Omniscient
(An International Multidisciplinary Peer Reviewed Journal)
Vol 3 Issue 3 July-Sept 2025 EISSN: 2583-7575

Enhancing Cybersecurity Awareness Among Undergraduates in Assam: An Experimental Intervention Approach

Birina Das[1], Avani Maniar[2]

[1, 2]Department of Extension and Communication, The Maharaja Sayajirao University of Baroda
Corresponding author: birina.d-extcommphd@msubaroda.ac.in

Available at https://omniscientmjprujournal.com

Abstract

This study investigates the effectiveness of a targeted intervention program in enhancing cybersecurity literacy among undergraduate university students of Assam. A total of 80 students were selected using convenient sampling, and the research employed a pretest-posttest non-equivalent control group design within a quasi-experimental framework. Quantitative data were analyzed using the Mann-Whitney U test and intensity index. The findings revealed a significant improvement in cybersecurity literacy among the experimental group compared to the control group. Intensity analysis also revealed that the intervention programme provided relevant information and enhanced behavioural aspects among learners. The study concludes that structured intervention programs are effective in fostering cybersecurity literacy. It emphasizes the need for their integration into higher education curricula to prepare students for the challenges of an increasingly digitalized world.

Keywords: Cyberliteracy, cybersecurity, students, higher education, intervention.

Introduction

In today's digital age, cybersecurity literacy has become an essential competency for individuals navigating the online world. The proliferation of technology in everyday life has brought unparalleled convenience, but it has also introduced significant vulnerabilities. Cyberattacks, such as phishing, ransomware, and data breaches, have escalated in frequency and sophistication, making digital security a pressing concern globally (Von Solms & Van Niekerk, 2013). Despite this reality, research consistently reveals a lack of basic cybersecurity knowledge and practices among young adults, particularly university students, who are among the most active users of digital platforms (Hadlington, 2017; Haque, 2023).

Cybersecurity awareness encompasses understanding potential risks and adopting behaviours to mitigate those risks effectively. However, existing studies suggest that educational institutions have not adequately integrated cybersecurity into their curricula (Jagdeesan et al., 2023; Oluwatosin, 2024; Binh, 2023), leaving a gap in students' preparedness to handle cyber threats (Livingstone & Haddon, 2012). Given the critical role that university students will play in the future workforce and society, empowering them with cybersecurity literacy is imperative.

Cybersecurity

Protecting computer systems, networks, and data against online attacks using tools like firewalls and encryption is known as cybersecurity, and it is crucial for defending against ever-changing cyber threats (Rajani and Thakur, 2024). However, some authors argued that cybersecurity encompasses more than data security, including disinformation and social media threats. It involves technical measures and institutional efforts to safeguard against cyber threats and promote collective cybersecurity in cyberspace (Miller & Bossomaier, 2024). According to Miller et al. (2024), cybersecurity is different from cyber safety because cybersecurity is committed against intentional harm, but safety word used against accidental harm. This cyber security can be practiced when we have awareness and knowledge of the potential threats.

Cybersecurity: Awareness, Knowledge, Behaviour

Cybersecurity awareness, knowledge, and behaviour are interconnected but distinct aspects of an individual's ability to navigate the digital landscape securely. Cybersecurity awareness refers to the understanding of potential cyber threats, such as phishing, malware, or data breaches, and recognizing the importance of protective measures. It serves as the first step in fostering a secure digital environment by helping individuals identify risks. Cybersecurity knowledge goes a step further by encompassing the technical and procedural understanding required to respond to and mitigate these threats effectively. This includes knowing how firewalls, encryption, and multi-factor authentication work, as well as understanding organizational policies. The proper knowledge of the individual pushes towards practicing the event (Lee& Chua, 2023). Cybersecurity behaviour, in contrast, reflects the practical application of awareness and knowledge. It entails the consistent execution of secure practices, such as creating strong passwords, avoiding suspicious links, and updating software regularly. These three components are collectively called literacy.

