Journal of Applied Informatics and Computing (JAIC)
Vol.9, No.5, October 2025, pp. 2076~2088
e-ISSN: 2548-6861

Cybersecurity Awareness in Government Institutions: A Systematic Review of Behavioral Strategies and Policy Readiness

Gardner Mwansa[1]*
* Department of Information Technology, Walter Sisulu University
gmwansa@wsu.ac.za [1]

Article Info

Article history:

Received 2025-07-02
Revised 2025-07-26
Accepted 2025-08-17

Keyword:

Cybersecurity Awareness,
Cybercrime Prevention,
Cybersecurity Training,
Government Institutions,
Protection Motivation Theory,
Theory of Planned Behavior,
NIST Cybersecurity Framework.

ABSTRACT

This systematic literature review (SLR) examines 38 peer-reviewed studies published between 2015 and 2024 on cybersecurity awareness in Government institutions, following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure transparency and methodological rigor. Despite increasing cyber threats and the digitization of public services, awareness efforts remain fragmented, particularly in developing nations. The review identifies critical gaps in leadership engagement, policy standardization, training quality, and behavioral reinforcement. Countries with stable policy frameworks and sustained leadership involvement tend to implement more effective, behaviorally informed training using techniques like gamification and simulations. In contrast, others rely on outdated and underfunded strategies. Notably, theoretical models such as the Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), and institutional frameworks like the NIST Cybersecurity Framework are rarely applied, limiting impact and sustainability. This study highlights the urgent need for adaptive, role-specific, and interactive training initiatives anchored in both behavioral science and institutional readiness frameworks. By synthesizing findings across diverse contexts and applying PRISMA methodology for evidence selection and quality assessment, the review offers a timely contribution to improving cybersecurity resilience and shaping future Government awareness strategies.

I. INTRODUCTION

Cybercrime is any attack or criminal activity that involves a computer, network device or network. Further, cybercrime can also be associated with traditional crimes in which computers or networks are used in enabling a criminal activity or where evidence of a traditional crime has been found to be stored on a computer or network [1], [2]. In most cases, cybercrimes are conducted for profit gains although in some cases, it is for fun and also a way of spreading malware for the purpose of gaining some information [3]. Cybercrimes can be mitigated by cybersecurity, which is a practice used in defending any internet-based systems, software and networks from cyberattacks. NIST defines cybersecurity as "*The ability to protect or defend the use of cyberspace from cyberattacks.*" [4]. The practical implementation of this involves understanding the specific environment, analysis of various possible threats and devising necessary strategies to mitigate such malicious threats and attacks [5], [6]. It is a global trend to develop cybersecurity awareness strategies aimed at setting policy goals, measures, and institutional responsibilities as a way of ensuring the confidentiality, integrity and availability of computer data and systems against intentional and unintentional incidents and attacks.

The advent of the fourth industrial revolution (sometimes referred to as a cyber-physical system) has been driving a push for universal access to the internet, and Government departments are not immune to this push [7]. In addition, post-COVID-19 has resulted in Government departments using more cyber-based applications, such as for meetings and communication. As a result, departments have promoted an increased use of digital services amidst a growing concern about a range of threats and attacks which are characterised by ambiguity, dynamism, speed of occurrence and

anonymity, making it difficult to implement measures of control and prevention [8]. The South African national Government has recognised the seriousness of cybercrimes and has deliberately instituted comprehensive use of communication technology solutions supporting high-level security measures with an objective of embedding a broad and sophisticated cybersecurity culture [9]. The International Telecommunication Union (ITU) recommended responsibility strategies within Government institutions with respect to curbing cybercrime. These involve addressing the multi-dimensional challenges requiring a comprehensive approach that includes policies, legislation, education and awareness raising, capacity building, research, as well as technical approaches [10].

Considering the case of awareness, it is interesting to note that there are limited studies, such as those of [11]; [12] and [13] that have advanced empirical evidence in dealing with the relationship between cybercrime awareness, prevention and control in the South African Government context. For instance, [11], analysed the effectiveness of cybersecurity awareness initiatives in South Africa against the key factors of cybersecurity awareness programmes such as the analysis of cybercrime, identification of the target group, identification of the need of the target group, evaluation of plans, evaluation methods and the involvement of the Government. The study was done with the exception of Government involvement due to limited or absent participation of the Government in the awareness initiatives. This remains a huge concern as the Government plays a critical role in rolling out cybersecurity awareness to wider communities. Another study by [12] found that although cybercrime was an increase in Ghana, there was evidence of unreported crimes and arresting authorities lacked technical know-how and adequate legal support to effectively deal with cybercrimes.

Despite increased attention to cybersecurity awareness, there remains a limited understanding of its prevention and control within Government institutions [5]. Cyber threats pose serious risks to Governments, businesses, and individuals, yet the global shortage of trained cybersecurity professionals and insufficient academic programs to address this continue to undermine progress [14]. Countries like the US and New Zealand have recognized this as a human capital crisis, exacerbating the gap in effective cybersecurity promotion [15].

In South Africa, notable gaps persist in both research and implementation. Empirical data measuring awareness levels among Government employees is lacking, and existing initiatives are rarely evaluated for effectiveness. Moreover, little attention has been given to developing role-specific training or conducting longitudinal studies to assess the sustained impact of awareness programs.

While the literature on cybersecurity awareness has grown, few studies systematically compare different behavioral training models or explore how leadership involvement, policy coherence, and infrastructural limitations jointly influence the effectiveness of awareness programs in Government institutions. There is also limited synthesis of findings from both developed and developing nations, particularly in the Global South, where resource constraints heavily influence implementation. As cyber threats escalate alongside public sector digitization, a comprehensive review is urgently needed to identify which strategies work, for whom, and under what conditions. This study addresses that gap by thematically analyzing 38 peer-reviewed articles (2015–2024), offering critical insights into the effectiveness and contextual relevance of awareness initiatives in Government institutions.

Therefore, this study aims to address these challenges through three key objectives: (1) evaluating the current levels of cybersecurity awareness in Government institutions, (2) identifying the factors influencing the adoption and effectiveness of cybersecurity training programmes, and (3) analyzing the impact of threat perception and coping mechanisms on employee cybersecurity behavior. By investigating these aspects and addressing their associated deficiencies, research-driven policy interventions can be developed to enhance cybersecurity awareness initiatives significantly. Furthermore, there is limited understanding of how Government institutions interpret, adopt, and sustain cybersecurity awareness efforts as part of broader organizational culture and policy frameworks. This review addresses that gap by exploring institutional behavior, comparative intervention models, and readiness to manage cyber risk at scale.

The next section presents the literature review, followed by Section 3, which outlines the methodology used for the study. In Section 4, study results are presented. Finally, Section 4 concludes the study.

II. LITERATURE REVIEW

Cybercrime is an evolving threat that leverages technology to exploit vulnerabilities in networks, systems, and digital infrastructure. In Government institutions, cybercriminals target sensitive data, essential systems, and citizen services, posing risks to national stability and diminishing public trust. A report by the National Audit Office (NAO) highlighted that UK Government departments face a severe and rapidly advancing threat from cyber-attacks, with significant vulnerabilities identified in critical IT systems. The report criticized senior civil servants for not prioritizing cyber-resilience, leading to inadequate investment and staffing. The growing reliance on digital platforms for Government operations has significantly expanded their vulnerability to sophisticated cyber-attacks. Accordingly, hostile states such as China, Russia, Iran, and North Korea are increasingly targeting public sector systems, posing an evolving and severe threat to national security [16]. Additionally, a study by [17] emphasizes that political entities confront unparalleled challenges in securing sensitive data, upholding democratic procedures, and countering cyber threats. The research highlights the intricate interplay between state-sponsored hacking, disinformation campaigns, and the erosion of public

trust, underscoring the imperative for robust cybersecurity measures to safeguard the integrity of political systems.

