equation $\frac{dC}{dt} = f(D, M, B, A, S, I)$, where C signifies the level of cybersecurity concerns, and t denotes time. The variables $D, M, and\ B$ represent the consistency of data breach perceptions, concerns about malware and ransomware, and beliefs in the efficacy of big data in mitigation, respectively. Additionally, A accounts for age, S for gender (1 for male, 0 for female), and I for income and education levels. The model posits that an increase in D and M escalates cybersecurity concerns, while an increase in B diminishes them. To determine the optimal levels of $D, M, and\ B$ that influence the rate of change of cybersecurity concerns ($\frac{dC}{dt}$), we utilize a Lagrangian optimization approach. This involves setting up constraints within a normalized range for D and M and solving the Lagrangian function's partial derivatives concerning these variables and the Lagrangian multiplier (λ).

Building on the theoretical model, we have conducted empirical analysis using logistic regression, applied to primary data gathered from a survey. The survey, designed to capture a comprehensive view of cybersecurity perceptions, was distributed to 200 participants from diverse demographic and socioeconomic backgrounds. The survey specifically probed into areas such as data breach consistency, malware and ransomware concerns, confidence in big data technologies for cybersecurity, and demographic variables like age, gender, income, and education level. This primary data, collected directly through our survey efforts, forms the basis of our logistic regression analysis. This approach allows us to test the theoretical model's predictions against data, ensuring a robust examination of the factors influencing cybersecurity concerns in the field of accounting. The logistic regression model is formulated as follows:

$$y_i = \begin{cases} 1, y_i *> 0 \\ 0, y_i *\leq 0 \end{cases} y_i^* = x_i'\beta + \varepsilon_i$$

$$P(y_i = 1|x) = P({y_i}^* > 0|x) = P(x_i'\beta + \varepsilon_i > 0|x) = P(\varepsilon_i > -x_i'\beta|x) = 1 - F(-x_i'\beta)$$

$$P(y_i = 1|x) = 1 - \emptyset(-\frac{x_i'\beta}{\sigma}),\ \sigma \equiv 1 \qquad F(x_i'\beta = \emptyset(x_i'\beta) = \int_{-\infty}^{x_i'\beta} \emptyset z.dz$$

The logistic model addresses the issue of boundedness seen in linear probability models, making it more suitable for binary outcome variables in our study. A higher value of x may either raise or decrease the probability that $y_i = 1$. Thus, the range of possible outcomes can only be 1 or 0. Moreover, we have included McFadden's R square in our estimates to verify the appropriateness of the model. The maximum likelihood (ML) of a model is compared to a nested null model in these. In addition, if the McFadden R squared value is between 0.2 and 0.4, the model fits the data perfectly [22; 23]. By blending theoretical modelling with empirical data analysis, our methodology aims to offer a nuanced understanding of cybersecurity dynamics in accounting, providing valuable insights for effective risk management and mitigation strategies [40].

Our research draws upon data meticulously gathered from a survey distributed to a well-rounded cohort of 200 individuals. This survey was strategically designed to capture a representative cross-section of the population, thereby ensuring that the responses reflect a broad spectrum of perspectives and experiences. Such a diverse sample base enhances the robustness and generalizability of our findings. Central to our investigation are several key variables, each chosen to shed light on different facets of cybersecurity concerns within the context of forensic accounting. The first of these, *Data Breach Consistency*, is a critical measure that evaluates the extent to which respondents view data breaches as significant threats. This variable not only gauges general awareness about data breaches but also assesses their perceived impact in the realm of forensic accounting.

In parallel, we scrutinize the *Malware & Ransomware Concerns*. As cyber threats evolve in complexity and frequency, understanding how seriously individuals consider these types of risks becomes crucial. This variable provides insight into the level of concern about these specific forms of cyber threats during accounting investigations. Another pivotal aspect of our study is the role of technology in mitigating cyber risks. Here, the *Big Data Mitigation Confidence* variable comes into play. It measures respondents' trust in the capabilities of big data technologies to reduce cybersecurity threats, reflecting public perception of the effectiveness of data analytics in counteracting cyber risks.

In addition to these technology-focused variables, our study also delves into the demographic and socioeconomic dimensions of cybersecurity perceptions. The inclusion of *age* as a demographic variable allows us to explore whether and how concerns about cyber threats vary across different age groups. To examine gender-specific perspectives, responses from women were categorized under the variable '*Sex (Female)'*. This enables a nuanced analysis of the differential experiences and perceptions of cybersecurity issues among men and women. Moreover, we factor in *income and education level* to assess the influence of socioeconomic status on cyber-awareness and concerns, thereby providing a holistic view of the cybersecurity landscape.

