Oluka, Alexander

Article

Analysing the implications of cybersecurity breaches on firm leadership

Technology audit and production reserves

Provided in Cooperation with:
ZBW OAS

Reference: Oluka, Alexander (2023). Analysing the implications of cybersecurity breaches on firm leadership. In: Technology audit and production reserves 6 (4/74), S. 20 - 26. https://journals.uran.ua/tarp/article/download/286985/284957/673518. doi:10.15587/2706-5448.2023.286985.

ISSN 2664-9969

UDC 338.1
JEL Classification: D29
DOI: 10.15587/2706-5448.2023.286985

Alexander Oluka

ANALYSING THE IMPLICATIONS OF CYBERSECURITY BREACHES ON FIRM LEADERSHIP

The object of this research is the implications of cybersecurity breaches on the leaders of accounting firms in KwaZulu-Natal, South Africa. The research employed a qualitative approach with interviews as the primary data collection technique. The researcher adopted a rigorous analytical framework, utilising different scholarly sources to analyse and explain the intricate experiences of firm leaders. The study revealed that leaders of accounting firms experience psychological, financial, and social consequences due to cybersecurity breaches. It highlights the emotional impact, including anxiety and increased stress. The fear of potential job losses was found to be one issue leaders were worried about after the data breach. The stress from dealing with the aftermath of data breaches affected their family relationships. In addition, leaders experienced low productivity and increased pressure dealing with the media and organization stakeholders and the stigma associated with data breaches. Given the critical role that accounting firms play in the financial ecosystem and the sensitive nature of the data they handle, it is imperative that cybersecurity is prioritised. However, studies have focused on the financial implications of cybersecurity breaches on businesses, but less attention has been paid to the psychological, social, and financial implications of breaches on firm leaders. The findings are significant for academic discourse but also provide leaders with strategies to mitigate the adverse effects of breaches, while also offering a framework for other researchers and practitioners in different regions and sectors to understand and study the phenomenon further.

Keywords: *accounting firm, cybersecurity breaches, emotional impact, management, firm leaders, work stress.*

Received date: 05.09.2023
Accepted date: 09.10.2023
Published date: 23.10.2023

How to cite
Oluka, A. (2023). Analysing the implications of cybersecurity breaches on firm leadership. Technology Audit and Production Reserves, 6 (4 (74)), 20–26. doi: https://doi.org/10.15587/2706-5448.2023.286985

1. Introduction

The rapid advancement of technology has revolutionized the accounting sector, particularly in regions such as KwaZulu-Natal, South Africa. While technological innovations have streamlined accounting processes, they have also introduced new vulnerabilities in the form of cybersecurity breaches. In [1] defined a cybersecurity data breach as the accidental or malicious dissemination of sensitive information. The accounting profession deals with sensitive financial data, making it a prime target for cyber-attacks. For instance, in 2019, Wolters Kluwer, a tax and accounting service provider, fell victim to a ransomware attack. The attack led to an extended outage of its cloud services during a crucial tax filing period. Furthermore, Deloitte was targeted by a sophisticated cyberattack in 2017. The breach compromised confidential data, including client private emails, and affected various branches of the company, including auditing, tax consultancy, and government advisory services.

In KwaZulu-Natal, a region with a growing economy and a growing accounting sector, understanding the implications of cybersecurity breaches on management is crucial. Previous studies have primarily focused on the financial costs of cybersecurity breaches on businesses, but there is a lack of research on the psychological, social, and financial implications on firm leadership, particularly within the accounting sector in South Africa. The management in accounting firms plays a pivotal role in safeguarding client data and ensuring compliance with regulatory standards. A cybersecurity breach can have far-reaching consequences, including reputational damage, legal repercussions, and loss of client trust. The research investigates the implications of cybersecurity breaches on management within accounting firms in KwaZulu-Natal, South Africa. By focusing on this specific region and sector, the study seeks to provide insights into the hidden implications of cybersecurity breaches on managers within accounting firms in KwaZulu-Natal.