South Africa faces significant challenges in addressing cybercrime. According to the Council for Scientific and Industrial Research (CSIR), the country ranks among the most targeted in Africa for cyberattacks, with Government departments frequently exposed due to outdated infrastructure and limited cybersecurity measures.

South Africa faces significant challenges in addressing cybercrime. According to the Council for Scientific and Industrial Research (CSIR), the country ranks among the most targeted in Africa for cyberattacks, often due to outdated infrastructure and limited cybersecurity measures. These challenges are compounded in rural regions, where digital exclusion and poor connectivity limit access to cybersecurity resources and awareness initiatives, as highlighted by [18]. A national survey carried out by the CSIR in collaboration with the Cybersecurity Hub under the Department of Communication and Digital Technologies revealed that 47% of public sector institutions reported experiencing between one to five cybersecurity incidents in the past year. The survey also highlighted that only 32% of organizations provided cybersecurity awareness training to more than half of their employees, indicating a significant gap in preparedness. Another incident to note is the ransomware assault on the Department of Justice in 2021, which exposed significant weaknesses in the public sector, since the attack made systems unavailable for weeks, postponing court processes and compromising sensitive information. Additionally, the CSIR emphasized the critical cybersecurity skills gap, with 63% of cybersecurity roles partially or fully unfilled, further exacerbating the country's vulnerability to cyber threats [19]

There are also a few international incidents, such as the following:

1) Colonial Pipeline Ransomware Attack (2021, USA): This attack caused major disruptions to fuel supplies along the U.S. East Coast, underscoring the vulnerability of critical infrastructure to cyber threats. This incident highlighted the urgent need for robust cybersecurity measures in sectors connected to national infrastructure and Government operations [20].
2) Australian Parliament Cyberattack (2019): Hackers infiltrated the Australian Parliament's network, compromising the data of politicians and their staff. The attack, reportedly linked to a state-sponsored actor, emphasized the geopolitical risks associated with cybercrime and the pressing need for enhanced security within political institutions [21].
3) Brazil's Ministry of Health Ransomware Attack (2021): This ransomware incident disrupted COVID-19 vaccination data systems, delaying vaccine distribution and triggering widespread public concern. The attack highlighted the severe impact cybercrime can have on public health and safety [22].

These instances demonstrate the varied and extensive effects of cybercrime on essential systems, highlighting the necessity for proactive and thorough cybersecurity measures worldwide.

A. Cybersecurity Awareness in Government Institutions

Understanding cybersecurity is a crucial safeguard against cyber threats, especially in settings that manage sensitive and vital information, like Government agencies. Awareness programs seek to inform staff about possible dangers, safe methods, and procedures to effectively reduce risks [23]. A study conducted by [11] emphasizes the importance of cybersecurity awareness in reducing human mistakes, a factor in more than 90% of successful cyberattacks. The research highlights that successful awareness initiatives should integrate technical training, behavioral modification, and cultural transformations to promote a security-aware workplace.

Social media has also revolutionized employee communication by enabling instant updates and facilitating teamwork. However, its use in the workplace introduces risks, such as phishing and social engineering attacks. Organizations must strike a balance between leveraging the benefits of social media, including improved employee engagement and seamless information sharing, while simultaneously mitigating its potential as a cybersecurity threat [24]. Additionally, social media can help reduce workplace stress by keeping employees informed about critical updates, but it requires careful monitoring to prevent misuse.

B. Theoretical Frameworks for Cybersecurity Behavior

Well-established theoretical models can enhance the understanding of cybersecurity behavior in Government institutions. Among these, the Theory of Planned Behavior (TPB) [25] and Protection Motivation Theory (PMT) [26] are widely used to explain why people engage in safe online activities. According to PMT, two appraisal processes, threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy and self-efficacy), influence protective behavior. PMT has been used in Government settings to evaluate public servants' perceptions of cyberthreats and readiness to take preventative action. For example, a study on public sector employees found that perceived threat severity and self-efficacy were strong predictors of cybersecurity behavior [27]. However, TPB contends that attitudes, subjective norms, and perceived behavioral control all influence behavior. This theory has been used extensively to examine cybersecurity policy compliance, especially in contexts where peer pressure and organizational culture influence safe behavior. According to research, TPB-based interventions can increase public institutions' intentions to adhere to cybersecurity protocols [28], [29]. Few of the 38 publications examined in this study specifically use PMT or TPB, despite their applicability, indicating a lost chance to create behavioral science-based awareness campaigns. On the contrary, institutional

frameworks like the NIST Cybersecurity Framework [30] focus on organizational risk management. NIST states that its five primary functions - Identify, Protect, Detect, Respond, and Recover offer a framework for implementing policies. However, because of capacity limitations and fragmented policy environments, adoption in the Global South is still restricted [31]. By bringing behavioral (e.g., PMT, TPB) and structural (e.g., NIST) frameworks into alignment with institutional realities such as leadership support, policy coherence, and employee norms cybersecurity awareness initiatives demonstrate improved compliance and sustainable behavior change.

C. Challenges in Promoting Cybersecurity Awareness

Initiatives to improve cybersecurity awareness in Government agencies frequently face major challenges, with a lack of adequate funding being a key issue. A study conducted by the International City/County Management Association (ICMA) found that 52% of local Governments reported a significant shortage of funds as a major obstacle to attaining high standards of cybersecurity. Furthermore, 58% of those surveyed stated that the lack of competitive salaries impacted their cybersecurity initiatives, making it even more difficult to create and implement effective awareness programmes [32]

A 2023 survey showed that 64% of local Government IT leaders believed their organization's cybersecurity funding was insufficient for essential cyber initiatives. This ongoing lack of funding greatly hinders the development and execution of successful cybersecurity awareness initiatives in Government agencies [33].

A further challenge is the ever-evolving and fast-changing landscape of cyber threats, which requires ongoing updates to awareness initiatives. Organizations encounter major difficulties in sustaining effective cybersecurity awareness initiatives because of the constantly changing threat environment. The National Institute of Standards and Technology (NIST) points out that federal agencies frequently face challenges due to constrained resources and the necessity to regularly revise training materials for new threats, resulting in programs that become outdated and ineffective [34].

Employee resistance to change and the perception that cybersecurity training is insignificant further weaken awareness programmes. Research by [34] revealed that shifting security awareness programs from being compliance-centered to influencing behavior necessitates addressing employees' views of training as merely a "check-the-box" task.

To improve the engagement and retention of cybersecurity knowledge, using interactive methods like gamification and simulations has been shown to be effective. Studies show that gamified training often results in better self-reported outcomes regarding attitudes, perceived behavioral control, intentions, and behaviors than non-gamified approaches [35].