Cybersecurity Literacy

The ability to comprehend, evaluate and successfully address cyber hazards and security difficulties in the digital world is known as cybersecurity literacy. It includes the fundamental understanding of cybersecurity concepts—like identifying threats like malware, phishing, and social engineering and the hands-on abilities required to put preventative measures into place, like creating strong passwords, turning on multi-factor authentication, and keeping software updated. Critical thinking abilities are also necessary for cybersecurity literacy in order to evaluate the reliability of material found online, identify harmful intent, and adopt safe practices in both personal and professional settings.

Cybersecurity literacy is especially focused on maintaining safe interactions inside the digital domain, as opposed to general digital literacy, which emphasizes the capacity to use digital tools efficiently. In the linked world of today, when people and organizations must contend with constantly changing cyber threats, it is a critical ability.

Review of literature

The study by Lim et al. (2021), titled Towards Effective Cybercrime Intervention, aimed to analyze the impact of interventions on students' understanding of cybercrime consequences. Using secondary data, it revealed that such interventions help students grasp the harmful effects of cyber-attacks on systems and livelihoods, potentially deterring malicious activities. The study also highlighted the importance of instilling ethical cyber practices and inspiring careers in cybersecurity. Singaravelu and Pillai (2014) investigated cybercrime awareness among 200 B.Ed. students in the Perambalur district using a normative survey method and cluster sampling. Their study found low awareness levels across urban and rural students, with no significant differences based on location, computer ownership, or participation in cyber forums.

Khan et al. (2018) explored Cyber Crime Awareness Among MSW Students, School of Social Work, Mangaluru, surveying 100 students. The study revealed that 68% were somewhat familiar with the term "cybercrime," while only 22% were very familiar. Students identified various components of cybercrime, with the majority recognizing its intersection with networks, technology, and human involvement. Financial institutions emerged as the most vulnerable to cybercrime. Mobite et al. (2023), in their study Awareness About Cybercrime Among College Students, analyzed 50 students from various disciplines in Narhe using stratified random sampling. The results showed that most participants had antivirus software, were cautious about online activities, and shopped only on trusted websites. They also expressed confidence in safeguarding personal devices and supported legal frameworks against cybercrime.

Sahu and Shukla (2024) conducted a study on Cyber-Crime Awareness Among Students in Chhattisgarh, examining 60 students from urban and rural areas of Pt. Ravishankar University. They aimed to assess awareness levels, revealing variations across gender and location. Rajasekar (2011) employed a questionnaire-based survey to analyze cybercrime awareness among students, considering gender and location. Using t-tests, the study found no gender differences but significant rural-urban disparities in understanding cyber threats. Similarly, Narahari and Shah (2016), in their study on Cyber Crime and Security Awareness Among Young Netizens of Anand, Gujarat, reported that 47% of participants were somewhat familiar with cybercrime, while 36% were very familiar. Awareness of specific cyber threats like hacking was relatively high (64.4%), but knowledge of issues like phishing and cyberbullying remained low.

Malhotra and Malhotra (2017) studied Cybercrime Awareness Among Teacher Trainees in Haryana, sampling 240 trainees from six colleges using a random selection method. Most participants exhibited moderate awareness (62%), with only a minority achieving high or excellent levels. Lastly, Bhate (2023) investigated Cyber Security Awareness Among Female University Students at The Maharaja Sayajirao University of Baroda, engaging 167 participants in an online survey. The study found low awareness of terms like phishing and cyberstalking but noted better understanding in areas such as passwords and social media security. An awareness session significantly improved knowledge, emphasizing the need for more extensive training efforts.

The review of the literature highlights several studies exploring cybercrime awareness among various demographic groups, such as students, teacher trainees, and young netizens, using diverse methodologies. While these studies underscore the importance of understanding cyber threats, gaps remain in comprehensively addressing cybersecurity literacy as a multi-dimensional construct encompassing both awareness and knowledge, skills, and ethical behaviour in digital environments. Most research focuses on descriptive awareness levels or demographic differences, often neglecting the depth of actionable cybersecurity practices and critical thinking skills needed to prevent cyber threats. Moreover, limited attention is given to tailored interventions that incorporate experiential or technology-integrated approaches to foster long-term behavioural change. One study reported in special reference to the M. S. University of Baroda, which only emphasizes the awareness aspect. After reviewing the above studies, researchers identified a scarcity of cybersecurity literacy aspect. Addressing these gaps is critical to transitioning from awareness to actionable literacy, ensuring individuals not only recognize cyber risks but also confidently navigate and secure digital spaces.