Through the careful integration of these variables, our study aims to construct a comprehensive picture of cybersecurity perceptions. This approach not only facilitates a deeper understanding of the prevalent attitudes and concerns but also enables us to uncover subtle trends and variations across different demographic and socioeconomic groups. Descriptive statistics of variables are presented in Table 1.

Table 1. Descriptive statistical analysis of cybersecurity factors in accounting

Variable	Mean	St.Dev.	Min.	Max.	Range	Median	Skewness	Kurtosis
Data Breach Consistency	3.72	0.89	2	5	3	3.75	-0.45	1.21
Malware & Ransomware	3.48	0.74	2	5	3	3.50	0.12	-0.76
Big Data Mitigation	4.15	0.62	3	5	2	4.20	-0.67	1.54
Age	40.62	12.35	22	65	43	39.50	0.98	1.07
Income	2.68	1.02	1	5	4	2.75	-0.25	-0.94
Education Level	3.20	0.75	2	5	3	3.00	0.57	-0.35

3. Results and discussion

In our study, a differential equation model was constructed to analyze the dynamics of cybersecurity concerns over time. The model denoted as $\frac{dC}{dt} = f(D, M, B, A, S, I)$ encapsulates various factors influencing cybersecurity perceptions. Our findings indicate that heightened concerns about malware and ransomware $f(M)$ positively correlate with an increase in overall cybersecurity concerns over time. Conversely, a strong belief in the efficacy of big data technologies (function $f(B)$) is associated with a decrease in these concerns, suggesting a mitigating effect. The impact of age on cybersecurity concerns is noted to be complex and potentially nonlinear, possibly moderating the influence of other factors. Gender also plays a role in shaping perceptions and responses to cybersecurity risks, which is reflected in the binary function *f*(*S*). Additionally, higher income and education levels are observed to have a relationship with lower cybersecurity concerns, though this association may also be nonlinear.

We hypothesized that increased perceptions of data breaches and malware/ransomware as significant threats (D *and* M) *would correlate with elevated cybersecurity concerns. The model validates this hypothesis, indicating a direct positive relationship* $\frac{dC}{dt} = f(D, M) > 0$, *where higher values of D and M lead to increased concerns (C).* To simplify, we have assumed that both D *and* M are continuous variables within a normalized range of [0,1], where 0 represents no concern, and 1 represents maximum concern. $f(D, M)$is a function that quantifies the impact of these concerns on the rate of change of cybersecurity concerns (C). When individuals consistently perceive data breaches and malware/ransomware as significant threats (i.e., D and M are both close to 1), their concerns (C) increase over time. Therefore, it is written as $\frac{dC}{dt} = f(D, M) > 0$. We have $Maximize$ $\frac{dC}{dt}$ Subject to $D, M \in [0,1]$ and introduced a Lagrangian multiplier (λ) to incorporate the constraint

$$L(D, M, \lambda) = \frac{dC}{dt} - \lambda(D^2 + M^2 - 1)$$

Here, $D^2 + M^2$ is used to ensure that D and M remain within the normalized range. Then we took partial derivatives of L concerning D, M, and λ and set them equal to zero to find the optimal values.

$\frac{\partial L}{\partial D} = 0, \frac{\partial L}{\partial D} = 0, \frac{\partial L}{\partial \lambda} = 0$

Solving these equations yields the values of D and M that maximize the rate of change of cybersecurity concerns ($\frac{dC}{dt}$). These values represent the optimal levels of perceived data breach and malware/ransomware concerns that lead to the greatest increase in cybersecurity concerns over time.