A study by [36] emphasizes that human error significantly contributes to modern security breaches, highlighting the critical role of human factors in cybersecurity. [37] also highlight that successful cyberattacks can have profound and long-lasting consequences on organizations. Beyond immediate operational disruption, organizations often experience substantial financial losses, reduced investor confidence, and reputational damage, which may manifest through credit rating downgrades and declines in sales growth. These external impacts are compounded by internal organizational strain, employees may face job insecurity, increased workloads due to recovery efforts, and heightened psychological stress, especially when personal or HR-related data is compromised. The ripple effects of such breaches emphasize the need for comprehensive risk management strategies that address both technical vulnerabilities and human factors in organizational cybersecurity preparedness. These findings underscore the necessity for comprehensive, well-supported, and coordinated cybersecurity awareness initiatives tailored to the specific requirements of organizations, including Government agencies.

D. Global Best Practices in Cybersecurity Awareness

Various nations have developed extensive cybersecurity awareness plans that provide useful insights and can act as models for South Africa. In the United States, the "Stop. Think. Connect." initiative aims to inform both workers and the general public about recognizing and reducing cyber threats. This program utilizes a mix of webinars, public service announcements, and online materials to encourage safe digital behaviors [38]. In the United Kingdom, the National Cyber Security Centre (NCSC) offers numerous resources designed for public sector workers. This encompasses simulated cyberattacks, e-learning courses, and workshops aimed at improving cybersecurity awareness. The NCSC places a strong emphasis on working with private sector specialists to enhance the quality and impact of training initiatives [38]. Singapore also, through its Cyber Security Agency (CSA), launched the "Go Safe Online" initiative, which combines awareness campaigns, gamified learning experiences, and interactive cyber threat simulators to engage diverse audiences effectively [39]. Although these models emphasize the significance of combining interactive and adaptive methods for cybersecurity awareness, implementing them in the South African context necessitates addressing certain challenges. These involve bridging digital literacy gaps, handling resource limitations, and addressing socio-economic inequalities that could obstruct the broad implementation of these initiatives [11], [18].

These involve bridging digital literacy gaps, handling resource limitations, and addressing socio-economic inequalities that could obstruct the broad implementation of these initiatives [11], particularly in rural areas where digital exclusion remains a persistent barrier [18].

E. Cybersecurity Awareness in South Africa

South Africa's cybersecurity efforts are anchored in the Cybercrimes Act and the National Cybersecurity Framework, which aim to enhance cybersecurity awareness and capacity within the public sector [40]. The Cybersecurity Hub has been instrumental in disseminating resources and coordinating awareness initiatives. However, studies indicate that these efforts are often siloed and fail to address the specific needs of different Government departments [41].

Frontline workers who are the initial contact for cyberattacks do not receive sufficient training. Additionally, many departments fail to evaluate the effectiveness of their awareness initiatives, restricting their capacity to adjust and enhance in response to new threats [11].

The growing dependence on technology for vital services considerably raises the threat of cyberattacks and data breaches. Such events can jeopardize private citizen data, interrupt service provision, and diminish public confidence.

Government entities in South Africa are especially susceptible to different types of cybercrime, such as hacking, phishing, and ransomware assaults [42]. These harmful actions can cause considerable financial and reputational damage. Research conducted by [43] emphasizes that cybercrimes like phishing scams, online harassment, identity theft, malware, hacking, and denial-of-service attacks present significant challenges for society and harm those who fall victim to them.

F. The Role of Training and Capacity Building

Efficient training is critical for enhancing cybersecurity awareness and robustness in Government organizations. Regular workshops, e-learning platforms, and scenario-based simulations can equip employees with the skills to identify and respond to cyber threats effectively [44]. Addressing the worldwide deficit of qualified cybersecurity experts is a major challenge; however, efforts such as Microsoft's initiative to train one million South Africans in cybersecurity and artificial intelligence by 2026 showcase the potential of public-private collaborations in bridging this skills gap [45]. Likewise, integrating cybersecurity components into higher education programmes helps in creating a sustainable flow of qualified experts to fulfil the particular needs of Governmental agencies [46], [47].

Interactive methods, like gamification, have shown considerable potential in enhancing employee involvement and training results. For example, research conducted by [48] emphasizes that the integration of virtual reality (VR) and augmented reality (AR) into cybersecurity training can enhance educational experiences and results.

Thorough training programmes provide various benefits, such as reducing human mistakes, improving security protocols, boosting compliance with regulations, protecting organizational reputations, enhancing employee morale, and promoting peace of mind. These advantages are especially important in Government agencies, where the risks of cyberattacks are significant [49].

III. METHODOLOGY

This study employed a Systematic Literature Review (SLR) adhering to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to synthesize existing evidence on cybersecurity awareness in Government institutions. The methodology was designed to address the research objectives and questions through a structured, transparent, and reproducible process.

A. Research Design

The SLR focused on three primary objectives: (1) evaluating current levels of cybersecurity awareness in Government institutions, (2) identifying factors influencing the adoption and effectiveness of cybersecurity training programmes, and (3) analyzing the impact of threat perception and coping mechanisms on employee cybersecurity behavior. The research questions guiding the review were:

1. What are the current levels of cybersecurity awareness in Government institutions?
2. What factors influence the adoption and effectiveness of cybersecurity training programs?
3. How do threat perception and coping mechanisms impact cybersecurity behavior in Government employees?

B. Search Strategy

A systematic search was conducted across four academic databases: IEEE Xplore, Scopus, Springer Link, and Web of Science. The search query combined keywords related to cybersecurity awareness and Government institutions as follows:

("cybersecurity awareness" OR "information security awareness") AND ("Government" OR "public sector")

The search was limited to studies published from 2015 onward (2024) to ensure relevance to current cybersecurity practices.

C. Selection Criteria

Studies were screened using predefined inclusion and exclusion criteria to ensure relevance and focus. To be included, articles had to be published between January 2015 and 2024, focus specifically on cybersecurity awareness within Government or public sector institutions, and evaluate at least one of the following dimensions: training program adoption, employee behavior, threat perception, or coping mechanisms. Excluded from the review were studies centered on private sector organizations or general public awareness, publications not in English, and those that did not explicitly address cybersecurity training programs or behavioral outcomes.

D. Study Selection Process

The study selection process adhered to the PRISMA framework, as illustrated in Figure 1. An initial search across four academic databases, IEEE Xplore, Scopus, Springer Link, and Web of Science, yielded a total of 139 studies (32 from IEEE Xplore, 52 from Scopus, 21 from Springer Link,

and 34 from Web of Science). After merging results and removing duplicates, 105 unique records remained.

These 105 studies were then subjected to a title and abstract screening phase, during which those not focused on Government institutions or entities were excluded. This process reduced the dataset to 66 studies. A subsequent full-text review identified studies that did not prioritize cybersecurity awareness as a core focus. As a result, a final total of 38 studies were selected for in-depth thematic analysis.

