Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 16

February 2024

University of Johannesburg Institutional Repository Cybersecurity Output: 2015-2021 Interdisciplinary Study

Mancha J. Sekgololo
University of Johannesburg, manchajohanness@uj.ac.za

Recommended Citation
Sekgololo, Mancha J. (2024) "University of Johannesburg Institutional Repository Cybersecurity Output: 2015-2021 Interdisciplinary Study," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 16.
DOI: https://doi.org/10.62915/2472-2707.1161
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/16

University of Johannesburg Institutional Repository Cybersecurity Output: 2015-2021 Interdisciplinary Study

Abstract

This study examines cybersecurity awareness in universities by analyzing related research output across different disciplines at the University of Johannesburg. The diffusion of innovation theory is used in this study as a theoretical framework to explain how cybersecurity awareness diffuses across disciplines. The University of Johannesburg Institutional Repository database was the data source for this study. Variations in cybersecurity keyword searches and topic modeling techniques were used to identify the frequency and distribution of research output across different disciplines. The study reveals that cybersecurity awareness has diffused across various disciplines, including non-computer science disciplines such as business, accounting, and social sciences. However, there are significant differences in cybersecurity awareness across academic disciplines, highlighting the need for targeted efforts to promote cybersecurity awareness in underrepresented academic disciplines and for intra and interdisciplinary collaboration.

Keywords

Cybersecurity Awareness, Diffusion of Innovation, Interdisciplinary Collaboration, Research Output, University Disciplines.

Cover Page Footnote

I would like to acknowledge Mutali Lithole for her stellar role in cleaning up the data collected from the UJIR database. her support, as the UJIR Specialist were invaluable.

University of Johannesburg Institutional Repository Cybersecurity Output: 2015-2021 Interdisciplinary Study

Mancha J. Sekgololo
Department of Politics and International Relations
University of Johannesburg
Johannesburg, South Africa
manchajohanness@uj.ac.za
0000000268982018

Abstract: This study examines cybersecurity awareness in universities by analyzing related research output across different disciplines at the University of Johannesburg. The diffusion of innovation theory is used in this study as a theoretical framework to explain how cybersecurity awareness diffuses across disciplines. The University of Johannesburg Institutional Repository database was the data source for this study. Variations in cybersecurity keyword searches and topic modeling techniques were used to identify the frequency and distribution of research output across different disciplines. The study reveals that cybersecurity awareness has diffused across various disciplines, including non-computer science disciplines such as business, accounting, and social sciences. However, there are significant differences in cybersecurity awareness across academic disciplines, highlighting the need for targeted efforts to promote cybersecurity awareness in underrepresented academic disciplines and for intra and interdisciplinary collaboration.

Keywords: CSA, DoI, interdisciplinary collaboration, research output, university disciplines.

I. INTRODUCTION

Cybersecurity, the safekeeping of digital assets, is a pressing concern in today's digitally wired society [1]. According to various metrics [2], South Africa will overtake Nigeria as Africa's cybercrime-leading hub by 2023. According to [3], the risk of cyberattacks and data breaches is becoming more prevalent and sophisticated. The 2017 Master Deeds data leak is one of the most significant data breaches to affect South Africa [4]. Initially estimated to comprise 30 million pieces of personally identifiable information (identification, physical addresses, among others) [4]. However, the lack of cybersecurity awareness (CSA) has made the data openly accessible on an open web server since 2014 [4]. As noted by [5] and [6], cognitive dissonance, a concept often exploited by cybercriminals, occurs when individuals behave in a manner that suggests they possess knowledge, yet their actions contradict what they know. Cybercriminals also rely on compliance fatigue or what [7] termed "security fatigue", hoping that users neglect or disregard security measures and precautions. Such grave security oversight underscores the need for constant CSA exposure.

Universities have a bearing on addressing the knowledge-action disjuncture by training the next generation of cybersecurity professionals [8]. The Cybercrime Act 19 of 2020, South Africa's digital criminal procedure law, in Section 55C, says;

> In cooperation with any institution of higher learning in the Republic or elsewhere, develop and implement accredited training programmes for members of the SAPS primarily involved with the detection, prevention and investigation of cybercrimes [9].

Additionally, the [10], South Africa's cybersecurity framework policy in Section 12.2C calls for the: "development of a cybersecurity research and development agenda and enhancement of Cybersecurity research within South African Universities, industry and the Department of Science and Technology." Thus, there is a recognizable intersection between academia and government on CSA's diffusion. However, suppose the Cybercrime Act and National Cybersecurity Policy Framework (NCPF) assertions are to be tangible. In that case, all stakeholders need better insights into the level of CSA across different universities and disciplines. However, if the [9] and [10] assertions are to be tangible, the level of CSA across different universities and disciplines beckons better insight. In this context, this study investigates the level of CSA within the University of Johannesburg between 2015 and 2021.

Roger's diffusion of innovation (DoI) appealed to this study in explaining how CSA spread and gained traction over time [11]. The DoI further posits that the diffusion of ideas, such as CSA, is influenced by various factors, including the characteristics of the invention, communication channels, and social system [11]. By applying the DoI to the context of CSA in universities, this study aims to gain insights into the factors that ease or hinder the diffusion of CSA across disciplines. [11] and [12]. In applying the DoI to the context of CSA in universities, the study aims to understand the factors that ease or hinder the diffusion of the CSA across disciplines. The study used the University of Johannesburg Institutional Repository (UJIR) database of theses, dissertations, and journal articles as the data source. The analysis involved keyword searches and topic modeling techniques in identifying the frequency and distribution of the CSA output across different disciplines. Ultimately, this study contributes to the literature on CSA diffusion and provides a foundation for future research in this field. The study hypothesizes that computer science students demonstrate a higher CSA than non-computer science students (NCD). This study hypothesizes that computer science students demonstrate a higher CSA than NCD students.

Section II provides an overview of the literature review, indicating the current knowledge of CSA in South Africa and the gap justifying this study. Section III describes the methodology employed in this study. The penultimate section, IV, encapsulates and discusses the findings of this study. Ultimately, Section V unveils the conclusion, recommendation, study's limitations and future research.

II. LITERATURE REVIEW

A. Diffusion of Innovation

The study is guided by the foundational theory of DoI, which draws on Rogers' work [11]. The DoI theory, which has found application in diverse domains such as healthcare, marketing, and technology, provides a framework for comprehending the acceptance and dissemination of new concepts, products, or technologies [11]. The diffusion process is a model that explains how new ideas, products, or technologies spread through a population. It comprises five stages [11]:

1. The innovation stage involves the introduction of a new idea, product, or technology, which is first adopted by innovators, who are typically risk-takers and willing to try new things.
2. Early adopters are the second group of people to adopt innovation; they tend to be opinion leaders, respected by their peers, often seeking advice, and willing to take risks; however, early adopters are more cautious than innovators.
3. The early majority, which is the third group of people to adopt the innovation, is made up of individuals who are more skeptical and require evidence that the innovation works before they adopt it. Early majority are also more likely to seek information and advice from others before making a decision.
4. The late majority is the fourth group of people to adopt innovation, consisting of people who are even more skeptical than the early majority and tend to adopt innovation only when it has become the norm.
5. Laggards refer to the last group of people who adopt an innovation, characterized by their strong resistance to change and tendency to maintain the status quo [11].