Our second hypothesis posited that belief in the efficacy of big data in mitigating cybersecurity risks reduces concerns over time $(i.e., \frac{dC}{dt} = -f(B) < 0)$. The model supports this hypothesis as well, demonstrating an inverse relationship. Individuals who believe in the effectiveness of big data technologies for cybersecurity are likely to see their concerns mitigated as they perceive these technologies as protective measures. B is a continuous variable within a normalized range of [0,1], where 0 represents no belief in the efficacy of big data, and 1 represents full belief. While $-f(B)$ is a function that quantifies the impact of the belief in the efficacy of big data on the rate of change of cybersecurity concerns (C). Therefore, individuals strongly believe in the efficacy of big data in mitigating cybersecurity risks (i.e., B is close to 1), and their concerns (C) decrease over time. Therefore, we can write this function as, $\frac{dC}{dt} = -f(B) < 0$. Now $\frac{dC}{dt}$ is $maximized$ subject to $B \in [0,1]$

$$L(B, \lambda) = -\frac{dC}{dt} - \lambda(B^2 - 1)$$

B^2 is used to ensure that B remains within the normalized range. While $\frac{\partial L}{\partial B} = 0, \frac{\partial L}{\partial \lambda} = 0$. Solving these equations yield the value of B that maximizes the rate of change of cybersecurity concerns $(\frac{dC}{dt})$. This value represents the optimal level of belief in the efficacy of big data that leads to the greatest reduction in cybersecurity concerns over time. *The empirical validation of our hypotheses was conducted through logistic regression analysis, utilizing data from a survey of 200 individuals.*

Table 2. Model I, Factors Influencing Cybersecurity Risk: Logistic Regression Analysis

Variable	Coefficient (β)	Odds Ratio (OR)	95% CI (Odds Ratio)	p-value
Data Breach Consistency	1.204	3.331	[2.097, 5.288]	<0.001
Malware and Ransomware	0.907	2.477	[1.543, 3.982]	<0.001
Big Data Mitigation	0.491	1.633	[1.102, 2.416]	0.014
Age	-0.032	0.969	[0.930, 1.010]	0.178
Sex (Female)	-0.671	0.511	[0.279, 0.936]	0.032
McFadden's R-squared				0.303

Model I presented in Table 2, revealed significant variables influencing cybersecurity concerns. 'Data Breach Consistency' showed a strong positive association (β = 1.204, OR = 3.331), indicating heightened concerns about cybersecurity. *'Malware and Ransomware'* also had a notable positive impact (β = 0.907, OR = 2.477). Conversely, *'Big Data Mitigation'* demonstrated a mitigating effect on concerns (β = 0.491, OR = 1.633). Age and gender ('Sex: Female') had less pronounced effects, with age showing a slightly negative correlation and gender indicating lower concern among females. The model's overall fit, indicated by McFadden's R-squared of 0.303, suggests a moderate explanatory power.

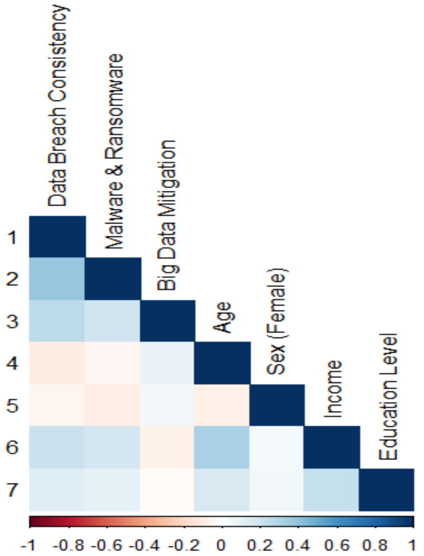

Figure 1. Correlation heatmap

These subsections cater to different research approaches quantitative and qualitative offering specific insights into the methodologies and techniques utilized within each approach. Depending on the research conducted, these subsections can be tailored and expanded to detail the specific methodologies employed within each paradigm.

4.1. Data analysis

The Data Analysis section is a pivotal segment within the research, elucidating the systematic processes employed to interpret, organize, and derive meaningful insights from the collected data. It outlines the methodologies, techniques, and tools utilized to analyze the gathered information, aiming to uncover patterns, trends, relationships, or associations relevant to the research objectives. This section not only expounds on the specific analytical approaches but also elucidates the reasoning behind their selection and their alignment with the research questions or hypotheses. Through transparent documentation of the analytical procedures, this section contributes to the rigor and credibility of the study's findings, offering a clear understanding of how data was processed and interpreted to draw conclusions. We used a correlation study to look at the bonds between our independent variables. The correlation between malware and ransomware and the regularity of data breaches is 0.389. Data breach consistency is 0.270 larger than big data mitigation presented in figure 1. Linear connections between independent variables are represented by these correlation coefficients. When two variables are positively correlated, it suggests that, as one variable grows, the other tends to increase as well, whereas when two variables are negatively correlated, it suggests that, as one increases, the other tends to decline. Here, we have modest correlations, which point to some interdependence among the critical variables but not severe multicollinearity.