Rationale

The rapid digitization of daily life has made cybersecurity a critical concern for individuals, organizations, and societies. As active participants in the digital ecosystem, university students often lack adequate awareness and preparedness to navigate the complexities of cybersecurity risks. While many are proficient in using technology, they are frequently unaware of best practices for protecting personal information, safeguarding digital assets, and mitigating threats such as phishing, malware, and identity theft. In the Indian context, Indian residents lost more than Rs 1,750 crore as a result of cybercrime between January and April of 2024. The Ministry of Home Affairs oversees the National Cybercrime Reporting Portal, where more than 740,000 complaints have been filed. If we see trends, in the year 2021, a total of 52974, and in 2022, 65893 (Manral, 2023), in the year 2024, a total of 740000 cases were registered. This is showing a drastic increase in cybercrime incidence in India. The National Crime Record Bureau's data stated that 44,546 cases of cybercrimes were registered in 2019 as compared to 28,248 in 2018. The highest number of cybercrime cases were registered in Karnataka (12,020) closely followed by Uttar Pradesh (11,416), Maharashtra (4,967), Telangana (2,691) and Assam (2,231) (NCRB, 2019). Assam being one of the hotspot for cybercrime has seen the rise in the rate of cybercrimes in the last few years tremendously. National Crime Bureau (NCB) data reveals that a total of 2,231 cybercrime cases were registered in the State in 2019, which went up to 3,530 cases in 2020 and in 2021, cybercrimes in the State shot up to 4,846 cases, which is 13.8 per cent higher than the then National Rate. About 60 per cent of the youth of Assam face mental health issue due to cyber bullying (UNICEF: NSS Study). But the alarming data is that, even after such high number of cybercrime cases in Assam, the youth or the people of Assam hesitate to report it to the authority (The New Indian Express, 2024).

The researcher analyzed the curriculum of universities in Assam. The universities run no syllabus or literacy programme as part of the curriculum. Oluwatosin (2024) and Jagdeesan et al. (2023) also identified the lack of cybersecurity courses in the institution. In this continuum from the reviews, the researcher identified the scarcity of literature on cybersecurity literacy and intervention programmes on cybersecurity literacy. This gap in cybersecurity literacy underscores the urgent need for targeted educational interventions. Developing effective training programs that equip students with the knowledge and skills to identify and address cybersecurity threats is essential for fostering responsible digital citizenship. Such efforts not only enhance personal security but also contribute to broader societal resilience against cybercrime and digital exploitation.

By assessing the current levels of cybersecurity awareness among university students, the study identifies critical areas of vulnerability and knowledge deficits. Drawing on these insights, it proposes a structured and evidence-based training program designed to empower students with practical strategies to enhance their cybersecurity practices.

Research Questions

1. How far does the intervention programme enhance literacy on cybersecurity among learners?

Objectives

1. To analyse the curriculum of the State University with respect to the cybersecurity programme.
2. To develop an intervention programme to enhance literacy on cybersecurity among learners.
3. To check the effectiveness of the intervention programme for enhancing literacy on cybersecurity among learners.
4. To study the reaction of the learners to the intervention programme.

Hypothesis

H_{01}: There is no significant difference between the mean scores of post-test scores of the experimental and control groups.

Operational definition of the terms

Effectiveness of the intervention programme: The effectiveness of the intervention programme is the difference between the mean scores of the post-test scores of the experimental and control groups.

Intervention Programme: This intervention programme provides literacy training on cybersecurity. This programme includes components of cybersecurity, cyber threats, cybersecurity myths, laws on cybersecurity, precaution, and safety measures.

Methodology

This is an experimental study. The present study followed the quasi-experimental pre-test and post-test control group design. The study population was university students from Guwahati. The study sample was 80 university students selected by purposive sampling. The purpose of the sampling was the availability of the students for experimentation and permission granted by the faculty deans for experimentation in the faculty.