The Protection Motivation Theory (PMT) offers a relevant framework for analyzing the implications of cybersecurity breaches on management within accounting firms [2]. PMT delves into the cognitive processes that underpin an individual's or entity's response to perceived threats. The theory delineates two primary appraisal processes: threat appraisal, which assesses the perceived severity and vulnerability of the threat, and coping appraisal, which evaluates the efficacy of the recommended protective behaviour and one's capability to implement it [2]. Therefore, PMT can be instrumental in understanding how management in accounting firms perceives the threats associated with cyber breaches and the subsequent protective

measures they adopt. In [3] suggest that the PMT helps to explain strategies employed by management to navigate the complex landscape of cybersecurity threats, thereby offering insights into the decision-making paradigms that drive protective actions in the face of cyber vulnerabilities.

The aim of the study is to examine the implications of data breaches in firm leaders.

2. Materials and Methods

2.1. Overview of the literature

2.1.1. Psychological implications of cybersecurity breaches. Data breaches have become common in the digital age, and their psychological consequences on individuals are increasingly being recognized. The aftermath of a breach is often characterized by a flurry of activities aimed at damage control, and management is at the forefront of these efforts. The emotional response to data breaches is the feeling of violation and loss of control. In [4] explain that when personal information is compromised, individuals often feel that their privacy has been invaded. The sense of violation can lead to heightened levels of anxiety as individuals worry about the potential misuse of their data [5]. The realization that personal and often sensitive information is in the hands of unauthorized individuals can lead to feelings of helplessness and despair. The uncertainty about the potential consequences and the inability to change what has happened can create a sense of hopelessness, which is a common symptom of depression [6].

Moreover, the psychological effect of data breaches can be so severe that it mirrors the symptoms of post-traumatic stress disorder (PTSD) [6]. Individuals may experience sleep disturbances, flashbacks, and a heightened state of arousal. This can be the case when a data breach involves highly sensitive information such as business secrets, medical records, and personal photographs. Accountants are custodians of very sensitive clients' information like business strategies and secrets, banking details, signed contracts, Wills, physical addresses, emails, and telephone numbers. The constant worry about when and how this information might be used can create a state of hyper-vigilance similar to that experienced by individuals who have undergone a traumatic event [5]. According to a study by [7], managers are subjected to additional stress as they grapple with the immediate technical challenges of containing the breach, communicating with stakeholders, and coordinating response efforts. The high-pressure environment and the worry that the organization's reputation and assets are at stake contribute to the elevated stress levels.

Information is closely linked to the organization's identity in the contemporary business environment. When organization's information is stolen, managers may feel as though they have lost a part of their business. The loss of sensitive information can lead to an identity crisis as individuals struggle to reconcile their sense of self with the violation they have experienced [8]. Furthermore, the fear of potential misuse of stolen data can exacerbate the emotional trauma. For instance, if financial information is stolen, managers may live in constant fear of financial damage. If medical information is compromised, individuals may worry about discrimination and stigmatization. The fear of the unknown can be paralyzing and can affect an individual's ability to function in their daily life [8].

In [9] draw parallels between the psychological impact of cyber-attacks and traditional terrorism. They argue that, like terrorism, cyber-attacks create a climate of fear and uncertainty. For example, a cyber-physical attack on a German steel factory caused the blast furnace essential parameters to become uncontrollable resulting in significant damage that ultimately resulted in the deaths of two employees [10]. The psychological effect is severe when the cyber-attack is perceived as an attack on the community. In such cases, individuals worry about their personal data but also feel a sense of collective violation and insecurity. Moreover, the psychological consequences of data breaches can have ripple effects on social relationships and community dynamics. The stress and anxiety experienced by individuals can strain relationships with family and friends. Additionally, data breaches can erode trust in institutions and systems, leading to decreased social cohesion in the community [11].