Table 3. Model II, Factors affecting cybersecurity risk: Logistic regression analysis model II

Variable	Coefficient (β)	Odds Ratio	95% CI (Odds Ratio)	p-value
Data Breach Consistency	1.204	3.331	[2.097, 5.288]	<0.001
Malware & Ransomware	0.907	2.477	[1.543, 3.982]	<0.001
Big Data Mitigation	0.491	1.633	[1.102, 2.416]	0.014
Age	-0.032	0.969	[0.930, 1.010]	0.178
Sex (Female)	-0.671	0.511	[0.279, 0.936]	0.032
Income	0.297	1.346	[1.097, 1.651]	0.005
Education Level	0.142	1.153	[0.980, 1.356]	0.085
McFadden's R-squared				0.408

McFadden's R-squared values closer to one indicate a stronger model fit (McFadden, 1974). In Table 3, model II explains around 40.8% of the variation in the binary outcome variable, which reflects concern about cybersecurity threats in accounting investigations. Those who routinely acknowledge the gravity of *data breaches* are more than three times as likely to express strong concern about cybersecurity threats, as shown by a higher coefficient of 1.204 and odds ratio of 3.331. *Malware and ransomware attacks* are often regarded as among the gravest dangers to computer systems. People who give these dangers a lot of thought are almost twice as likely to be very worried about them (coefficient = 0.907, odds ratio = 2.477). The logistic regression results strongly support our first hypothesis.

In line with our second hypothesis, Big Data Mitigation shows a positive impact on reducing cybersecurity concerns, evidenced by its coefficient (β = 0.491) and odds ratio (1.633). This suggests that belief in the efficacy of big data correlates with lowered cybersecurity concerns, thus validating our theoretical proposition. Those who are aware of the benefits of big data technology in cyber security are more inclined to be wary of the threats they pose.

The age variable does not have a significant role in predicting strong concern about cybersecurity threats, with a coefficient of -0.032 and an odds ratio (OR) of 0.969. This research demonstrates that age is not a major predictor of cybersecurity knowledge, even though different older people would have different degrees of awareness. The demographic variable "Sex (Female)" indicates the respondents' gender. Female respondents are almost half as likely as male respondents to report high levels of concern (odds ratio = 0.511; coefficient = -0.671).

'Income' and 'Education Level' stand in for societal determinants of social status. A significant value of 0.297 for "Income" indicates that those with greater income are 1.346 times more likely to report a strong concern.

Although the coefficient for "*Education Level"* is not statistically significant, a positive trend may be inferred. Individuals' access to cybersecurity materials and knowledge may be influenced by socioeconomic factors such as income and level of education. High levels of concern about cybersecurity dangers are positively correlated with both "Income" and "Education Level," albeit the strength of the correlation varies. Access to information and knowledge of cybersecurity risks may be influenced by factors such as income and level of education. However, the importance of these characteristics in predicting concern may differ depending on the setting of the research and the group under investigation.

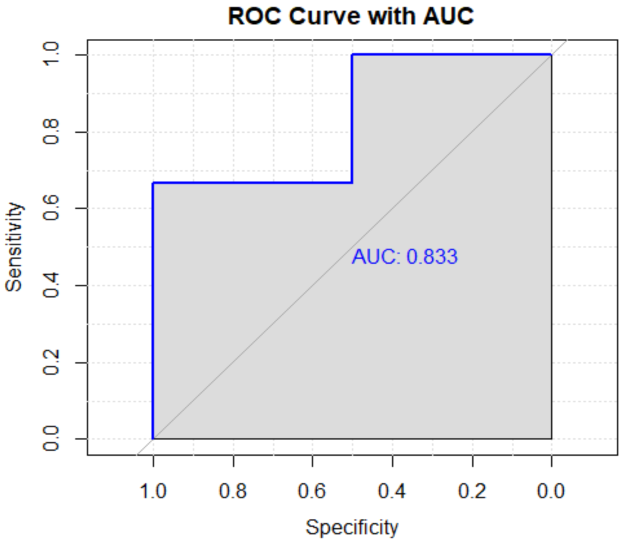

Figure 2. Area under the curve

The AUC is a measure of the model's predictive or discriminatory ability [14]. The model's discriminating ability between concerned people and those who are not about cybersecurity hazards in accounting investigations is shown by an AUC of 0.833 in Figure 2. The model's overall fit, as indicated by McFadden's R-squared value of 0.408 and an AUC value of 0.843, demonstrates moderate to strong predictive power. This lends further credibility to our hypotheses, suggesting that the model effectively captures the essence of how different factors influence cybersecurity concerns among individuals [31].