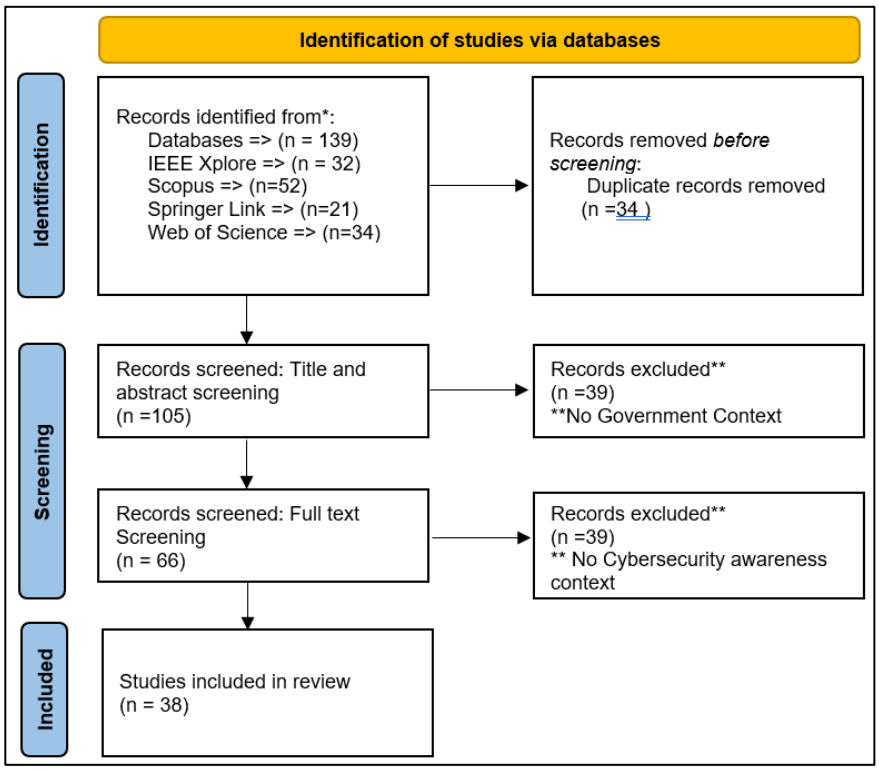

Figure 1, PRISMA flow diagram

E. Quality Assessment

To ensure methodological rigor, all included studies were evaluated for quality based on predefined criteria such as sample size, research design, and relevance to the study's research questions. During the eligibility phase, studies that lacked sufficient methodological detail or demonstrated a high risk of bias were excluded. A Quality Assessment (QA) was subsequently conducted on the final pool of 38 studies.

The assessment used a custom checklist adapted from established frameworks for evaluating empirical research, such as the Critical Appraisal Skills Programme (CASP). The checklist focused on five core dimensions: (1) clarity of objectives whether the study explicitly stated its purpose and research questions; (2) methodological rigor the appropriateness of the study's design, data collection, and analysis methods; (3) relevance to Government settings whether the focus was specifically on cybersecurity awareness within public-sector institutions; (4) quality of findings the credibility and adequacy of the evidence presented; and (5) transparency regarding limitations and bias.

Each criterion was scored on a three-point scale: 0 for not addressed, 1 for partially addressed, and 2 for fully addressed. With five criteria, the maximum score was 10. Only studies that scored at least 5 out of 10 were deemed acceptable for inclusion. All 38 articles satisfied this minimum threshold. While a few exhibited minor limitations, such as small sample sizes or partial reporting, they nonetheless offered meaningful contributions to understanding cybersecurity awareness in Government contexts.

F. Data Extraction and Analysis

For each of the 38 included studies, key information such as the scope of cybersecurity awareness, training factors, and employee behavior was extracted. Specific attention was given to how threat perception and coping mechanisms were implemented and measured, as these directly link to the third research objective. The extracted data were then organized in a spreadsheet**,** allowing for comparison and thematic analysis aligned with the research questions.

G. Ethical Considerations

Since this research solely focused on analyzing already published articles, there was no gathering of primary data,

which meant that no further ethical approval was necessary. All extracted data were anonymized and attributed to original authors to maintain academic integrity.

H. Methodological Limitations

The methodology has several potential limitations. Restricting the review to four major databases may have led to the omission of relevant studies indexed elsewhere. The exclusion of non-English publications could have overlooked valuable insights from research in other languages. Additionally, given the rapidly evolving nature of cybersecurity, findings from certain years may become outdated quickly. The focus on Government institutions also limits the generalizability of the results to other sectors. Despite these constraints, adherence to PRISMA guidelines and the application of rigorous inclusion, exclusion, and quality assessment criteria enhance the reliability and validity of the findings.

IV. RESULTS AND FINDINGS

A. Number of publications

The results obtained from the systematic review of 38 articles reveal a trend in publishing literature on articles discussing the key concepts relating to cybersecurity awareness within Government institutions. Figure 2 shows the number of publications per year in the space of 2015 to 2024. The results show an increasing trend in the publications.

I. Relevance of Articles

During the analysis, the articles were classified as highly relevant articles and moderately relevant articles, with details in Tables 1 and 2 below.

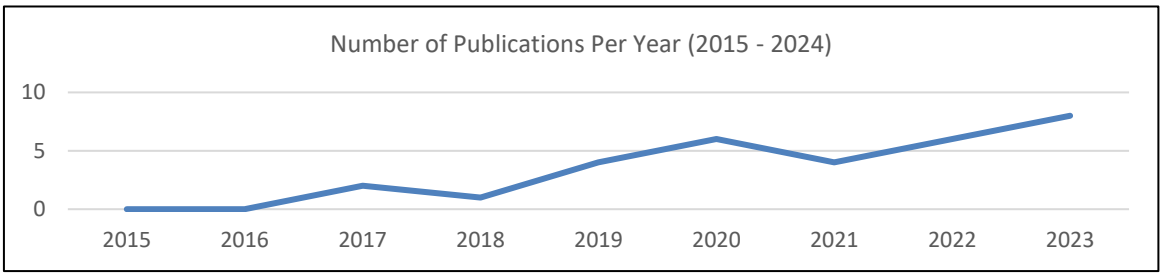

Figure 2. Number of Publications per Year

TABLE 1
HIGHLY RELEVANT ARTICLES

Article Title	Authors	Objectives	Findings	SLR Alignment
A Comparative Review of South Africa's Government-Led Cybersecurity Awareness Measures	Rama, P.; Keevy, M.	Compare South Africa's cybersecurity awareness measures to global best practices	South Africa should enhance collaboration with external entities for effective awareness programs	Directly addresses RQ1 & RQ2
Cyber Security Awareness Initiatives in South Africa: A Synergy Approach	Dlamini, Z; Modise, M	Assess effectiveness of cybersecurity awareness initiatives Analyze alignment with cybersecurity threats Propose a coordinated approach for better impact	Fragmented awareness efforts with no national policy framework Minimal Government involvement, dominated by universities and private sector Lack of coordination and standardized evaluation limits effectiveness	Directly addresses RQ1, RQ2 & RQ3
A Rollout Strategy for Cybersecurity Awareness Campaigns	Mashiane, T.; Dlamini, Z.; Mahlangu, T.	Develop a cybersecurity awareness campaign strategy for large audiences	Multi-format campaigns (e-learning, posters, face-to-face) improve awareness	Directly addresses RQ2
Unraveling Influential Factors Shaping Employee Cybersecurity Behaviors in Vietnam	Tran, D.V.; Nguyen, P.V.; Vrontis, D.	Investigate how organizational policies influence cybersecurity awareness	Organizational policies and training improve employee behavior	Directly addresses RQ3
What Behavior Change Techniques Do Government-Led Cybersecurity Awareness Campaigns Use?	van Steen, T.; Norris, E.; Atha, K.	Analyze the effectiveness of Government-led awareness campaigns	Most campaigns lack behavior change techniques, relying only on information sharing	Directly addresses RQ2
Cybersecurity Regulation and Governance	Alelayani, A.M.; Al Zahrani, F.M.; Munshi, A.M.	Evaluate governance frameworks for cybersecurity awareness	Awareness programs are essential for compliance and risk reduction	Supports RQ1 & RQ2