2.1.2. Social implications of cybersecurity breaches. Data breaches have social implications that extend beyond the immediate victims to encompass the broader community and society. The stigma associated with being part of an organization that has suffered a data breach can also have social implications for management. There is often a perception that data breaches are the result of negligence, incompetence, and managers may be unfairly judged and stigmatized by their association with the breached organization. This can affect managers' social interactions and relationships, as they may feel judged by their social circles and media. Study by [7] found that a third of managers had to cancel personal plans, 32 % had to work through the night while 27 % had to postpone vacations in the wake of a cybersecurity incident.

Leaders are often seen as the custodians of organizational data, and a breach can be perceived as a failure of leadership. This can lead to a loss of trust and credibility within the organization but also in the wider business community. Leaders may find their professional reputations tarnished, and their ability to secure future employment may be compromised [12]. Additionally, leaders and employees may experience a reluctance to engage in financial transactions such as applying for loans. The concern that their financial information may have been compromised and may be unfairly associated with fraudulent activities can cause hesitation. This can be true for leaders who may be subject to greater scrutiny by financial institutions. The reluctance to engage in normal financial transactions can have an impact on the personal and financial well-being of leaders and employees [12].

Data breaches can erode trust among employees and between employees and leadership. Employees may question the competence and integrity of leaders who were unable to prevent the breach. Similarly, leaders may become suspicious of employees, if internal actors were involved in the breach. The erosion of trust can undermine teamwork and collaboration, which are essential for organizational success [13]. Employees and leaders can find their social interactions and relationships strained within and outside the organization.

2.1.3. Financial implications of cybersecurity breaches. Cybersecurity breaches can affect the professional and personal lives of management and employees. The costs associated with a cybersecurity incident can be substantial. These include the costs of forensic investigations to understand the scope and nature of the breach, the costs of

ISSN 2664-9969

communicating the breach to customers and regulators, and the costs associated with implementing remedial measures [14]. Additionally, there may be business interruption costs if the breach affects the organization's ability to operate normally. Management is often held accountable for these financial losses.

Equifax, a credit reporting company, suffered a cybersecurity breach in 2017 that exposed millions of customers' personal information. The breach had far-reaching consequences; several high-ranking executives, including top management, resigned in the aftermath, and Equifax was subjected to lawsuits and regulatory scrutiny [15]. Similarly, Yahoo experienced data breaches in 2013 and 2014, compromising 3 billion user accounts. The incident had a detrimental effect on Yahoo's stock price and led to the replacement of the CEO and several other executives [16]. Management plays a crucial role in safeguarding the organization's intellectual property and is often held responsible for any failure.

Managers often have to re-prioritize their duties in the aftermath of a data breach. The focus shifts from regular operational tasks to crisis management. This can lead to delays in project timelines and can have a cascading effect on the organization's operations and financial performance. Furthermore, management may face legal liabilities, especially if there is a failure to adhere to data protection laws and industry regulations. Moreover, management is responsible for ensuring that the organization complies with legal requirements, and a breach can expose gaps in compliance. Cybersecurity breaches can lead to lawsuits, fines, and regulatory actions, which can financially impact the organization [14]. Additionally, there is a likelihood that managers may lose their performance bonuses when the organization loses revenue due to lawsuits, fines, and regulatory actions. In [17] elaborate that the loss of intellectual property can have long-term effects on the organization's market position and financial performance.

2.1.4. Implications of cybersecurity breaches on employee morale and turnover. Cybersecurity breaches may affect an organization's internal dynamics regarding employee morale and turnover. The aftermath of a breach creates an environment of uncertainty and stress, which can have detrimental effects on the workforce. The breach can create a sense of insecurity among employees regarding the stability and integrity of the organization [18]. Employees may feel that their personal data and work are at risk, leading to anxiety and a loss of motivation. Moreover, the breach does create an atmosphere of mistrust within the organization, as employees may question the competence of both their peers and leadership in safeguarding sensitive information.

The impact on morale is pronounced if employees feel that the organization did not take adequate measures to prevent the breach and if the response to the breach is perceived as inadequate. The lack of clear communication from leadership regarding the breach and the steps being taken to address it can further exacerbate the decline in employee morale. The decline in morale can, in turn, lead to reduced productivity as demotivated employees are less likely to be engaged and committed to their work [18]. In cases where an employee is found to have contributed to the breach, whether through negligence or malicious intent, they may face disciplinary action [19]. Disciplinary action against employees creates a culture of fear within the organization, as staff worry about being blamed for security incidents. The fear of punitive action can hinder open communication and collaboration, which is essential for an effective cybersecurity posture.