The empirical results largely confirm our theoretical predictions, validating both of our initial hypotheses. The findings highlight the significant role of individual perceptions, especially regarding data breaches and the mitigating potential of big data technologies, in shaping cybersecurity concerns. The results also highlight the nuanced influence of demographic and socioeconomic factors on these concerns, providing valuable insights for future research and policy-making in the realm of cybersecurity.

In an increasingly digitalized world, the imperatives of cybersecurity are more pressing than ever, both for organizations and individuals. This study's findings, as revealed through logistic regression analysis, provide important insights into the various factors influencing cybersecurity concerns, particularly in the context of accounting investigations. Our results identify Data Breach Consistency as a crucial determinant of heightened cybersecurity concerns. This echoes the findings of Algarni et al. [4] and Klein [17], highlighting the persistent relevance of data breaches as a major cause for concern. High-profile incidents like the SolarWinds intrusion, as discussed by Kshetri [19], have amplified awareness about the vulnerabilities in software supply chains. Similarly, the direct correlation between public reaction to data breaches and cybersecurity apprehensions in accounting, as reported by Saleem and Naveed [33], finds resonance in our findings. The impact of events like the Equifax data leak [15] illustrates the significant influence of data breaches on public perception and concern. This parallels earlier studies that underscore the growing public consciousness and response to data breaches. Notably, recent high-profile data breaches have amplified public sensitivity to these threats, reflecting a shift in perception about the seriousness of cybersecurity in the digital age.

The concern associated with *Malware and Ransomware* is another significant finding of our study. Our results reflect the evolving nature of these risks and their implications for individuals and organizations alike. This aligns with the research by Langlois [20] and Mayer et al. [21], which highlights the growing prevalence and severity of these cyber threats. Reports like Verizon's Data Breach Investigations and the real-world implications seen in the Not Petya ransomware outbreak and the WannaCry ransomware attack from 2017 demonstrate the critical need for effective countermeasures against such threats.

Interestingly, our findings regarding the *Big Data Mitigation* variable suggest that awareness of the benefits of big data technology in cybersecurity leads to increased vigilance against threats. This aligns with the perspectives of Rezaee et al. [32] on the importance of big data analytics in cybersecurity risk management and is exemplified by the practices of financial institutions like JPMorgan Chase, as mentioned by Ramachandran et al. [29] and Wewege et al. [41].

Unlike some previous studies that have suggested varying levels of concern across different age groups, our analysis indicates that age does not significantly impact cybersecurity concern levels. This might hint at a universal recognition of cybersecurity threats irrespective of age, suggesting a more widespread digital literacy than previously assumed. While age did not emerge as a significant predictor in our study. Similarly, previous research by Xu et al. [42] and Dinev and Hart [11] suggests that different age groups may exhibit varied concerns about online privacy. This divergence points to the potential for future research to further explore age-related dynamics in cybersecurity concerns.

The gender-related findings, particularly the lower reported concern among female respondents, offer a unique perspective when compared to existing literature, which often indicates a gender gap in cybersecurity perceptions. This aspect of our findings could imply an evolving landscape in gender dynamics within cybersecurity awareness and education [12; 13; 36]. Our study also sheds light on the role of socioeconomic factors, such as income and education, in shaping cybersecurity concerns as highlighted by Calderon and Gao [8]. The positive correlation of these factors with heightened cybersecurity awareness suggests that access to resources and information plays a crucial role in determining one's level of concern and preparedness against cyber threats.

The insights gained from this research have significant implications for policymakers and educators in the realm of cybersecurity. By understanding the factors that influence public concern, targeted strategies can be developed to enhance awareness and preparedness across different demographic and socioeconomic groups. Future research in this area could explore the evolving nature of cybersecurity threats and their impact on different sectors. Investigations into the efficacy of various mitigation strategies, especially in the context of emerging technologies, could provide valuable insights. Additionally, a deeper dive into the gender dynamics and the role of digital literacy in shaping cybersecurity perceptions would further enrich the discourse in this field. In conclusion, this study not only adds to the existing body of knowledge on cybersecurity concerns but also opens avenues for further research, emphasizing the need for continual adaptation and vigilance in the face of ever-evolving digital threats.