TABLE 2
MODERATELY RELEVANT ARTICLES

Article Title	Authors	Objectives	Findings	SLR Alignment
Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies	de Bruijn, H.; Janssen, M.	Examine how cybersecurity awareness is framed in policies	Poor communication strategies hinder awareness effectiveness	Supports RQ1
A Survey on Cybersecurity Awareness Concerns, Practices, and Conceptual Measures	Tirumala, S.S.; Valluri, M.R.; Babu, G.	Survey cybersecurity awareness practices	Awareness levels vary significantly across institutions	Supports RQ1
Cybersecurity Awareness Framework for Academia	Khader, M.; Karam, M.; Fares, H.	Propose an awareness framework for universities	Awareness must be integrated into educational programs	Supports RQ2
Cybersecurity Awareness and Fear of Cyberattacks Among Online Banking Users in Malaysia	Vafaei-Zadeh, A.; Nikbin, D.	Examine the role of fear in cybersecurity awareness	Fear influences awareness but does not directly change behavior	Supports RQ3
The Impact of COVID-19 on Cybersecurity Awareness in the SADC Region	Bagui, L.; Lusinga, S.	Analyze changes in cybersecurity awareness post-COVID-19	Increased digital reliance did not improve cybersecurity mindsets	Supports RQ1

B. Key Findings and Discussion

The following were the findings based on research questions (RQ) 1, 2 and 3.

RQ1: "What Are the Current Levels of Cybersecurity Awareness in Government Institutions?"

Many Government institutions exhibit fragmented cybersecurity awareness efforts. For instance, [50] highlight that South Africa lacks a unified national framework, with universities and private entities leading isolated campaigns in the absence of structured Government policy. Similarly, [51] found that some departments use posters and face-to-face sessions while others rely solely on e-learning, indicating inconsistent program adoption across Government sectors. A concrete example of leadership gaps can be seen in the findings of [52], where organizational policies directly influenced employee awareness levels. Government entities with strong policy direction and leadership-led initiatives had measurably higher compliance. In contrast, institutions with passive or unclear leadership showed lower awareness and weaker behavior change.

According to Rama and Keevy [53], Governments, particularly the South African Government, should prioritize strategies that focus on educating the public and ensuring that citizens remain informed about the latest cybersecurity threats. While some countries implement structured awareness programmes, others, particularly in developing countries, struggle with outdated strategies and low employee engagement [11]. Notably, the analysis of the 38 studies revealed that organizational leadership significantly influences the success of cybersecurity awareness programs. For instance, [52] found that clear organizational policies and leadership-driven training initiatives positively shaped employee cybersecurity behavior. Similarly, [50] reported fragmented awareness efforts in South Africa due to the absence of coordinated leadership and a lack of a national policy framework. These leadership gaps often translate into inconsistent communication and poor training reinforcement. The review also uncovered inter-ministerial misalignment, where awareness responsibilities were siloed across departments with minimal collaboration. In addition, training remains uneven between employee levels, with campaigns primarily targeting managerial or IT personnel while neglecting administrative and frontline staff. This disparity undermines the perceived behavioral control essential for secure conduct, as highlighted by both the PMT and the TPB. Without role-relevant reinforcement and strategic leadership engagement, many awareness efforts fail to achieve long-term behavioral impact.

The literature highlights inconsistent cybersecurity awareness levels among Government institutions, driven by fragmented implementation, outdated policies, and low employee engagement [51], [53], [54]. The Cybersecurity Hub in South Africa was established by the Department of Communications and Digital Technologies (DCDT) as a centralized platform to enhance cybersecurity awareness, facilitate collaboration, and coordinate incident response efforts among Government institutions, industry, and civil society [53]. The initiative aims to strengthen national cybersecurity resilience and ensure that individuals and organizations remain informed about emerging threats.

Despite its intended role in centralizing cybersecurity awareness, research suggests that its effectiveness varies across different Government departments. While some institutions have successfully integrated its resources, others face challenges due to limited engagement, fragmented implementation, and a lack of standardized cybersecurity policies [51], [54]. [53] emphasize that South Africa's cybersecurity strategy requires updating, incorporating collaboration with external stakeholders such as academia and

the private sector to enhance cybersecurity awareness initiatives.

To address these challenges, studies recommend improving interdepartmental coordination, increasing cybersecurity training efforts, and ensuring consistent implementation of cybersecurity policies across all Government sectors [55], [56]Strengthening these areas would maximize the Cybersecurity Hub's impact and many other initiates to contribute to a more uniform national cybersecurity framework.

It is evident that while some Government institutions in South Africa have allocated funds for cybersecurity awareness initiatives, many continue to face financial constraints that hinder the implementation of consistent, well-funded, and regularly updated awareness programmes. The uneven distribution of resources and varying levels of investment across departments contribute to a fragmented cybersecurity awareness landscape. This underscores the urgent need for standardized national policies, sustained funding, and continuous employee engagement to ensure a cohesive and resilient cybersecurity framework.

RQ2: "What Factors Influence the Adoption and Effectiveness of Cybersecurity Training Programmes?"

[57] report that budget constraints significantly impair program scalability and refresh rates. In their study, one Government agency reduced training frequency from quarterly to annually due to budget cuts, a decision linked to declining employee performance on simulated phishing tests. Interactive, behaviorally informed interventions prove more effective than static training. For example, [44] examined various Government campaigns and found that most lacked behavioral change techniques like self-efficacy reinforcement or role-based customization. On the other hand, [58] demonstrated that when fear-based messaging was supplemented with structured simulations, user engagement and compliance improved.

The effectiveness of cybersecurity training in Government institutions is influenced by several critical factors, including funding availability, leadership commitment, training methodologies, and policy implementation strategies [51], [57], [59]**.** One of the primary challenges is budget constraints, as cybersecurity training often competes with other Governmental priorities, resulting in insufficient funding for comprehensive awareness programmes [51] [53]. Without adequate financial investment, training initiatives remain inconsistent and outdated, limiting their long-term effectiveness.

Another key factor influencing cybersecurity awareness is leadership commitment. The involvement and support of senior management are essential for cultivating a culture of cybersecurity compliance and engagement among employees [59]. Organizations where leadership actively promotes cybersecurity initiatives tend to have higher levels of adherence to security policies and awareness programmes.

The methodology used in cybersecurity training also plays a crucial role in its effectiveness. Research indicates that interactive learning techniques, such as gamification, role-playing, and scenario-based exercises, significantly enhance knowledge retention and application in real-world contexts [38], [44], [58]. Traditional, passive training approaches often fail to engage employees effectively, leading to poor cybersecurity habits.

Furthermore, fragmented policy implementation remains a persistent issue. The lack of standardized frameworks across different Government departments results in inconsistent cybersecurity awareness levels, making it difficult to achieve a unified national strategy [57].