The diffusion process is influenced by five critical factors: innovation, communication channels, time, social system, and adopter categories [11] and [33]. The concept of CSA is dynamic and evolving, and as such, the relevance of the DoI theory has become increasingly significant. The DoI also considers factors such as relative advantages, compatibility, complexity, trialability, and observability of the innovation for its success or lack thereof [33].

By applying the DoI framework to CSA, this study identifies factors that either facilitate or hinder the diffusion of CSA across various disciplines within universities [11]. The DoI framework illuminates nuanced stages of the diffusion process beyond the broad categories of adopters, acknowledging that the characteristics of early and late adopters vary significantly. The adoption of CSA is not a one-size-fits-all process, and it requires a tailored approach that considers the account of the unique characteristics of each adopter category [11]. By having insights into factors that influence the diffusion of CSA, universities can develop effective strategies to promote and ensure that CSA is integrated into their academic programs.

The DoI theory was first proposed by Everett Rogers in 1962. Since its inception, DoI has been widely implemented across various fields, including healthcare, marketing, and technology. The theory presents an explanation of how new ideas, products, or technologies gain acceptance and spread over time [11]. Five key factors that influence the diffusion process are innovation, communication channels, time, social system, and adopter categories [12]. With time, DoI has evolved to encompass a range of sub-theories, including the perceived attributes theory, social network theory, and innovation-decision process theory. These sub-theories offer comprehensive insights into the diffusion process and the factors that impact it. In the context of CSA, a relatively new and continuously evolving concept, the DoI theory is incredibly relevant. Researchers can use DoI to identify the factors that facilitate or impede the diffusion of CSA across various disciplines, allowing them to design awareness campaigns tailored to the needs and characteristics of different adopter categories.

B. Cybersecurity Landscape in South Africa

South Africa's cybersecurity landscape presents unique challenges [13]. With the growth of internet connectivity and digital services, the country has witnessed an escalation in cyber threats. Cyberattacks have surged globally since COVID-19 [14], causing financial damage across various sectors in South Africa. The financial sector, government institutions, and critical infrastructure are particularly vulnerable to cyber threats [15]. For example, in July 2021, Transnet, the South African state-owned logistics company, was attacked through ransomware [16]. Transnet could not operate at its maximum capacity, "increasing logistical congestion" to domestic and international supply chain bottlenecks [14]. There is a growing concern about the South African general population and their understanding of cybersecurity risks [18]. Numerous studies suggest that the low CSA in South Africa is tied to the need for more independent use

of digital technologies [17]. For example, studies have shown that many South African students did not possess a personal laptop, particularly during the peak of the COVID-19 pandemic [17]. These studies indicate that despite efforts to combat cybercrime, there are still unexplored approaches that could effectively address the rise in cyberattacks, with CSA diffusion being one of the methods.

C. Existing Research on CSA

Several studies assessed CSA in South Africa. These studies often focus on specific sectors or demographics. For example, research conducted among university students reveals a need for basic CSA principles [18]. According to [19], who investigated how academic institutions communicate CSA-related information to students. The survey focused on students enrolled in computer security at the Central University of Technology Free State [19]. The recommendation suggests that because students typically have institutional email addresses and student portals, it is essential to diffuse CSA through regular posters and relevant content [19]. Academic institutions are responsible for consistently communicating valuable CSA materials to students [11] to foster awareness. This can be achieved through appropriate communication channels and mediums accessible to students, such as Facebook [11], where 98% of the participants indicated Facebook as their preferred communication medium [19].

In another student-oriented investigation, [20] examined the CSA of South African students. Their questionnaire-led research focused on three private universities in KwaZulu-Natal Province and used an exploratory approach with non-probability sampling. The final analysis revealed that students experienced cognitive dissonance regarding cybercrime, especially phishing. Interestingly, despite this lack of understanding, most students paradoxically expressed confidence in identifying a phishing email. Equally, [21] found that most South African university students need more awareness of ethics when using technology, leading to uninformed decisions. In another CSA output, [18] advocated for enhanced CSA for information technology professionals in South Africa. This approach by [18] fosters a secure culture and improves system development security. It is evident from previous scholarly research that emphasizing CSA within the IT community has been a preferred strategy to mitigate cybersecurity incidents in South Africa.

Accordingly, [22] conducted CSA research in HLIs in accordance with the thesis of the current study. The results indicated that (i) computer science students had a better CSA score than students of non-computer science academic disciplines. Results indicated that (i) computer science students had a better CSA score than students of NCD academic disciplines. In other words, computer science education positively influenced CSA (ii). Their study showed that while women displayed low CSA in both groups, CSA improved for women in computer science than those in NCD academic disciplines [22]. Therefore, the observation is not that women possess lower levels of CSA but that women studying computer science have greater access to CSA information. This enables computer science students to navigate cyberspace more securely than their counterparts in the NCD disciplines [22]. This observation suggests that computer science students tend to have higher CSA levels because of their proximity to cybersecurity education. This, alternatively, implies a need for more frequent CSA training in NCD academic disciplines, as emphasized by [23], analogous to the need for constant security software updates [4].

CSA at HLIs can be successful if a prescribed framework is introduced. The research by [22] raised the need for targeted CSA at HLIs. In their study, [24] proposed a CSA framework to enhance graduates' security knowledge in academic institutions. The framework encompasses various elements to improve cybersecurity education’s integration, delivery, and assessment across diverse disciplines and majors, fostering heightened awareness among future university graduates. They recommend establishing a CSA unit within the institution. This could be a dedicated Unit with formal funding or a specialized unit within the teaching and learning center commonly found in universities to accelerate CSA [24]. Another approach is to train select faculty members to provide CSA services to other academic departments.

Another article [25] investigated the state of cybersecurity in South Africa, highlighting the growing concern about cyber threats and the vulnerabilities faced by the country. The author emphasizes the need for increased CSA and solid legislative measures to protect against cybercrime. The lack of CSA in South Africa is of significant concern to the author. The author recommends the establishment of diverse professional and academic institutes to deliver hands-on educational services to society through research-led activities to ensure that South Africa is resilient to growing cyber threats [25]. The emphasis is on networking and stakeholder collaboration to diffuse CSA broadly. In addition, the author highlights the importance of establishing police-oriented learning centers where citizens can be educated on the dangers of cybercrime [25].