Increased turnover is a natural consequence of declining employee morale [20]. Disillusioned and demotivated employees may seek employment elsewhere after a cyber-attack, perceiving that the organization cannot protect its assets. The loss of skilled employees can further weaken the organization's ability to recover from the breach and have long-term effects on its competitiveness and performance. Furthermore, the financial impact of a cybersecurity breach can lead to cost-cutting measures, including layoffs [21]. The loss of employment affects those laid off but also places additional strain on the remaining employees who may have to take on additional responsibilities. This can lead to burnout and a further decline in morale among the remaining employees.

2.2. Methodology. Qualitative research was conducted using open-ended questions to allow participants to contribute a wider range of ideas. In [22] highlighted that the qualitative research method enables the researcher to engage with participants in the locale where the studied phenomenon occurred, thereby eliminating the need for a controlled environment. Non-probability purposive sampling was employed in the study, enabling a focus on specific individuals – in this instance, leaders of accounting firms.

The strength of purposive sampling lies in its ability to collect data from pertinent participants. When conducting a study, it's crucial to extract a sample from the population that will yield meaningful results [23]. Purposive sampling enables the researcher to choose participants based on their relevance to the research question [24]. The sample for the study comprised thirteen leaders of accounting firms from Durban, KwaZulu-Natal, purposively selected based on their experience in the subject area.

Data were collected via semi-structured in-depth phone interviews, supplemented by secondary data analysis techniques, such as reviewing reports and related literature. This approach allowed the researcher to delve into recurring themes thoroughly. The collected interviews were recorded, transcribed verbatim and then coded. Thematic analysis was the chosen method for identifying key themes in the data with the aid of NVivo software. Before each interview, a consent form was collected from the participant. Ethical approval for the study was granted by Durban University of Technology.

3. Results and Discussion

Word cloud (Fig. 1) provides a visual representation of the frequency of words mentioned, with words like data breach, productivity, stress, and responsibility being prominent, reflecting the participant's views on the implications of data breaches.

3.1. Financial implications. Managers can end up losing their jobs or choose to resign due to the added pressure and stress. Participant *#13* suggests that fallout after a data breach may cause managers to resign or their contracts may be terminated.

«I have heard situations where some people have been forced to resign from their position because there was a data breach... maybe they did not do what they're supposed to do, and this can be traumatising if you are faced with that kind of situation».

Fig. 1. Word cloud

Participant *#9* reckons that managers may lose their jobs after data breach.

«...and you could possibly lose your job».

Participant *#11* indicates that managers worry about the consequences of any investigation after a data breach.

«If this happens, the big worry would be how will that affect you... if it's found that you didn't do the right thing to protect the client's information, you could go to jail or lose your job... this makes you anxious and distressed, and you cannot perform your duties when you are in this kind of state».

Participant *#6* suggests that productivity will be affected due to a lack of access to the system.

«When you're attacked, all your systems go down, which means there is no productivity... then when there's no productivity, you won't be in a position to service your clients therefore, you will be losing money».

Participant *#7* believes that managers may be worried about the future of their jobs especially if there is an investigation after a data breach which impairs their ability to execute their duties.

«I have seen in many cases where once management takes the heat they just resign and go elsewhere... so those are the implications that can actually happen. Just being in that space where you are constantly worrying about these things can also affect you psychologically and it can make you unproductivity».

Managers may decide to step down voluntarily or could be forced to resign due to data breaches. Moreover, managers may be unable to handle the pressure exerted on them and end up resigning. The criticism could come from the media and other stakeholders who may blame the organization's leadership for not doing enough to protect clients' information. In [25] states that «cyber threats have zoomed to the top of chief executives' worry lists for fear a data breach could cost them their jobs and take down their businesses». The fear could be associated with financial and reputation damage caused by data breaches in firms.