To address these gaps, studies highlight the importance of multi-format training programmes, combining e-learning modules, informational posters, and in-person workshops to maximize engagement and ensure broad accessibility [51]. By integrating structured policies, interactive methodologies, and leadership-driven engagement, Government institutions can significantly enhance their cybersecurity training effectiveness and build a more resilient cybersecurity culture.

It is clear that effectiveness of cybersecurity training in Government institutions depends on funding, leadership commitment, training methods, and policy implementation. Limited budgets often lead to underfunded programmes, while strong leadership fosters engagement. Interactive training methods, such as gamification and simulations, improve knowledge retention, but fragmented policies create inconsistencies. Multi-format training combining e-learning and workshops can enhance accessibility and engagement. Strengthening policies, training strategies, and leadership support is essential for improving cybersecurity resilience.

These results are consistent with PMT, which highlights that when people perceive a high level of threat and have self-efficacy (the belief that they can effectively take action), they are more likely to adopt protective behaviors, such as managing secure passwords or avoiding phishing. The "coping appraisal" component of PMT is weakened in a number of studies because cybersecurity awareness programs were not created to increase employee confidence or perceived control. Furthermore, the Theory of Planned Behavior (TPB) sheds light on the significance of perceived behavioral control and social norms. Since attitudes and perceived expectations from others have a significant influence on behavior, TPB suggests that Government institutions that lack peer-driven engagement or visible leadership support have lower employee motivation to comply. However, none of the interventions under review made explicit use of TPB constructs, indicating lost chances to use theoretically informed design to influence employee intent and culture.

RQ3: "How Do Threat Perception and Coping Mechanisms Impact Cybersecurity Behavior in Government Employees?"

[52] found that staff who underwent scenario-based cyberattack drills were significantly more confident in identifying and reporting real incidents. Meanwhile, institutions lacking real-time simulation or continuous reinforcement showed rapid decay in awareness retention, even when initial training was well-received. Similarly, [59]

found that academic institutions with structured coping strategies (like peer-support forums and clear incident-reporting protocols) had 28% fewer unreported cybersecurity incidents compared to those without.

Employees' perception of cyber threats significantly influences their compliance with security policies and their ability to adopt proactive cybersecurity behaviors [52], [58]. Comparative studies across Vietnam, Malaysia, and South Africa indicate that institutional adherence to secure practices is significantly reinforced by strong leadership support, frequent simulated drills, and well-defined reporting structures. For example, Vietnamese public sector institutions that integrate policy reinforcement with role-specific training show higher behavioral compliance than contexts with fragmented awareness efforts.

The review also highlights that fear alone is insufficient to drive long-term secure behaviors. Instead, success depends on structured reinforcement mechanisms, contextualized threat perception, and behavioral nudges that integrate cybersecurity into institutional identity. Organizations that foster a culture of continuous awareness through gamified learning, adaptive feedback, and real-time simulation report better preparedness and policy adherence. This highlights the need for behaviorally anchored cybersecurity strategies that go beyond one-time interventions and reflect institutional values and routines.

For cybersecurity awareness programmes to be effective, continuous reinforcement is necessary. Without ongoing education, regular reminders, and real-time cybersecurity simulations, employees may gradually become complacent, reducing their adherence to security protocols [59]. Organizations that implement clear reporting procedures and structured coping mechanisms, such as simulated cyber drills, tend to develop a stronger cybersecurity culture, ensuring that employees remain prepared to handle emerging cyber threats [57].

A study on cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia found that fear alone does not significantly improve security behavior. Instead, cybersecurity training and structured support mechanisms play a more critical role in fostering compliance and enhancing preparedness [58]. By integrating continuous reinforcement, coping mechanisms, and interactive cybersecurity education, organizations can strengthen employee engagement and ensure sustainable cybersecurity awareness and adherence to best practices.

Employees' perception of cyber threats influences their compliance with security policies and proactive cybersecurity behavior. Those who view cyber threats as high-risk are more likely to follow security protocols, but without continuous reinforcement, awareness tends to fade over time. Regular training, reminders, and simulated cyber trainings help sustain awareness and strengthen security culture. Organizations that establish clear reporting procedures and structured coping mechanisms create a more resilient workforce. Fear alone is not enough to drive compliance; instead, ongoing education and support systems play a crucial role in ensuring long-term adherence to cybersecurity best practices.

A notable finding across the reviewed studies was the limited integration of established behavioral and structural frameworks in the design and evaluation of cybersecurity awareness efforts. Specifically, models such as PMT and the TPB, both well-established in explaining secure online behavior were rarely referenced. Additionally, institutional frameworks like the NIST Cybersecurity Framework, which could support structured risk management and organizational readiness, were scarcely applied. This theoretical gap not only limits the effectiveness of existing interventions but also constrains their ability to drive sustainable behavior change. Applying PMT can help explain how employees assess threats and their own coping capacity, while TPB highlights the importance of perceived behavioral control and social norms, especially relevant in hierarchical institutions. Meanwhile, NIST provides a scaffold for embedding these behavioral considerations within broader cybersecurity policy and leadership structures. Integrating these models into future awareness strategies could significantly enhance both individual behavioral outcomes and institutional cybersecurity resilience.

C. Synthesis Across Research Questions

The findings indicate that cybersecurity awareness levels vary significantly, often constrained by insufficient funding and outdated initiatives. The effectiveness of cybersecurity training depends on adequate budget allocation, strong leadership, engaging training methods, and cohesive policy implementation across Government entities. Additionally, cybersecurity awareness has a psychological aspect, as employees' threat perception and coping mechanisms play a crucial role in influencing security behavior. However, without ongoing reinforcement and a supportive workplace culture, maintaining secure practices becomes challenging.

A comprehensive approach is necessary to enhance cybersecurity awareness and training. This requires strengthening organizational infrastructure, promoting a culture of security awareness, ensuring leadership commitment, securing sufficient funding, and prioritizing continuous reinforcement. Implementing role-specific and department-focused training, enriched with interactive learning techniques, can help address many of the challenges identified, leading to more effective and sustainable cybersecurity practices.

D. Comparative Patterns Across Contexts

A key insight that emerged from the review is the disparity in implementation and success of cybersecurity awareness programs between developed and developing countries. In developed nations, awareness efforts are often supported by stable policy frameworks, consistent funding, and integration of behavioral science techniques such as gamification and adaptive learning. In contrast, developing countries, including those in the Global South, face challenges such as fragmented policies, limited budgets, and inadequate training infrastructure. For instance, while interactive learning is widely used in countries like the UK and South Korea, institutions in South Africa and other SADC nations tend to

rely on outdated, one-size-fits-all approaches. This uneven adoption suggests that contextual constraints, particularly institutional readiness, leadership buy-in, and infrastructure, play a significant role in shaping the effectiveness of awareness initiatives.

V. Conclusion and Future Work

This review reaffirms that cybersecurity awareness in Government institutions remains fragmented and inconsistent, particularly in developing nations. Critical gaps persist in leadership involvement, training equity, funding, and the integration of behaviorally informed strategies. The review revealed that awareness initiatives often lack a theoretical foundation, with minimal application of models such as PMT, the TPB, and the NIST Cybersecurity Framework. These omissions limit the design, targeting, and sustainability of awareness programs.