D. Factors Affecting CSA

Understanding the factors that influence CSA is crucial for developing targeted interventions. Studies in other polities suggest that factors such as education level, technical expertise, and organizational culture significantly shape CSA [11].

However, it is essential to investigate whether these factors hold in South Africa. Similarly, studies of small and medium-sized enterprises (SMEs) highlight the need to understand CSA [23]. In their qualitative study, [23] interviewed 15 SMEs in South Africa. Findings revealed that SMEs demonstrate the cognitive dissonance-CSA nexus because of their first-hand experience as cyberattack victims. Participants identified the main challenges in implementing CSA programs as budget and time constraints [23]. Additionally, despite some SMEs having cybersecurity policies, they need to be regularly updated or enforced, highlighting potential gaps in their effectiveness and cognitive dissonance [6], [23]. The author [26] concurs with [23]; the former investigation interviewed 20 SMEs using semi-structured interviews in South Africa. The findings indicated challenges for SMEs needing more NCPF awareness, resource constraints, and the CSA-profit nexus [26]. The CSA-profit nexus implies that SMEs still need to see the link between CSA and profit [23]. Thus, CSA is treated by SMEs as an afterthought [23]. In this context, [19] postulates that more CSA is needed for industry-ready students. They suggest, in accordance with [10], that the industry's CSA is linked to HLI's efforts [19].

In their study, [27] investigated the disconnect between the level of internet penetration in South Africa and the county's security efforts. Several factors hinder the diffusion of CSA in South Africa, such as inadequate government accountability, limited resources, ineffective stakeholder management [27], insufficient regulation, scarcity of skilled human resources, lack of research and development, and insufficient monitoring and evaluation [11]. Furthermore, socio-cultural and economic factors may also impact CSA in South Africa [11]. For example, language diversity and socioeconomic disparities can affect the accessibility of CSA resources and training programs [11], [27].

E. Promoting CSA: Policy Perspective

The South African government recognized the importance of cybersecurity and established initiatives such as the [10]. Section 6.3.4 calls for CSA campaigns [10]. In full realization of [10], the South African government established the Cybersecurity Hub (CSHub). CSHub aims to "increase security awareness for citizens through disseminating various artefacts" [28]. However, the effectiveness of these initiatives in promoting CSA best practices requires further evaluation. Collaboration among government, academia, industry, and civil society is crucial for promoting CSA [10]. Partnerships can facilitate knowledge sharing, capacity building, and the development of tailored cybersecurity training programs [25]. Thus, public awareness campaigns, educational initiatives in schools and universities, and the integration of cybersecurity into curricula are necessary to ensure a cyber-resilient future workforce [10] and [19].

While research has been conducted on specific sectors and target groups, there is a need for comprehensive national-level studies to assess CSA across different industries, organizations, and demographics. Factors influencing CSA, such as education, technical expertise, organizational culture, and contextual factors, require further investigation. Promoting CSA in South Africa requires collaborative efforts among the government, academia, industry, and civil society, including public awareness campaigns, educational initiatives, and partnerships [10]. CSA in South Africa has primarily focused on student behavior in cyberspace [18], [20], [21] and institutional CSA engagement [19]. This approach needs to pay more attention to the diffusion of CSA through research outputs. These studies show that the diffusion of CSA can be achieved in multiple ways. While many studies [20] and [21] have traditionally assessed students' knowledge on topics such as phishing, a notable gap exists in exploring students' and universities' CSA through research outputs. Collectively, these investigations indicate that CSA is disseminated through various means. Thus, using university research output is a compelling method for evaluating the CSA diffusion level [10]. In this context, the current study addresses the following gaps: (i) the need for scholarly investigation on CSA-related research outputs by South African universities; (ii) the need for comparative analysis of the CSA output between computer science and NCD academic disciplines on a longitudinal basis; and (iii) insufficient research on how CSA diffuses within a university, including the channels and actors involved.

III. METHODOLOGY

The study followed a data collection approach using desktop research gathered from the UJIR database between February 2023 and August 2023. UJIR is an open source that collects and

Table 1: Items Searched through the UJIR

Source	Description	Applicability
Books	Aggregate outputs written by a student, researcher, or lecturer associated with the University of Johannesburg	It is not applicable in this study with 0 hits.
Chapter in the Book	Aggregate outputs written by a student, researcher, or lecturer associated with the University of Johannesburg	It is not applicable in this study with 0 hits.
Conference Proceedings	Aggregate outputs presented (published) by a student, researcher, or lecturer associated with the University of Johannesburg.	Providing 5,88% (n=1) of total outputs; individually, inter or intra-collaboratively
Journal Articles	This could be written by a student, researcher, or lecturer associated with the University of Johannesburg	Providing over 17.64% (n=3) of total outputs) individually, inter, or intra-collaboratively.
Theses	Aggregate outputs by Master's degree students who completed their studies.	Providing 58.82%% (n=10) of total outputs). Thus, it excludes researchers and lecturers.
Dissertations	Aggregate outputs by doctoral candidates who have completed their dissertations.	Providing 17.64% (n=3) of total outputs). Thus, it excludes researchers and lecturers.

stores research outputs such as theses, dissertations, journal articles, books, and book chapters by individuals affiliated with the University of Johannesburg. According to [11], CSA, which refers to knowledge about cybercrime, should permeate higher learning institutions (HLIs). This aligns with the DoI's emphasis on information channels and communication [11]. According to [11], DoI emphasizes the role of communication channels [19], adopter categories, and innovation attributes. These concepts were applied to the current study by examining communication channels (e.g., journal articles, theses), adopter categories (e.g., students, departments), and innovation attributes (e.g., relevance, novelty) of CSA research [11].

The study used keyword searches and topic modeling techniques to identify the frequency and distribution of CSA research output across different disciplines. Network analysis was used to uncover patterns of interdisciplinary collaboration, which is central to the DoI's concept of communication channels [11]. Network analysis, according to [30], is a field of study that focuses on relationships and interactions between individuals or groups. Network analysis seeks insights on how relationships shape the behavior and outcomes of individuals and the groups to which they belong. The UJIR underwent a search with the associated terms "cybersecurity", "cyber security", and "cyber-security" parameters that filtered outputs (n=151) that merely mention any of those three terms as an incidental remark. From the focus of this study, the CSA could not have been effectively communicated in such studies[11]. Thus, it became essential to focus on outputs that provide a comprehensive and detailed discussion on CSA promotion. To eliminate these outputs, the study focused on those outputs that substantively (in methodology, literature review and empirical chapters) discussed cybersecurity, resulting in only 17 relevant CSA outputs with "cybersecurity" in their titles. The final outputs chosen for this study are categorized in Table 1 and 2. Microsoft Excel software presented the data through graphs and figures. With the methodology described, the preceding section, IV, accounts for the results of this study.