3.2. Psychological implications. It will cause tremendous stress on the management as the losses and reputational damage will affect the firm significantly. They would also have to be able to explain the breach to the organization's board and provide alternative solutions and recovery plans. This can further exacerbate stress levels experienced by managers. Participant *#2* suggests that the pressure to get the company back to normality increases stress levels on the firm leadership.

«Number one would be stress... I mean as management you are the face of the organization, and clients would want to know why, how this happened and how you're going to fix it... so definitely stress».

Participant *#4* believes that demand for action against data breaches may cause stress on the firm leadership.

«I know from our board members have been worried if we are ready to deal with cyber security breach because if we lose clients information, we may get sued... and we lose a lot of money out of that so if the breach happens you will be under a lot of stress to explain to the board and maybe law enforcement authority's on how it happened».

Participant *#6* elaborates that the worry about the potential loss of clients due to data breach increases the stress levels of the management.

«When you encounter a cyber-attack or data breach, you will not sleep because you as a leader of that organization has the responsibility to ensure that everything is restored to normalcy... so that comes with a huge amount of stress».

Dealing with the aftermath of a cyberattack can be a very traumatic and stressful experience for management. This may entail responding to queries from the media, employees, government agencies and other stakeholders who would be seeking answers from the organization. Cybercrime has become an increasing worry for business executives as they face increasing pressure from regulators to address cybersecurity threats. In [26] explain that managers may experience anxiety when dealing with data breaches as a result of making certain decisions because of uncertainty regarding the potential outcomes of such choices. In [5] points out that people whose personal data has been compromised can experience anxiety, depression, and post-traumatic stress disorder because of the exposure. Therefore, dealing with the aftermath of a cyberattack has a psychological impact on firms' leadership.

3.3. Social implications. The social implications of data breaches within an organization are profound, affecting personal and professional relationships. Participant *#7* explains that dealing with a data breach can be stressful and even affect your relationship with family and friends.

«You are paid a lot of money so that you make sure these things like this don't happen so, if they do happen you have to take responsibility... so management responsibility now comes into play and that can obviously have a huge strain on your family and your work environment... it can get

ISSN 2664-9969

worse where your family will not be free to go down the shop because of the media coverage of the incident».

The social implications of data breaches are particularly pronounced among employees and leaders. One notable social implication of data breaches within an organization is the strain it places on the personal relationships between managers, employees and their families. According to a study by [27], 76 % of workers reported that a data breach had adversely affected their personal relationships. This can be attributed to the stress and anxiety that managers experience in the aftermath of a data breach, which can spill over into their personal lives. The constant worry about the potential misuse of stolen information and the uncertainty surrounding the security of their data can cause managers to become irritable, withdrawn, and overly anxious, which can strain relationships with family and friends.

3.4. Low productivity. A data breach would definitely have an impact on the productivity of the leadership. The breach will cause disruptions and loss to the firm which is led by the manager. This will cause added pressure as they will try to focus on the breach and dedicate resources and time towards that rather than anything else and this can lead to loss of productivity. Participant *#1* indicates that dealing with a data breach for the first time may be challenging and stressful for the organization's leadership which can affect their productivity.

«If this happens for the first time... you may not know how best to handle this matter and as a human being your level of productivity can be affected and if you are not careful... you are bound to make a lot of mistakes and make things even worse. if you are working in financial reporting, it can affect even the reports that you produce».

Participant *#2* points out that leadership may experience anxiety when dealing with data breaches and this diverts their attention from other duties.

«Anxiety lowers productivity for sure because your mind is so focused now trying to fix the problem».

Participant *#3* highlights that management may shift their attention to getting the company to operate, and they may neglect other duties.

«When a data breach happens in your company, your focus will be finding a way on how to get the company operational therefore, you will not be thinking of anything else other than rebuilding this new system... so definitely, it will affect you in terms of your ability to perform other duties».

Participant *#5* believes managers may not perform at their best when stressed.