Importantly, the analysis uncovered stark contrasts between developed and developing countries. While developed nations benefit from stable policies, adaptive training methods, and institutionalized behavioral reinforcement, developing countries such as those in the Global South struggle with outdated content, siloed interdepartmental coordination, and limited role-based training. Even within South Africa, implementation varies across departments, with uneven resource allocation and inconsistent integration of national platforms such as the Cybersecurity Hub.

To address these challenges, future research and policy implementation should prioritize tailored training interventions that consider the specific needs of administrative, technical, and executive staff. These programs should be grounded in theoretical models like TPB, which emphasizes perceived behavioral control and subjective norms, and PMT, which highlights the importance of coping appraisal in motivating secure behavior. Interactive learning methods, such as gamification and simulations, should replace passive training approaches to improve engagement and long-term retention. At the institutional level, structured frameworks like the NIST Cybersecurity Framework can guide the standardization of awareness initiatives, promote leadership accountability, and embed cybersecurity readiness within organizational practices.

Additionally, longitudinal assessments are necessary to evaluate the sustained behavioral impact of cybersecurity awareness efforts. Future programs should also consider both cross-national insights and context-specific constraints, including limited budgets, policy fragmentation, and digital infrastructure disparities. By integrating behavioral science with institutional frameworks and aligning global standards with local realities, Government institutions can move toward more effective, resilient, and adaptive cybersecurity awareness strategies.

Declarations

Funding: The author declare that no funding, grants, or financial support were received for this research paper.

Conflict of interest: All authors declare no conflict of interest.

Ethics & Informed consent: This Systematic Literature Review (SLR) relies solely on publicly available secondary data obtained from academic databases and published literature. No human participants, personal data, or confidential information were involved in this study. As a result, ethical approval and informed consent were not required. The research adheres to established guidelines for ethical academic research, ensuring proper citation and acknowledgement of all referenced sources.

Data Availability: The data used in this Systematic Literature Review (SLR) were obtained from publicly available sources, including academic databases such Scopus, Web of Science and IEEE Xplore. All included studies were selected based on predefined inclusion and exclusion criteria. No new empirical data were generated for this study. The full list of reviewed articles, along with their relevant metadata, is available upon reasonable request.

Author Contributions: The sole author of this study was responsible for conceptualization, methodology, data collection, analysis, writing, and revision of the manuscript. All aspects of the research, including the systematic literature review, interpretation of findings, and manuscript preparation, were conducted independently by the author.

References

[1] J. Balkin *et al.*, *Cybercrime: Digital Cops in a Networked Environment*, vol. 3, no. 1. 2007. doi: 10.1080/15536548.2007.10855811.

[2] D. Loundy, “Computer Crime, Information Warfare and Economic Espionage,” *Public Policy*, 2003.

[3] Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang, and H. Deng, “A survey of cyber crimes,” *Security and Communication Networks*, vol. 5, no. 4, pp. 422–437, 2012, doi: 10.1002/sec.331.

[4] National Institute of Standards and Technology, “Guide for conducting risk assessments,” Gaithersburg, MD, 2012. doi: 10.6028/NIST.SP.800-30r1.

[5] G. Mwansa, R. Ngandu, and O. Khala, “Cyberbullying Prevalence at a Rural Based University in the Eastern Cape, South Africa,” *International Journal of Social Science Research and Review*, vol. 6, no. 12, pp. 361–386, Dec. 2023, doi: 10.47814/ijssrr.v7i1.1783.

[6] D. Galinec, D. Moznik, and B. Guberina, “Cybersecurity and cyber defence: national level strategic approach,” *Automatika*, vol. 58, no. 3, pp. 273–286, 2017, doi: 10.1080/00051144.2017.1407022.

[7] K. Schwab, “The Fourth Industrial Revolution: what it means and how to respond,” *World Economic Forum*, pp. 1–7, 2016.

[8] Ewan Sutherland, “Governance of Cybersecurity - The Case of South Africa,” *The African Journal of Information and Communication (AJIC)*, no. 20, 2017, doi: 10.23962/10539/23574.

[9] NCPF, “The National Cybersecurity Policy Framework (NCPF) For South Africa - 2015,” *Government Gazette*, no. 39475, pp. 1–30, 2015.

[10] M. Gercke, “Cybercrime Understanding Cybercrime :,” *Understanding cybercrime: phenomena, challenges and legal response*, no. ITU, p. 366, 2012, doi: 10.1088/1367-2630/11/1/013005.

[11] Z. Dlamini and M. Modise, “Cyber security awareness initiatives in South Africa: A synergy approach,” *7th International Conference on Information Warfare and Security, ICIW 2012*, pp. 98–107, 2012.

[12] R. Boateng, O. B. Longe, and V. W. A. Mbarika, “Cyber Crime and Criminality in Ghana: Its Forms and Implications,” 2010.