IV. RESULTS

A. CSA Research outputs: 2015-2021

Universities are pivotal in spreading novel concepts and innovations [29]. The spread of novel concepts is accomplished through academic instruction, research endeavors, and external engagements with society, industry, and other key stakeholders [11]. This study examines how CSA diffuses throughout the University of Johannesburg, focusing on the impact of CSA-centred research. In this context, Table 2 illustrates that the conference proceedings produced one output in 2019, accounting for 20% of the total research outputs for that year. Meanwhile, three journal articles were published, with an equal distribution of 33.3% for 2019, 2020, and 2021.

Table 2: CSA Research Outputs (UJIR) 2015-2021

	Book	Chapter in the Book	Conference Proceedings	Journal Articles	Thesis	Dissertations
2015					2	
2016						
2017						
2018						2
2019			1	1	2	1
2020				1		
2021				1	6	
Total Output	0	0	1	3	10	3

Additionally, two CSA outputs were produced both in 2015 and 2019 and six in 2021. The significant increase of 200% from two in 2019 to six in 2021 can be attributed to the COVID-19 pandemic. Ultimately, the increase in CSA is because of the shift towards remote work, online communication, and digital interaction, which has increased the importance of cybersecurity due to the higher reliance on digital platforms [17]. As a result, there has been a rise in research interest in the field, leading to a surge in theses on cybersecurity in 2021. Table 2 provides valuable insights into the distribution and growth of research outputs related to CSA diffusion. This study highlights the potential impact of external factors, such as the COVID-19 pandemic, on research trends in this domain and, thus, the diffusion of CSA [11]. Equally, the government can affect the research trajectory if it outlines and funds university priorities [11].

Table 1 highlights the presence of just three doctoral-level dissertations between 2018 and 2019, which, in contrast to the 2021 thesis, remain unaffected by the impact of COVID-19. The outputs outside COVID-19 restrain underscores a strong and sustained interest in CSA at the University of Johannesburg, regardless of external factors [11]. Sub-section B provides an overview of the CSA research output categorized by type to accommodate differences in CSA production led by students against the inclusivity of all the University of Johannesburg associates.

.

B. Research output by type

The research output from the University of Johannesburg related to CSA diffusion between 2015 and 2021 takes a holistic approach. The CSA output predominantly concentrated on four categories: Conference proceedings, journal articles, theses, and dissertations. Each category contributes differently to the overall CSA diffusion [11]. Conference proceedings, as illustrated in Figure 1, at 5.88% (n=1), represent a modest research output. Thus, the University of Johannesburg has actively shared its findings and insights with a larger audience through conference platforms. Although the contribution is comparatively small, it demonstrates ongoing involvement in academic discourse and CSA diffusion [11]. However, there is a need to improve CSA diffusion through conference proceedings, as this category has been dormant since 2019. Therefore, there exists an opportunity for the University of Johannesburg and its various departments to arrange a CSA conference, potentially leading to publications. This initiative can expedite the diffusion of CSA knowledge through the conference proceedings avenue [11].

Journal articles, at 17.64% (n=3), constitute a notable proportion of the research output, accounting for a commitment to in-depth analysis and publication in established peer-reviewed academic journals. The consistent distribution of these articles between 2019 and 2021 underscores a sustained effort to contribute to scholarly discussions on CSA diffusion [11]. Only one (in 2020) journal article is noted for its lead author as a student. Thus, students have an opportunity to tap into the journal article stream to increase their CSA engagement within the top-tier knowledge ecosystem.

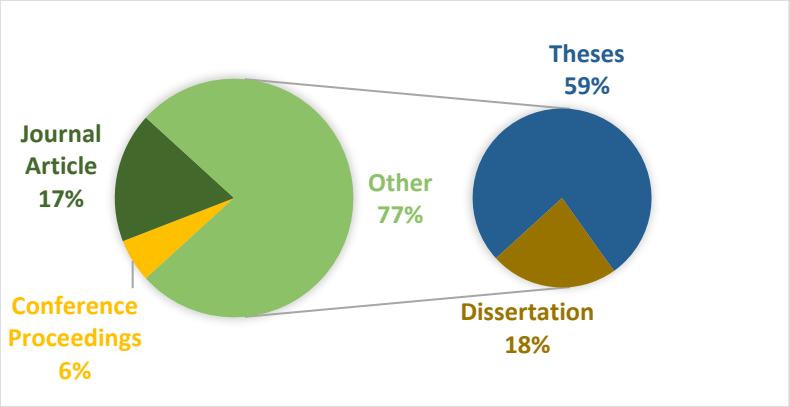

Figure 1: CSA UJ Research Total Output (%), 2015-2021

Dissertations constitute 17.64% (n=3) of the research output, emphasizing the University of Johannesburg's commitment to conducting thorough research. Although this percentage is modest, it demonstrates a proactive approach to investigating specific aspects of CSA diffusion in depth. However, the presence of just three dissertations also indicates the potential for growth in the production of cybersecurity experts. Given this observation, fostering doctoral studies in cybersecurity could be a strategic step. Doctoral programs often yield experts in the field. Thus, the limited number of three outputs provides an opportunity for the University of Johannesburg and its departments to advocate and facilitate more doctoral research in CSA. This strategy will likely result in an enhanced CSA landscape and a more knowledgeable cohort of individuals adept at CSA diffusion [11].

The emphasis on theses as the leading contributor, with 58.82% (n=10), highlights the University of Johannesburg's commitment to nurturing student involvement in CSA research. The distribution across various years (2015, 2019 and 2021) highlights a growing interest. It also indicates that students recognize the need to become Masters in CSA as they probe multiple ways to alleviate the debilitating South African CSA situation [11]. Thesis and dissertation studies are independent, from title conception to execution. Ultimately, this study finds that the exclusive student category (thesis [59%] and dissertations [18%]) accounts for 77% (n=13) of all CSA outputs. The student's cohort is followed by the category inclusive of students (books, chapters in a book, journal articles, conference proceedings) and other University of Johannesburg associates at 23%.

The observation from the analysis of theses and dissertations implies that CSA diffusion occurs between students and their supervisors. This observation highlights a significant aspect of CSA research: each research output, whether a thesis or a dissertation, possesses a ripple effect. To begin with, when a student conducts CSA research under the guidance of their supervisor, the knowledge and awareness cultivated during the research process are shared and transferred between the student and supervisor [11]. This collaborative effort ensures that both parties are well-versed in CSA, thus contributing to a mutual increase in CSA awareness. In addition, as students progresses and potentially continue their career in academia or industry, they carry the CSA knowledge forward [18]. Students become ambassadors of the CSA, disseminating their findings and insights to a broader audience [18]. Thus, diffusion can take various forms, including publications, presentations, and practical applications in the cybersecurity field [11]. Sub-section C unveils the CSA output by year to reveal the oscillation of outputs.