4. Conclusions

This study aimed to unravel the complicated relationship between cybersecurity risks, big data applications, and their impacts on accounting. Through a differential equations-based model, we explored how perceptions of cybersecurity threats evolve and how these perceptions shape strategic responses within organizational contexts. Our findings reveal that the perception of cybersecurity threats, particularly those related to data breaches and malware/ransomware, is influenced by multiple factors. These include trust in technological solutions, demographic variations, and socioeconomic status. The study demonstrated that heightened awareness and knowledge about cybersecurity risks are critical and that confidence in big data technologies can effectively reduce these concerns over time. This underscores the role of technology as a crucial component in comprehensive cybersecurity strategies.

Significantly, the results highlighted disparities in the understanding of cybersecurity issues across different age and gender groups, as well as other demographic categories. This suggests a need for customized cybersecurity education and awareness programs to cater to diverse groups effectively. The impact of socioeconomic factors, such as education level and income, on cybersecurity perceptions further points to the need for widespread and accessible cybersecurity education. These insights support the development of policies that foster a diverse and inclusive cybersecurity environment.

Our study emphasizes the importance of adopting a multifaceted approach to cybersecurity. This approach should consider socioeconomic, demographic, and technological factors. The findings offer a strategic framework for businesses, educational institutions, and policymakers to navigate the challenges of cybersecurity in today's digital world. They advocate for proactive, inclusive, and informed measures to safeguard sensitive data and effectively manage cyber threats.

5. Policy implications: A global perspective

Our research highlights the necessity of comprehensive cybersecurity measures on a global scale. It highlights the importance of integrating cybersecurity education at all levels of educational and professional training. This is essential for building robust defences against cyber threats. The collaboration between public and private sectors emerges as a critical factor, promoting the sharing of intelligence and best practices to strengthen cybersecurity governance.

Investment in cybersecurity research and development is vital for economic resilience and adaptability to technological shifts. Ensuring equitable access to cybersecurity resources and education is crucial, calling for policies that support diverse and inclusive training initiatives. Furthermore, international cooperation is paramount in effectively managing global cybersecurity challenges, requiring joint efforts in knowledge exchange and institutional collaboration.

To conclude, the study provides valuable insights and strategic guidance for managing cybersecurity risks, emphasizing the need for well-rounded and adaptive approaches to safeguarding the digital landscape.

Declaration of competing interest

The author declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] E. Bonsón and M. Bednárová, “Blockchain and its implications for accounting and auditing,” Meditari Account. Res., vol. 27, no. 5, pp. 725–740, 2019.

[2] J. W. Goodell and S. Corbet, “Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack,” Fin. Res. Lett., vol. 51, no. 103329, p. 103329, 2023.

[3] M. Wiguna, K. Aswar, E. Hariyani, M. Sumardjo, and A. Nasir, “Determinants of accrual accounting adoption: The role of organizational culture,” Probl. Perspect. Manag., vol. 21, no. 1, pp. 83–91, 2023.

[4] M. Algarni, V. Thayananthan, and Y. K. Malaiya, “Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems,” Appl. Sci., vol. 11, no. 8, p. 3678, 2021. [Online]. Available: https://doi.org/10.3390/app11083678

[5] Almansoori, M. Al-Emran, and K. Shaalan, “Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories,” Appl. Sci., vol. 13, no. 9, p. 5700, 2023. [Online]. Available: https://doi.org/10.3390/app13095700

[6] R. A. Ariyaluran Habeeb, F. Nasaruddin, A. Gani, I. A. Targio Hashem, E. Ahmed, and M. Imran, “Real-time big data processing for anomaly detection: A Survey,” Int. J. Inf. Manage., vol. 45, pp. 289–307, 2019. [Online]. Available: https://doi.org/10.1016/j.ijinfomgt.2018.08.006

[7] F. Brantly, “Risk and uncertainty can be analyzed in cyberspace,” J. Cybersecurity, vol. 7, no. 1, 2021. [Online]. Available: https://doi.org/10.1093/cybsec/tyab001

[8] T. G. Calderon and L. Gao, “Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees,” Int. J. Audit., vol. 25, no. 1, pp. 24–39, 2021. [Online]. Available: https://doi.org/10.1111/ijau.12209

[9] Y. Connolly and H. Borrion, “Reducing ransomware crime: Analysis of victims’ payment decisions,” Comput. Secur., vol. 119, p. 102760, 2022. [Online]. Available: https://doi.org/10.1016/j.cose.2022.102760