[Online]. Available: https://www.researchgate.net/publication/220889824
[13] M. Grobler, J. Jansen van Vuuren, and J. Zaaiman, "Preparing South Africa for Cyber Crime and Cyber Defense," *Systemics, Cybernetics and Informatics*, vol. 11, no. 7, pp. 32–41, 2013.
[14] D. C. Rowe, B. M. Lunt, and J. J. Ekstrom, "The role of cyber-security in information technology education," *SIGITE'11 - Proceedings of the 2011 ACM Special Interest Group for Information Technology Education Conference*, pp. 113–121, 2011, doi: 10.1145/2047594.2047628.
[15] L. Fourie, B. Sarrafzadeh, S. Pang, T. Kingston, H. Hettema, and P. Watters, "The global cyber security workforce - an ongoing human capital crisis," *Global Business and Technology Association Conference*, pp. 173–184, 2014.
[16] NAO, "Threat of cyber-attacks on Whitehall 'is severe and advancing quickly,'" 2025. Accessed: Feb. 02, 2025. [Online]. Available: https://www.theguardian.com/technology/2025/jan/29/cyber-attack-threat-uk-Government-departments-whitehall-nao
[17] M. Nkongolo, "Navigating the complex nexus: cybersecurity in political landscapes," Aug. 2023.
[18] G. Mwansa, M. R. Ngandu, and Z. Mkwambi, "Bridging the digital divide: exploring the challenges and solutions for digital exclusion in rural South Africa," *Discover Global Society*, vol. 3, no. 1, p. 54, Jun. 2025, doi: 10.1007/s44282-025-00189-2.
[19] CSIR, "National survey results on the state of cybersecurity in South Africa," 2024. Accessed: Feb. 02, 2025. [Online]. Available: https://www.csir.co.za/csir-issues-national-survey-results-on-state-cybersecurity-south-africa
[20] CISA, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years ," 2023. Accessed: Feb. 02, 2025. [Online]. Available: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
[21] C. Packham, "Exclusive: Australia concluded China was behind hack on parliament, political parties – sources ," Sydney, 2019. Accessed: Feb. 02, 2025. [Online]. Available: https://www.reuters.com/article/world/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-pa-idUSKBN1W106H/
[22] Reuters, "Brazil health ministry website hit by hackers, vaccination data targeted," 2021. Accessed: Feb. 02, 2025. [Online]. Available: https://www.reuters.com/technology/brazils-health-ministry-website-hit-by-hacker-attack-systems-down-2021-12-10/
[23] D. Galinec, D. Možnik, and B. Guberina, "Cybersecurity and cyber defence: national level strategic approach," *Automatika*, vol. 58, no. 3, pp. 273–286, Jul. 2017, doi: 10.1080/00051144.2017.1407022.
[24] C. McGowan, "Social Media as a Growing Threat to the Workplace ," ISACA. Accessed: Feb. 02, 2025. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2023/social-media-as-a-growing-threat-to-the-workplace
[25] I. Ajzen, "From Intentions to Actions: A Theory of Planned Behavior," in *Action Control*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 11–39. doi: 10.1007/978-3-642-69746-3_2.
[26] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *J Psychol*, vol. 91, no. 1, pp. 93–114, Sep. 1975, doi: 10.1080/00223980.1975.9915803.
[27] M. Siponen, M. Adam Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Information & Management*, vol. 51, no. 2, pp. 217–224, Mar. 2014, doi: 10.1016/j.im.2013.08.006.
[28] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, vol. 49, no. 3–4, pp. 190–198, May 2012, doi: 10.1016/j.im.2012.04.002.
[29] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput Secur*, vol. 31, no. 1, pp. 83–95, Feb. 2012, doi: 10.1016/j.cose.2011.10.007.
[30] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.
[31] N. Kshetri, *Cybercrime and Cybersecurity in the Global South*. London: Palgrave Macmillan UK, 2013. doi: 10.1057/9781137021946.
[32] ACMA, "Inadequate Funding Biggest Barrier to Local Governments Achieving high Levels of Cybersecurity," WASHINGTON, D.C, 2017. Accessed: Feb. 02, 2025. [Online]. Available: https://icma.org/articles/press-release/inadequate-funding-biggest-barrier-local-Governments-achieving-high-levels-cybersecurity
[33] C. Teale, "Funding for local cybersecurity efforts is insufficient," Route Fifty. Accessed: Feb. 02, 2025. [Online]. Available: https://www.route-fifty.com/cybersecurity/2023/11/funding-local-cybersecurity-efforts-insufficient-survey-says/392280/
[34] J. Haney, J. Jacobs, S. Furman, and F. Barrientos, "Federal cybersecurity awareness programs :," Mar. 2022. doi: 10.6028/NIST.IR.8420A.
[35] T. van Steen and J. R. A. Deeleman, "Successful Gamification of Cybersecurity Training," *Cyberpsychol Behav Soc Netw*, vol. 24, no. 9, pp. 593–598, Sep. 2021, doi: 10.1089/cyber.2020.0526.
[36] D. C. Streeter, "The Effect of Human Error on Modern Security Breaches," 2013. [Online]. Available: http://www.economist.com/node/1389553.
[37] S. Kamiya, J. K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," *J financ econ*, vol. 139, no. 3, pp. 719–749, Mar. 2021, doi: 10.1016/j.jfineco.2019.05.019.
[38] T. van Steen, E. Norris, K. Atha, and A. Joinson, "What (if any) behaviour change techniques do Government-led cybersecurity awareness campaigns use?," *J Cybersecur*, vol. 6, no. 1, Jan. 2020, doi: 10.1093/cybsec/tyaa019.
[39] C. Vu, "Policy Report Cyber Security In Singapore," 2016.
[40] D. Mahlobo and M. David, "The National Cybersecurity Policy Framework (NCPF)," 2015. [Online]. Available: www.gpwonline.co.za
[41] CSIRT, "Cybersecurity Hub," 2012. Accessed: Feb. 02, 2025. [Online]. Available: https://www.cybersecurityhub.gov.za/
[42] H. Pieterse, "The Cyber Threat Landscape in South Africa: A 10-Year Review," *The African Journal of Information and Communication*, vol. 28, 2021, doi: 10.23962/10539/32213.
[43] D. Chudasama and R. S. Deora, "Brief Study of Cybercrime on an Internet," *Journal of Communication Engineering & Systems*, 2021.
[44] J. Prümmer, T. van Steen, and B. van den Berg, "A systematic review of current cybersecurity training methods," *Comput Secur*, vol. 136, p. 103585, Jan. 2024, doi: 10.1016/j.cose.2023.103585.
[45] N. Dludla, "Microsoft to train 1 million South Africans on AI skills," *Microsoft*, 2025. Accessed: Feb. 02, 2025. [Online]. Available: https://www.reuters.com/technology/artificial-intelligence/microsoft-train-1-million-south-africans-ai-skills-2025-01-23/
[46] S. Mishra, "Integrating Cybersecurity Education into the Curriculum: Best Practices and Implementation Challenges," 2024.
[47] H.-J. Kam, P. Menard, D. Ormond, and R. E. Crossler, "Cultivating cybersecurity learning: An integration of self-determination and flow," *Comput Secur*, vol. 96, p. 101875, Sep. 2020, doi: 10.1016/j.cose.2020.101875.
[48] A. M. Alnajim, S. Habib, M. Islam, H. S. AlRawashdeh, and M. Wasim, "Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches," *Symmetry (Basel)*, vol. 15, no. 12, p. 2175, Dec. 2023, doi: 10.3390/sym15122175.
[49] T. O. Abrahams, O. A. Farayola, S. Kaggwa, P. U. Uwaoma, A. O. Hassan, and S. O. Dawodu, "Cybersecurity Awareness And Education Programs: A Review Of Employee Engagement And Accountability," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 100–119, Jan. 2024, doi: 10.51594/csitrj.v5i1.708.
[50] Z. Dlamini and M. Modise, "Cyber Security Awareness Initiatives in South Africa: A Synergy Approach," 2012.

[51] T. Mashiane, Z. Dlamini, and T. Mahlangu, "A rollout strategy for cybersecurity awareness campaigns," in *14th Inter- national Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch, South Africa*, 2019, pp. 243–250.

[52] D. Van Tran, P. Van Nguyen, D. Vrontis, S. T. N. Nguyen, and P. U. Dinh, "Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam," *Journal of Asia Business Studies*, Nov. 2024, doi: 10.1108/JABS-01-2024-0058.

[53] P. Rama and M. Keevy, "A comparative review of South Africa's Government-led cybersecurity awareness measures to those of world-leading countries," *Southern African Institute of Government Auditors* , 2022.

[54] S. S. Tirumala, M. R. Valluri, and G. Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures," in *2019 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, Jan. 2019, pp. 1–6. doi: 10.1109/ICCCI.2019.8821951.

[55] L. Bagui *et al.*, "The impact of COVID-19 on cybersecurity awareness-raising and mindset in the southern African development community (SADC)," *The Electronic Journal Of Information Systems In Developing Countries*, vol. 89, no. 4, Jul. 2023, doi: 10.1002/isd2.12264.

[56] Ewan Sutherland, "Governance of Cybersecurity - The Case of South Africa," *The African Journal of Information and Communication (AJIC)*, no. 20, Dec. 2017, doi: 10.23962/10539/23574.

[57] A. M. Alelayani, F. M. Al Zahrani, A. M. Munshi, R. M. Monshi, and S. A. Al-Sofyani, "Cybersecurity Regulation and Governance," 2020.

[58] A. Vafaei-Zadeh, D. Nikbin, K. Y. Teoh, and H. Hanifah, "Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia," *International Journal of Bank Marketing*, 2024, doi: 10.1108/IJBM-03-2024-0138.

[59] M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for Academia," *Information*, vol. 12, no. 10, p. 417, Oct. 2021, doi: 10.3390/info12100417.