C. CSA Research Output by Year

The investigation into CSA started in 2015 for this study, comprising 11.76% (n=2) of the CSA research output, as depicted in Figure 2. The 2015 CSA outputs coincide with the year the NCPF became public on December 4, 2015, following its approval in 2012 by the South African Cabinet.

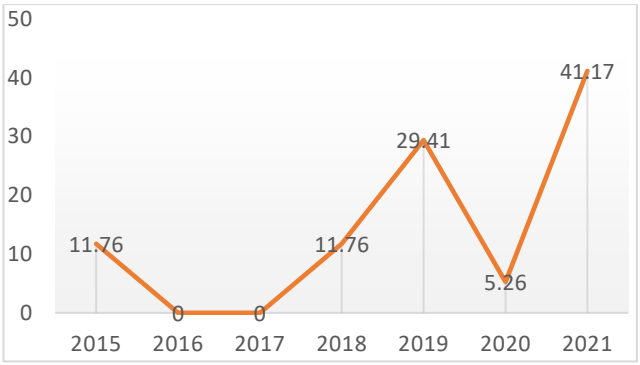

Figure 2: CSA output by year (%) 2015-2021

Conversely, 2016 and 2017 evidenced no research output on CSA. While implying a lapse in contribution during these years, plausible explanations could include shifts in research emphasis, data availability nuances, or variances in reporting protocols [11]. A resurgence, at 11.76% (n=2), surfaced in 2018, synchronizing with the broader trend discernible in subsequent years.

A substantial uptick, reaching 29.41% (n=5), occurred in 2019. The leap in 2019 is attributable to diverse factors. These include the escalating global prominence of cybersecurity issues [10], which consequently attract heightened attention. The significant input in 2019 also mirrors anticipation of emerging challenges and an urge to engage through research [16]. Compared with the preceding year, the subsequent dip to 5.26% (n=1) in 2020 likely bears the imprint of the COVID-19 pandemic. The upheaval brought about by the pandemic, spanning academic realms, manifested in disrupted research activities [11]. The downturn likely mirrors researchers' impediments while conducting and publishing research in a pandemic-dominated year. In addition, the decline could be accounted for by 2020, which is the year most students begin their thesis and dissertations on CSA, finalized in subsequent years, such as 2021.

A noticeable surge emerged in 2021, escalating to 41.17% (n=7), underscoring a remarkable augmentation of contributions. This boost in 20021 is attributable to the accelerated digital transformation induced by the COVID-19 pandemic[14], accentuating cybersecurity concerns and engendering a magnified focus on cyber threats [11]. Sub-section D unveils the CSA contribution by the department and the type of CSA output.

D. Contribution by Department and Type

As illustrated in Figure 3, the Academy of Computer Science and Software Engineering (ACSSE) produced two theses and two dissertations and is thus the leading contributor with 23.53% (n=4) of CSA research outputs. Two out of three dissertations also make the ACSSE the top contributor, with 66.66% of the dissertation cohort. The ACSSE is thus the leading contributor of new cybersecurity experts at the University of Johannesburg following the submission of dissertations. Equally, the drive for CSA within the ACSSE is driven wholly by students based on the thesis and dissertation research outputs. In parallel, Applied Information Systems (AIS) contributed two theses (11.76%) from 2015 to 2021. Although this number is small, only AIS has produced more theses. Thus, theses tie AIS with ACSSE and the Postgraduate School of Engineering Management (PSEM) at two each.

Thus, from the ten theses produced, the three computer science academic discipline members mentioned above contributed 60% (n=6). Thus, computer science academic disciplines dominate the student cohort's second tier (tier-one=dissertations). Therefore, the computer science field has a higher CSA diffusion rate than NCD studies based on student-led research output, as indicated by [22]. The PSEM produced two theses and one dissertation to further the dominance of computer science over NCD. PSEM's dissertation is the last of the dissertation cohort from the dataset. Thus, 100% of the CSA diffusion in the tier-one cohort among students comes solely from computer science.

Engineering and Built Environment (EBE) produced one thesis accounting for 5.88%. Thus, the diffusion rate of 5.88% or one output in EBE, which seeks the integration of engineering principles, design, and technology to create, develop, and manage the built environment, is an underlap. Most of the work by EBE is contemporaneously conducted through computers and stored in cyberspace. As such, the need for enriched research to substantively investigate the cybersecurity landscape is obvious for EBE [6]. Business Information Technology (BIT) contributed one thesis that reflects a focused pursuit that amalgamates CSA with business technological dimensions. Thus, CSA diffuses at 5.88% (n=1) at BIT, which calls for more efforts from the BIT to engage in CSA research as they focus on integrating information technology with various aspects of business operations and

management. The integration of information technology without a comprehensive understanding of cybersecurity could undo the very purpose of BIT.

Electrical and Electronic Engineering Studies (EEES) produced one journal article, representing a 33.33% contribution to the journal article cohort. The EEES aims to produce graduates who can undertake high-level research projects and patents and are proficient in technology innovation, project management, and safety reinforcement.

NCD studies have gained momentum in the CSA discourse, accounting for 29.41% (n=5) of the total, as they address the pervasive influence of the internet and its impact on every aspect of human life. Thus, the research by NCD studies suggests that cybersecurity is not an anachronism in fields other than computer science [31]. The Internet and cyberspace have a broader impact on various aspects of society and are thus multidisciplinary in operation and solution [10]. The College of Business and Economics (CBE) contributed 5.88% (n=1) to the 17 CSA research outputs within seven years via a thesis. While the internet is ubiquitous and shaping every facet of the human experience, the CBE needs to catch up in appreciating the cyber threats posed to business and the economy. However, the contribution is equally significant as it emanates from the student-led category.

The Department of Public Management and Governance (DPMG) contributed a journal article and thus follows the same trajectory as the CBE for various reasons, except that the DPMG has no internal diffusion from the student's perspective. While journal articles have a higher impact as they are peer-reviewed, outsiders tend to benefit more. Most consumers of the journal articles are experts and scholars [34]. Thus, the effect reverberates but never escapes the limit of the echo-chamber boundary. The Department of Communication (DoC) contributed a single conference proceedings on CSA. This single contribution accounted for 100% of the conference paper. While a small donation of 5.88% to the entire CSA output, conference proceedings bridge the academic chasm with the broader discourse, underscoring the significance of well-placed, impactful contributions. However, the DoC still has ground to cover within the strict student category as they have no CSA research in either the thesis or dissertation category. The Department of Politics and International Relations (DPIR) joins the pursuit of CSA with 5.88% (n=1) in the thesis category. While this achievement is praiseworthy due to its alignment with student-led initiatives, the DPIR, responsible for overseeing political trends and global geopolitics, should emphasize cybersecurity more [2]. State and non-state entities' escalating use of cyberspace to launch cyberattacks against crucial infrastructure, manipulate elections, and infringe upon human rights prompts further CSA research in the DPIR[6].