«A data breach will make you anxious and distressed, and you cannot perform your duties when you are in this kind of state. I would say productivity would be zero and this can also have an extended impact on your family and friends because you cannot be yourself, especially if an investigation has been instituted».

Process outage and production shutdown caused by a data breach has a psychological impact on a firm's leadership. Firms' leadership may neglect other duties while dealing with a data breach crisis thereby affecting productivity. Their attention could be shifted to restore the system to normality. In addition, external pressure may be exerted on management to have the incidents resolved quicker which could exacerbate the stress levels on management causing them to think irrationally. When confronted with challenging situations, people not only suffer from stress but also experience a decrease in productivity [28]. Individuals tend to react to incidents with stress and may avoid contact with other individuals if they believe they cannot effectively exert control over possible threats [8]. Therefore, the motivation and confidence of the manager may diminish.

3.5. Dealing with the media. The media can also create a negative image of the situation and the firm. Participant *#8* points out that the responsibility of dealing with the media rests on the firm's leadership, which may increase the management's stress and anxiety.

«When a data breach happens it's always the top guys that have to take the fall, so they are the ones that have to manage the flow information, have to deal with the media and have to explain to the staff basically the reason».

The firm's leadership must manage the heightened negative media coverage of the incident, which puts more strain on managers and damages their reputation. Therefore, a good risk communication strategy from the management about data breaches can ease public worry and fear. Shareholders may react differently to the announcement of data breaches depending on the language and tone used in various media sources [29]. Business leaders may be forced to apologize to their clients' and affected parties for the data breach. Moreover, an apology compels the company to publicly acknowledge wrongdoing for the data breach, which may invite legal action and weaken the company's defense in the case of litigation. However, it has been demonstrated that restoring confidence is more challenging when the issue is one of honesty rather than skill [30]. Financial and legal obligations may result from remedial efforts, including compensation.

3.6. Discussion. The study reveals the psychological consequences experienced by management personnel in accounting firms because of cybersecurity breaches. Incidents such as those involving Wolters Kluwer and Deloitte highlight the comprehensive role of management, which extends beyond immediate breach containment. They are saddled with the onerous task of addressing long-term implications, including legal liabilities, reputational erosion, and the arduous task of reinstating client trust. The psychological ramifications on management are severe, manifesting as heightened stress, disrupted personal plans, and the overarching pressure to assuage stakeholders, regulatory entities, and the media. The efficacy with which management navigates these tumultuous situations is fundamental to an organization's post-breach recovery and long-term sustainability.

Moreover, it is paramount for management to champion a forward-thinking approach to cybersecurity. This necessitates the institution of robust technological safeguards, relentless vigilance for potential breaches, and the crafting of comprehensive incident response blueprints. It is equally essential to foster a cybersecurity-conscious ethos within the organization, reinforced by rigorous employee training in security protocols. To remain at the vanguard of cybersecurity practices, management must actively seek collaboration with industry contemporaries, regulatory bodies, and cybersecurity specialists.

The insights drawn from this study are valuable for management in accounting firms, aiding in understanding,

and mitigating the psychological effects of cybersecurity breaches. These findings can inform the creation of training and support systems to assist management during cybersecurity incidents. While the study is based in KwaZulu-Natal, its findings are relevant globally, as the psychological effects on management during cybersecurity breaches are a universal concern. However, to generalize these findings, further research in various cultural and geographical contexts is necessary. The results should be applied considering the study's specific context. Firms should adapt these insights to their unique organizational structures and circumstances, acknowledging the study's geographical limitation.

4. Conclusions

The management within accounting firms is confronted with an array of challenges and responsibilities in the wake of cybersecurity breaches. The incidents highlighted in this paper, such as those involving Wolters Kluwer and Deloitte, demonstrate that management is tasked with the immediate containment and mitigation of breaches but also faces long-term repercussions including legal liabilities, reputational damage, and the restoration of client trust. The psychological effect of data breaches on management is significant as they grapple with stress, altered personal plans, possible job losses and the pressure of addressing the concerns of stakeholders, regulatory bodies, and the media. The ability of management to effectively navigate these challenges is critical to the recovery and sustainability of the organization post-breach.