[10] L. Danko, L. Bednář, K. Voštová, and Š. Harušťáková, “Modeling determinants of the Generation Z regional perception on the periphery: To stay or to leave,” Probl. Perspect. Manag. [Online]. Available: http://dx.doi.org/10.21511/ppm.21(2).2023.25

[11] T. Dinev and P. Hart, “Internet privacy concerns and social awareness as determinants of intention to transact,” Int. J. Electron. Commer., vol. 10, no. 2, pp. 7–29, 2005. [Online]. Available: https://doi.org/10.2753/jec1086-4415100201

[12] L. Dudás, “Nudging the public: Relevance, antecedents and the level of public support for behaviorally informed policies,” Budapesti Corvinus Egyetem, 2023. [Online]. Available: https://phd.lib.uni-corvinus.hu/1249/

[13] S. L. Erickson, M. Stone, G. Serdar, and B. Pfeffer, “When crisis victims are not customers: SCCT and the Equifax data breach,” J. Manag. Issues, vol. 35, no. 2, 2023. [Online]. Available: https://www.proquest.com/openview/7e6e210f6a28f256b617b1af9aeb25df/1?pq-origsite=gscholar&cbl=32030

[14] T. Fawcett, “An introduction to ROC analysis,” Pattern Recognit. Lett., vol. 27, no. 8, pp. 861–874, 2006. [Online]. Available: https://doi.org/10.1016/j.patrec.2005.10.010

[15] M. Gracy, B. R. Jeyavadhanam, P. K. Babu, S. H. Karthick, and R. Chandru, “Growing threats of cybersecurity: Protecting yourself in a digital world,” in 2023 Int. Conf. Netw. Commun. (ICNWC), pp. 1-5, IEEE, 2023. [Online]. Available: https://doi.org/10.1109/ICNWC57852.2023.10127398

[16] M. Jedynak, W. Czakon, A. Kuźniarska, and K. Mania, “Digital transformation of organizations: What do we know and where to go next?” J. Org. Change Manag., vol. 34, no. 3, pp. 629–652, 2021. [Online]. Available: https://doi.org/10.1108/jocm-10-2020-0336

[17] D. Klein, “Relying on firewalls? Here’s why you’ll be hacked,” Netw. Secur., no. 1, pp. 9–12, 2021. [Online]. Available: https://doi.org/10.1016/s1353-4858(21)00007-6

[18] Krishna, S. Krishnan, and M. P. Sebastian, “Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: An institutional trust theory perspective,” Inf. Syst. Front., vol. 25, no. 5, pp. 1713–1741, 2023. [Online]. Available: https://doi.org/10.1007/s10796-022-10280-7

[19] N. Kshetri, “Economics of supply chain cyberattacks,” IT Prof., vol. 24, no. 3, pp. 96–100, 2022. [Online]. Available: https://doi.org/10.1109/mitp.2022.3172877

[20] P. Langlois, “2020 Data Breach Investigations Report,” Verizon, 2020. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[21] P. Mayer, C. Schwartz, and M. Volkamer, “On the systematic development and evaluation of password security awareness-raising materials,” in Proc. 34th Annu. Comput. Secur. Appl. Conf., 2018, pp. 733-748. [Online]. Available: https://doi.org/10.1145/3274694.3274747

[22] McFadden, “Conditional logit analysis of qualitative choice behavior,” in Frontiers in Econometrics, Academic Press, 1974, pp. 105-142. ISBN: 0-12-776150-0.

[23] L. McFadden, “Econometric analysis of qualitative response models,” in Handbook of Econometrics, vol. 2, 1984, pp. 1395-1457. [Online]. Available: https://econpapers.repec.org/bookchap/eeeecochp/2-24.htm

[24] T. S. Msomi and S. P. Vilakazi, “Nexus between accounting and information systems and SMEs` operational efficiency in South Africa,” Probl. Perspect. Manag., vol. 21, no. 2, pp. 493-502, 2023. [Online]. Available: http://dx.doi.org/10.21511/ppm.21(2).2023.46

[25] Naseer, H. Naseer, A. Ahmad, S. B. Maynard, and A. Masood Siddiqui, “Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis,” Int. J. Inf. Manage., vol. 59, 102334, 2021. [Online]. Available: https://doi.org/10.1016/j.ijinfomgt.2021.102334

[26] J. M. A. Navia, C. Parra, and J. D. Cedeno, “Digital market orientation and organizational economic performance of service SME,” Probl. Perspect. Manag., vol. 21, no. 2, pp. 400-414