The Department of Accountancy (DoA) contributed one journal article, offering a glimpse into the interplay between accounting and cybersecurity. This output acknowledges the argument of [32] that most accountancy work has migrated into cyberspace. Thus, the protection of accounting digital assets should be the first in-line priority for most accounting experts and students.

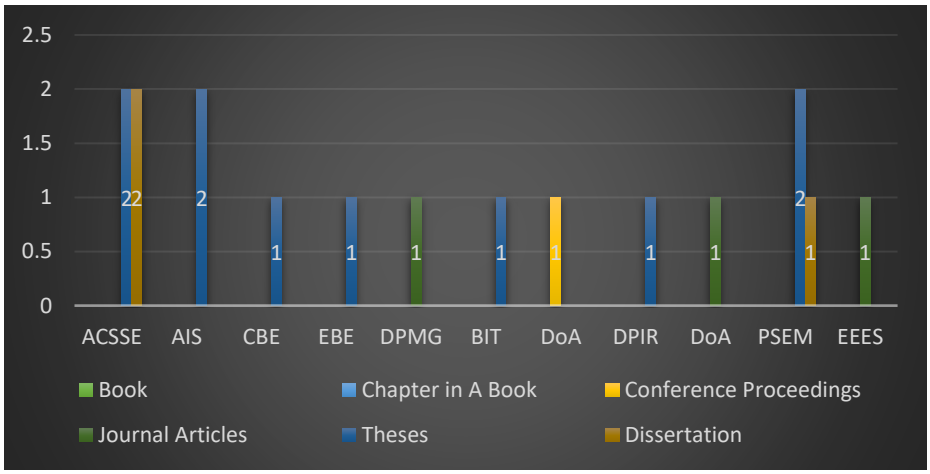

Figure 3: Departments' CSA Contribution and Type: 2015-2021

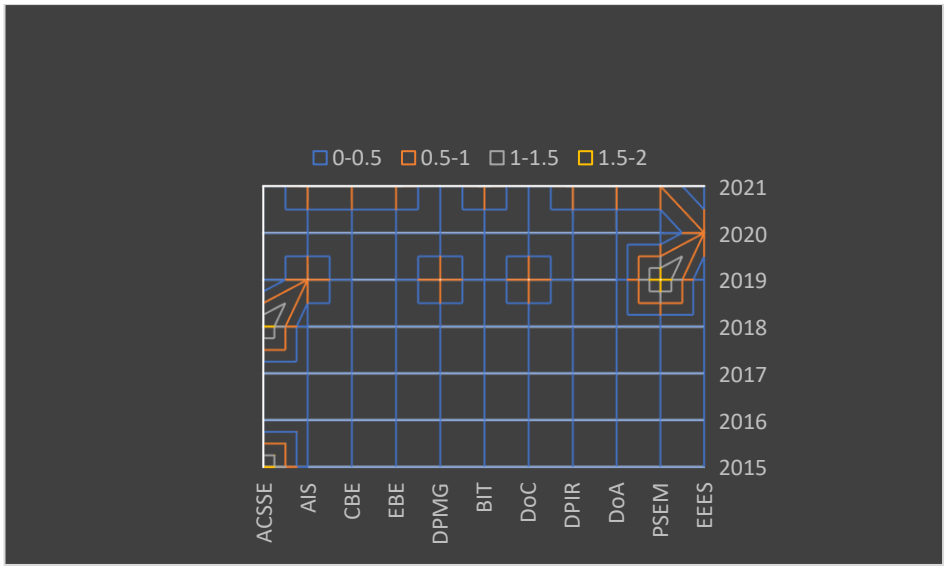

Figure 4: Department's CSA distribution by year: 2015-2021

However, the lack of any research output by the strictly student-led category (thesis or dissertation) means that the DoA has an opportunity to encourage students to consider the impact of cybersecurity on accountancy. The cybersecurity landscape is dynamic and changes occasionally [31]. As cyber threats evolve along with technology, there is a space for new observations and suggestions. Suffice it to say that each NCD academic discipline contributor has yet to produce multiple research outputs in a year. Approximately 40% (n=2) of the CSA research output from the NCD academic disciplines are theses, while 40% (n=2) are journal articles and 20% (n=1) from conference proceedings. Equally, the NCD academic discipline dominated the journal article cohort against the CS with 66.66% (n=2). In this context, sub-section E accounts for the interplay between departments on CSA and the year (s) of contribution to estimate how CSA output has evolved over the years; which departments have been critical contributors during specific periods; and whether there are any patterns or trends in the contributions of different departments to CSA over time.

E. Department's CSA Distribution by Year: 2015-2021

The analysis of CSA output evolution and departmental contributions based on Figure 4 (2015-2021) reveals several key insights.

1. Fluctuations in CSA Contributions: The CSA output at the University of Johannesburg has experienced changes over time. Notably, 2016 and 2017 witnessed no CSA contributions, possibly indicating a shift in priorities in CSA research during those years.
2. Significant Growth in 2021: 2021 is the most prominent year for CSA contributions, accounting for 41.17% of the total output. This surge is noteworthy, especially considering that 45.45% (n=5) of contributors in 2021 were making their inaugural CSA contributions. CSA gained substantial traction in 2021, likely due to the impact of the COVID-19 pandemic on digital technologies [14].
3. Departmental Dominance: The ACSSE emerged as a pioneer in CSA, initiating the trend in 2015 and maintaining a dominant presence. However, it is worth noting that the ACSSE has been dormant since 2018, signifying a shift in its contributions over time.
4. New Entrants in 2021: The year 2021 saw the entry of new contributors from various departments, including CBE, EBE, BIT, DPIR, and DOA. This correlates with the year's high CSA output; thus, new entrants significantly drove CSA research during that period.
5. Isolated Contributions: CSA contributions occurred in specific departments in some years. For example, in 2020, only the EEES department made CSA contributions. Variation in departmental engagement in CSA research is discernible.
6. Double Contributions: ACSSE and PSEM made double contributions in a year. ACSSE contributed to CSA in 2015 and 2018, while PSEM made two contributions in 2019. These instances of double contributions are dominated by the computer science academic disciplines category, reflecting its strong involvement in CSA research.

Table 3: Computer science versus NCD academic disciplines.

	# of Academic Disciplines	# of CSA Output	% of Contribution
Computer Sciences Disciplines	6	12	70.59
NCD	5	5	29.41

The analysis in Figure 4 implies that CSA output at the University of Johannesburg has evolved dynamically over the years, with contribution fluctuations and the emergence of new contributors in 2021. Figure 4 also highlights the historical dominance of ACSSE and the significance of specific years, such as 2021, in driving CSA research. These insights can guide the institution's strategic planning and collaboration efforts to enhance CSA research and awareness. Sub-section F unveils the computer science academic discipline viz-a-vis NCD comparison.