Furthermore, management must adopt a proactive stance on cybersecurity. This involves the implementation of robust technological safeguards, continuous monitoring for breach detection, and developing of comprehensive incident response plans. Additionally, fostering a culture of cybersecurity awareness within the organization and ensuring that employees are adequately trained in security best practices is essential. Management must also offer psychological counselling services for staff and managers to help them deal with the aftermath of data breaches. Management must also collaborate with industry peers, regulatory bodies, and cybersecurity experts to stay abreast of evolving threats and best practices. Future studies can explore the decision-making processes and strategies employed by management in accounting firms during and after cybersecurity breaches. Additionally, research into the psychological support and resources available to management in the aftermath of cybersecurity breaches could shed light on ways to mitigate the psychological impact on executives and employees.

Conflict of interest

The author declares that he has no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The research was performed without financial support.

Data availability

Data will be made available on reasonable request.

Use of artificial intelligence

The author confirms that he did not use artificial intelligence technologies when creating the current work.

References

1. Romanosky, S., Hoffman, D., Acquisti, A. (2014). Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies, 11 (1),* 74–104. doi: https://doi.org/10.1111/jels.12035
2. Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology, 91 (1),* 93–114. doi: https://doi.org/10.1080/00223980.1975.9915803
3. Floyd, D. L., Prentice-Dunn, S., Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology, 30 (2),* 407–429. doi: https://doi.org/10.1111/j.1559-1816.2000.tb02323.x
4. Durnell, E., Okabe-Miyamoto, K., Howell, R. T., Zizi, M. (2020). Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale. *International Journal of Human–Computer Interaction, 36 (19),* 1834–1848. doi: https://doi.org/10.1080/10447318.2020.1794626
5. Aboujaoude, E. (2019). Protecting privacy to protect mental health: the new ethical imperative. *Journal of Medical Ethics, 45 (9),* 604–607. doi: https://doi.org/10.1136/medethics-2018-105313
6. Kilovaty, I. (2021). Psychological Data Breach Harms. *North Carolina Journal of Law & Technology, 23 (1),* 1–66.
7. *Taking care of corporate security and employee privacy: why cyber-protection is vital for both businesses and their staff* (2020). Kaspersky. Available at: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2020/04/20043942/Kaspersky-2020_Report_Human_angle_FINAL.pdf Last accessed: 04.01.2023
8. Bada, M., Nurse, J. R. (2020). The social and psychological impact of cyberattacks. *Emerging cyber threats and cognitive vulnerabilities.* Academic Press, 73–92. doi: https://doi.org/10.1016/b978-0-12-816203-3.00004-6
9. Gross, M. L., Canetti, D., Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists, 72 (5),* 284–291. doi: https://doi.org/10.1080/00963402.2016.1216502
10. Padmanabhan, A., Zhang, J. (2018). Cybersecurity risks and mitigation strategies in additive manufacturing. *Progress in Additive Manufacturing, 3 (1-2),* 87–93. doi: https://doi.org/10.1007/s40964-017-0036-9
11. Bachura, E., Valecha, R., Chen, R., Rao, H. R. (2022). The OPM Data Breach: An Investigation of Shared Emotional Reactions on Twitter. *MIS Quarterly, 46 (2),* 881–910. doi: https://doi.org/10.25300/misq/2022/15596
12. Solove, D. J., Citron, D. K. (2018). Risk and Anxiety: A Theory of Data Breach Harms. *96 Texas Law Review.* doi: https://doi.org/10.2139/ssrn.2885638
13. Hecht, E. M., Wang, S. S., Fowler, K., Chernyak, V., Fung, A., Zafar, H. M. (2023). Building Effective Teams in the Real World From Traps to Triumph. *Journal of the American College of Radiology, 20 (3),* 377–384. doi: https://doi.org/10.1016/j.jacr.2022.12.009
14. Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security, 68,* 130–144. doi: https://doi.org/10.1016/j.cose.2017.04.010
15. Reuters Staff. (2017). *Lawsuits against Equifax pile up after massive data breach.* Available at: https://www.reuters.com/article/us-equifax-cyber-lawsuits-idUSKCN1BM2E3 Last accessed: 14.10.2023
16. Brumfield, C. (2019). *Equifax's data breach disaster: Will it change executive attitudes toward security?* Available at: https://www.csoonline.com/article/567545/equifax-s-billion-dollar-data-breach-disaster-will-it-change-executive-attitudes-toward-security.html#:~:text=Equifax%27s%202017%20breach%20will%20cost,Topics Last accessed: 14.10.2023
17. La Torre, M., Dumay, J., Rea, M. A. (2018). Breaching intellectual capital: critical reflections on Big Data security. *Meditari Accountancy Research, 26 (3),* 463–482. doi: https://doi.org/10.1108/medar-06-2017-0154