[27] S. Ovcharova, "On the relationship between digitalization and the national smart economy model to achieve strategies of innovative progress," *Futurity Economics&Law*, vol. 2, no. 3, pp. 28–38, 2022. [Online]. Available: https://doi.org/10.57125/FEL.2022.09.25.04

[28] Pawełoszek, N. Kumar, and U. Solanki, "Artificial intelligence, digital technologies and the future of law," *Futurity Economics&Law*, vol. 2, no. 2, pp. 24–33, 2022. [Online]. Available: https://doi.org/10.57125/FEL.2022.06.25.03

[29] N. Ramachandran, S. Suresh, S. Sunitha, V. Suneetha, and N. Tiwari, "Big data in cloud computing - A defense mechanism," in *IoT and AI Technologies for Sustainable Living*, CRC Press, 2022, pp. 219–236.

[30] M. M. Rathore, S. A. Shah, D. Shukla, E. Bentafat, and S. Bakiras, "The role of AI, machine learning, and big data in digital twinning: A systematic literature review, challenges, and opportunities," *IEEE Access: Practical Innovations, Open Solutions*, vol. 9, pp. 32030–32052, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3060863

[31] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2, pp. 100013, 2021. [Online]. Available: https://doi.org/10.1016/j.jjimei.2021.100013

[32] Z. Rezaee, A. Dorestani, and S. Aliabadi, "Application of time series analyses in Big Data: Practical, research, and education implications," *Journal of Emerging Technologies in Accounting*, vol. 15, no. 1, pp. 183–197, 2018. [Online]. Available: https://doi.org/10.2308/jeta-51967

[33] H. Saleem and M. Naveed, "SoK: Anatomy of data breaches," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 4, pp. 153–174, 2020. [Online]. Available: https://doi.org/10.2478/popets-2020-0067

[34] S. Sanetra-Półgrabi and Z. Tetłaka, "Protection of consumer rights in the advertising of the future in conditions of economic instability," *Futurity Economics&Law*, vol. 2, no. 3, pp. 12–18, 2022. [Online]. Available: https://doi.org/10.57125/FEL.2022.09.25.02

[35] S. S. Shah and S. A. H. Shah, "Trust as a determinant of Social Welfare in the Digital Economy," 2023. [Online]. Available: https://doi.org/10.21203/rs.3.rs-3117248/v1

[36] S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed IoT network," *IEEE Access: Practical Innovations, Open Solutions*, vol. 9, pp. 13938–13959, 2021. [Online]. Available: https://doi.org/10.1109/access.2021.3051602

[37] T. N. Thanh, H. P. Thanh, N. H. Van, T. V. T. Thuy, and T. M. Thi, "Factors affecting applied perception and applicability of fair value accounting: The case of construction firms in Vietnam," *Problems and Perspectives in Management*, vol. 21, no. 1, pp. 264-278, 2023. [Online]. Available: http://dx.doi.org/10.21511/ppm.21(1).2023.23

[38] T. Viana, J. Hemns, and J. Paterson, "Towards a multidimensional model to represent human behaviour on online social networks," *International Journal of Cyber-Security and Digital Forensics*, vol. 10, no. 3, pp. 91–99, 2021. [Online]. Available: https://eprints.glos.ac.uk/id/eprint/10736

[39] P. Wang and C. Johnson, "Cybersecurity incident handling: a case study of the Equifax data breach," *Issues in Information Systems*, vol. 19, no. 3, pp. 150-159, 2018. [Online]. Available: https://iacis.org/iis/2018/3_iis_2018_150-159.pdf

[40] P. A. Watters, "Data Analysis," in *Counterintelligence in a Cyber World*, Cham: Springer International Publishing, 2023, pp. 83-95. [Online]. Available: https://doi.org/10.1007/978-3-031-35287-4_8

[41] L. Wewege, J. Lee, and M. C. Thomsett, "Disruptions and digital banking trends," *Journal of Applied Finance and Banking*, vol. 10, no. 6, pp. 15-56, 2020. [Online]. Available: https://www.researchgate.net/publication/343050625_Disruptions_and_Digital_Banking_Trends

[42] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information privacy concerns: Linking individual perceptions with institutional privacy assurances," *Journal of the Association for Information Systems*, vol. 12, no. 12, pp. 798–824, 2011. [Online]. Available: https://doi.org/10.17705/1jais.00281