F. Comparison of Computer Science versus NCD Academic Disciplines

Table 3 demonstrates that computer science studies have made the predominant CSA contribution, accounting for 70.58% (n=12) of the total CSA research output. Meanwhile, the NCD studies comprise the remaining 29.41%.

Table 4 further supports the notion that departments, particularly those at the forefront of CSA, such as ACSSE, should explore collaboration opportunities with departments that have demonstrated lower performance, such as EBE, DPIR, DOA, and others. This collaborative approach should facilitate the exchange of CSA [11], fostering cross-pollination of ideas [25]. Table 4 also points to instances of collaboration at the inter-university level, accounting for 50% (n=2) of cases. Ultimately, the collaboration reflects a national endeavor for the diffusion of CSA. Nevertheless, external collaboration occurs predominantly within departments of a similar nature, resulting in a need for more evident cross-disciplinary knowledge exchange. Therefore, the collaboration deficit presents another promising avenue for further exploration and encouragement to promote the diffusion of CSA on an inter-department basis [22].

G. Collaboration: Interdisciplinary and inter-university.

Effective diffusion of ideas occurs through collaboration among different departments and external partners. Table 4 overviews collaborative efforts in CSA outputs at the University of Johannesburg from 2015 to 2021. Four of the 17 CSA outputs resulted from collaborations involving two or more authors. Notably, most collaborative works were observed in Journal Articles, accounting for three of the four instances, while one collaboration occurred in the conference proceedings category.

Table 4 provides additional insights, showing two instances of collaboration within the University of Johannesburg, both occurring at the departmental level. However, it is worth highlighting that data gleaned from Table 4 implies a potential opportunity for CSA diffusion and collaboration at the departmental level. Thus, exchanging cybersecurity knowledge from different disciplines can enhance CSA within the University of Johannesburg, mainly when approached from an interdisciplinary perspective.

Table 4: Interdisciplinary Collaboration Hits (2015-2021)

Year	Source Type	Collaboration Type	Lead Institution	Collaborating Departments
2019	Conference Proceedings	Inter-University	University of Kwa-Zulu Natal	School of Management Information Technology and Governance: DPMG
2019	Journal Article	Inter-University	Tshwane University of Technology	Faculty of Information and Communication Technology: DoC
2020	Journal Article	Intra-Department (EEES)	University of Johannesburg	EEES
2021	Journal Article	Intra-Department (DoA)	University of Johannesburg	DoA

V. CONCLUSIONS, RECOMMENDATIONS, STUDY'S LIMITATION AND FUTURE RESEARCH

This study examined the landscape of CSA research at the University of Johannesburg, employing DoI as a theoretical framework. The study offered valuable insights into disseminating CSA knowledge within the institution by examining research outputs across disciplines and employing various analytical techniques. Thus, the DoI contextualized the emergence of new contributors, the impact of external factors such as the COVID-19 pandemic, and the evolving landscape of CSA research. The findings revealed that CSA research has diffused across various disciplines at the University of Johannesburg, with significant contributions from NCD academic disciplines [22], reflecting the interdisciplinary nature of cybersecurity. However, challenges still need to be addressed, including limited inter-departmental collaboration, which hampers the full potential impact of national CSA efforts.

Moreover, the COVID-19 pandemic has amplified the relevance and urgency of CSA [14], leading to increased CSA research output. The study also emphasized the substantial role of students in CSA research, highlighting the potential to transform their work into journal articles for broader CSA diffusion. The current study, informed by the DoI, makes the following recommendations for the further diffusion of CSA access universities;

- Targeted Efforts in NCD Academic Discipline: Given their significant contributions, investing in targeted efforts to promote CSA in these underrepresented disciplines is advisable. The improved contribution can be achieved through dedicated funding and support for research initiatives [22], [24].
- Enhanced Collaboration: Encourage and facilitate greater inter-departmental collaboration to harness the full potential of CSA research. Cross-pollination of ideas and expertise can lead to more impactful research outcomes [22]
- Publication of Student Work: Encourage students and supervisors to transform their research findings into journal articles. The publications will enhance the visibility of CSA research and provide valuable contributions to the academic community.
- Assessment of Collaboration Efforts: Develop mechanisms to assess collaboration efforts among academia, industry, and government in cybersecurity. The assessment will enable a better understanding of the impact of collaborative initiatives.
- Departmental Cybersecurity Units: Considering the complexity of cybersecurity, universities, faculties, and departments should consider establishing dedicated cybersecurity units [24]. The Unit can facilitate focused research and CSA diffusion.
- Government Funding: Advocate for government funding for CSA projects at universities. The funding can further support CSA research and contribute to national cybersecurity efforts [24].
- Continuous Adaptation: Maintain the adaptive approach to CSA research [23], responding to evolving threats, technological advancements, and external influences [4]. This flexibility would position universities as proactive contributors to the CSA field.

Study's Limitation (s)

The study may have limited generalizability as it only used data from the University of Johannesburg. However, the current study can still pave the way for further exploration of utilizing institutional repositories of universities for examining CSA.

Future Investigations

- In this field, researchers can explore a promising direction for future research by collaborating between universities. To facilitate easier data access for researchers, universities can make other institutional repositories more accessible in the future.
- Future investigations could follow qualitative methods using interviews to probe universities' stance towards CSA in support of the NCPF and other CSA instruments in South Africa and elsewhere.
- For future investigations, a mixed-method approach could be used. A quantitative approach could determine the statistical presence of CSA in an institutional repository. At the same time, qualitative methods could capture the experiences and perceptions of stakeholders regarding the effective dissemination of CSA through institutional repositories.

- A possible future study could investigate the factors that impact the use of institutional repositories to disseminate research outputs. The hypothetical study could utilize the DoI theory to elucidate the benefits of adopting institutional repositories, as well as the obstacles and drawbacks of using them for research. Such a study could offer a more comprehensive understanding of how universities can promote the adoption of institutional repositories.

Funding

This study received no direct funding. However, the author's doctoral study is currently funded by the Global Excellence Stature Scholarship at the University of Johannesburg.

Data Availability Statement

Not Applicable.

Conflicts of Interest

The authors declare no conflict of interest.

REFERENCES

[1] Toni Hunt, "Cyber security awareness in higher education.". Symposium Of University Research and Creative Expression (SOURCE), Available at: https://digitalcommons.cwu.edu/source/2016/cob/1. vol. 1, 2016.

[2] Sizwe sama Yende, "SA "on the brink of being Africa's capital of cybercrime, says digital experts." Available at: https://www.news24.com/citypress/news/sa-on-the-brink-of-being-africas-capital-of-cybercrime-say-digital-experts-20230717.

[3] Markus Christen, Bert Gordijn and Michele Loi. "The ethics of cybersecurity,", CrimRxiv, (p. 384), 2020 [doi:10.21428/cb6ab371.d27262ff].