ISSN 2664-9969

18. Schaefer, T., Brown, B., Graessle, F., Salzsieder, L. (2017). Cybersecurity: common risks: a dynamic set of internal and external threats includes loss of data and revenue, sabotage at the hands of current or former employees, and a PR nightmare. *Strategic Finance, 99 (5),* 54–62.
19. *Why Do People Make Mistakes That Compromise Cybersecurity?* (2020). Tessian. Available at: https://www.tessian.com/resources/psychology-of-human-error-2022/ Last accessed: 06.01.2022
20. Ronen, S., Donia, M. B. L. (2020). Stifling My Fire: The Impact of Abusive Supervision on Employees' Motivation and Ensuing Outcomes at Work. *Revista de Psicología Del Trabajo y de Las Organizaciones, 36 (3),* 205–214. doi: https://doi.org/10.5093/jwop2020a20
21. *From data boom to data doom: the risks and rewards of protecting personal data* (2018). Kaspersky. Available at: https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_Lab_Business%20in%20a%20data%20boom.pdf Last accessed: 07.06.2023
22. Creswell, J. W., Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches.* Thousand Oaks: Sage publications.
23. Bryman, A., Bell, E. (2011). *Business research methods.* Oxford: Oxford University Press.
24. Gray, P. S., Williamson, J. B., Karp, D. A., Dalphin, J. R. (2007). *The research imagination: An introduction to qualitative and quantitative methods.* Cambridge University Press. doi: https://doi.org/10.1017/cbo9780511819391
25. Fuhrmans, V. (2017). New worry for CEOs: A career-ending cyberattack. *Wall Street Journal.* Available at: https://www.wsj.com/articles/cybersecurity-tops-priority-list-for-ceos-after-string-of-high-profile-hacks-1507821018 Last accessed: 07.10.2022
26. Nurse, J. R. C., Creese, S., De Roure, D. (2017). Security Risk Assessment in Internet of Things Systems. *IT Professional, 19 (5),* 20–26. doi: https://doi.org/10.1109/mitp.2017.3680959
27. Futuramo. (2023). *How Can a Business Data Breach Affect Employees.* Available at: https://futuramo.com/blog/how-can-a-business-data-breach-affect-employees/ Last accessed: 13.10.2023
28. Schlackl, F., Link, N., Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management, 59 (4),* 103638. doi: https://doi.org/10.1016/j.im.2022.103638
29. Banker, R. D., Feng, C. (Qian). (2019). The Impact of Information Security Breach Incidents on CIO Turnover. *Journal of Information Systems, 33 (3),* 309–329. doi: https://doi.org/10.2308/isys-52532
30. Ferrin, D. L., Cooper, C. D., Dirks, K. T., Kim, P. H. (2018). Heads will roll! Routes to effective trust repair in the aftermath of a CEO transgression. *Journal of Trust Research, 8 (1),* 7–30. doi: https://doi.org/10.1080/21515581.2017.1419877

Alexander Oluka, *PhD, Department of Entrepreneurial and Management Studies, Durban University of Technology, Durban, South Africa, e-mail: olukaam@gmail.com, ORCID: https://orcid.org/0000-0001-7632-1490*