[4] Eyewitness News and Bateman Barry. (2017), "Check If You Were Hit by Massive SA Data Leak." Available at: https://ewn.co.za/2017/10/18/check-if-you-were-hit-by-massive-sa-data-leak.

[5] Elmarie Kritzinger and Basie von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," *Computer and Security.*, vol. 29, no. 8, pp. 840-847, 2010 [doi:10.1016/j.cose.2010.08.001].

[6] David Omand, *How Spies Think*. United Kingdom: Penguin Books, 2021.

[7] Steven Furnell and Kerry-Lynn Thomson, "Recognizing and addressing 'security fatigue'," *Comput. Fraud Sec.*, vol. 2009, no. 11, pp. 7-11, 2009 [doi:10.1016/S1361-3723(09)70139-3].

[8] Eva Nagyfejeo and Basie Von Solms, "Why do national cybersecurity awareness programmes of ten fail," *In". J. Inf. Sec. Cybercrime*, vol. 9, no. 2, pp. 18-27, 2020 [doi:10.19107/IJISC.2020.02.03].

[9] Cybercrime Act, 2020. Available at: https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf.

[10] National Cybersecurity Policy Framework. 2015. Available at: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf.

[11] Everest Rogers, *Diffusion of Innovation*. New York: The Free Press, 1995.

[12] Stephen Vargo, Melisa Akaka and Heiko Weiland, "Rethinking the process of diffusion in innovation: A service-ecosystems and institutional perspective," *J. Bus. Res.*, vol. 116, pp. 526-534, 2020 [doi:10.1016/j.jbusres.2020.01.038].

[13] Salah Kabanda, Maureen Tanner and Cameron Kent, "Exploring SME cybersecurity practices in developing countries," *J.Organ. Comput. Electron. Com.*, vol. 28, no. 3, pp. 269-282, 2018 [doi:10.1080/10919392.2018.1484598].

[14] Denys Reva, 2021, "Cyber-attacks expose the vulnerability of South Africa's ports". Available at: https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports. Africa: ISS.

[15] Limba Tadas, Pleta Tomas, Agafonov Konstantin and Damkus Martynas "Cyber security management model for critical infrastructure". Available at: https://cris.mruni.eu/cris/handle/007/15671, *JESI*, vol. 4, no. 4, 559-573, 2019 [doi:10.9770/jesi.2017.4.4(12)].

[16] Heloise Pieterse, "The cyber threat landscape in South Africa: A 10-year review," *Af". J. Inf. Commun. (Online)*, vol. 28, pp. 1-21, 2021 [doi:10.23962/10539/32213].

[17] Johannes Sekgololo, 2021, "Cybersecurity, e-learning and the rise of online student protests". Available at: https://mg.co.za/thoughtleader/opinion/2021-06-09-cybersecurity-e-learning-and-the-rise-of-online-student-protests/.

[18] Brett van Niekerk, "An Analysis of cyber-incidents in South Africa," *Afr. J. Inf. Commun. (Online)*, vol. 20, no. 20, 2017. doi:10.23962/10539/23573.

[19] Pieter Potgieter, "The awareness behaviour of students on cyber security awareness by using social media platforms: A case study at the Central University of Technology" in *ICICIS*, (pp. 272-280), 2019, Oct.

[20] Rajesh Chandarman and Brett Van Niekerk, "Students' CSA at a private tertiary Educational Institution," *Afr. J. Inf. Commun. (AJIC)*, vol. 20, 2017.

[21] Tlou Maggie Masenya, "Awareness and knowledge of cyber ethical behaviour by students in higher education institutions in South Africa" in *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems*. IGI Global, 2023, pp. 33-48 [doi:10.4018/978-1-6684-7207-1.ch002].

[22] Isabella Venter, Renette Blignaut, Karen Renaud and Anja Venter, "Cyber security education is as essential as 'the three

R's," *Heliyon*, vol. 5, no. 12, e02855, 2019 [doi:10.1016/j.heliyon.2019.e02855].

[23] Sunet Eybers and Zenzo Mvundla, "Investigating cyber security awareness (CSA) amongst managers in small and medium enterprises (SMEs)" in *Comprehensible Science*. ICCS. Springer International Publishing, 2022, pp. 180-191 [doi:10.1007/978-3-030-85799-8_16].

[24] Mohammed Khader, Marcel Karam and Hanna Fares "CSA framework for academia," *Information*, vol. 12, no. 10, p. 417, 2021 [doi:10.3390/info12100417].

[25] Sogo Angel Olofinbiyi, "A Reassessment of Public Awareness and Legislative Framework on Cybersecurity in South Africa," *Ju". Sci.*, vol. 2, no. 2(20), 34-42, 2022 [doi:10.15587/2523-4153.2022.259764].

[26] Caitlyn Murphy, Chimwemwe Queen Mtegha, Wallace Chigona and Teofelus Tonateni Tuyeni, *Factors Affecting Compliance with the National Cybersecurity Policy by SMMEs in South Africa*, 2022. African Conference on Information Systems & Technology.

[27] Noluxolo Gcaza and Rossouw von Solms, "A strategy for a cybersecurity culture: A South African perspective," *E. J. Info. Sys. Dev. Countries*, vol. 80, no. 1, 1-17, 2017 [doi:10.1002/j.1681-4835.2017.tb00590.x].

[28] Department of Telecommunications and Postal Services, 2023, *Cybersecurity Hub*. Available at: https://www.cybersecurityhub.gov.za.

[29] Ola Tjörnbo and Katharinene McGowan, "A complex-systems perspective on the role of universities in social innovation," *Technol. Forecasting Soc. Change*, vol. 174, p. 121247, 2022 [doi:10.1016/j.techfore.2021.121247].

[30] Stephen Borgatti, Ajay Mehra, Daniel Brass and Giuseppe Labiance, "Network analysis in the social sciences," *Science*, vol. 323, no. 5916, pp. 892-895, 2009 [doi:10.1126/science.1165821].

[31] Mancha Johannes Sekgololo, "The State of Cybersecurity in South Africa, 2010-2019." Available at: https://hdl.handle.net/10210/501597, 2021 ([Masters thesis]. South Africa: University of Johannesburg).

[32] Tim V. Eaton, Jonathan H. Greiner and David Layman, "Accounting and cybersecurity risk management," *Curr. Issues Aud.*, vol. 13, no. 2, pp. C1-C9, 2019 [doi:10.2308/ciia-52419].

[33] Thomas W. Valente and Everett M. Rogers, "The origins and development of the diffusion of innovations paradigm as an example of scientific growth," Sc". Commun., vol. 16, no. 3, pp. 242-273, 1995. doi:10.1177/1075547095016003002

[34] Thura Mack, Tamara Miller, Marlbeth J. Manoff and Anthony D Smith, "Designing for experts: How scholars approach an academic library web site," *Inf. Technol. Libr.*, vol. 23, no. 1, p. 16, 2004.