Tools

Achievement Test: This test was a self-prepared tool. This test consists of a total of 25 items. In this test, the researchers took all aspects of the programme to assess the objective attainment by the students. This test includes the awareness, knowledge and behavioural aspects of the programme. The '1' mark was assigned for each correct answer, and the '0' mark was assigned for each wrong answer.

Reaction Scale: This is a Likert-type scale. This scale was used to know the reaction of the students towards the programme. A total of 10 items are present in the scale.

Data Collection

For the data collection, the researchers conducted sessions in person. First of all, the researcher administered a pre-test on students of both groups. After this, the experimental group was treated with the intervention programme. The intervention programme is divided into two parts, i.e. theory and practical. In the first phase, the experimental group was taught through the theory aspect; after that, all students underwent a practical session where the researcher asked them to identify and adopt strategies through which they could protect themselves.

Data Analysis and Result

Objective 1: To analyse the curriculum of the State University with respect to the cybersecurity programme.

Result: In the analysis of the curriculum of the state universities of Assam state, the researchers were unable to find any specific paper or course that is concerned with cybersecurity. Researchers also found that no credits were assigned to cybersecurity topics.

Objective 2: To develop an intervention programme to enhance literacy on cybersecurity among learners.

Result: An intervention programme consisting of PowerPoint presentation, lecture session and practical session on topics related to different cyberthreats, common myths regarding cybercrimes, cybersecurity measures, cybercrime reporting process and government laws concerning cybercrimes in India was developed and given to the experimental group.

Objective 3: To check the effectiveness of the intervention programme for enhancing literacy on cybersecurity among learners.

Table. 1: Post-Test Achievement Scores of Groups

Groups	N	Mean	Minimum	Maximum
Control	40	14.625	10	24
Experimental	40	18.05	14	23

Result: Table no. 1 shows that the mean score of the control group was 14.62 while as mean score of the experimental group was 18.05.

H$_{01}$: There is no significant difference between the mean scores of post-test scores of the experimental and control groups.

Table. 2: Comparison Between Post Test Scores of the Control and Experimental Groups

Groups	N	Mean Rank	U-Value	Z-Value	Result
Control	40	26.25	1370.000	5.518	Significant
Experimental	40	54.75			

Result: Table no. 2 shows that the mean rank of the control group was 26.25, and the experimental group was 54.75. The U-value was 1320, and the Z-value was 5.518. in the case of Mann-Whitney U, if the value of N is more than 20 (N>20), then significance is decided by the Z-value. When the value of Z is more than 2.56 (Z>2.56), then U is significant at the 0.01 level. Since Table no. 2 shows that the Z-value was 5.518 therefore, U is significant at 0.01 level, and the null hypothesis fails to be accepted.

Interpretation: The result shows that U is significant at 0.01, which means the experimental group possess a higher level of literacy than the control group after the implementation of the intervention programme. It shows that the intervention programme is effective for enhancing literacy on cybersecurity among university students.

Objective 4: To study the reaction of the learners to the intervention programme.

Table 3: Intensity and Percentage Analysis of Reaction for the Intervention Programme

Sr	Item	SA	A	UD	DA	SDA	Intensity
1	The program increased my understanding of key cybersecurity concepts.	30	10	0	0	0	4.7
		75	25	0	0	0	
2	I feel more confident identifying and avoiding phishing emails after attending the program.	28	10	2	0	0	4.6
		70	25	5	0	0	
3	The program provided practical and actionable tips for securing my digital devices.	20	10	5	5	0	4.1
		50	25	12.5	12.5	0	
4	The content of the program was engaging and easy to understand.	25	15	0	0	0	4.6
		62.5	37.5	0	0	0	
5		18	15	2	5	0	4.1

	The hands-on activities and demonstrations were effective in enhancing my learning.	45	37.5	5	12.5	0	
6	I feel more aware of the potential cyber threats in my personal and academic life.	30	8	2	0	0	4.7
		75	20	5	0	0	
7	The program has motivated me to adopt safer online practices (e.g., stronger passwords and two-factor authentication).	30	5	0	5	0	4.5
		75	12.5	0	12.5	0	
8	The duration of the program was sufficient to cover the intended topics effectively.	15	5	3	10	7	3.2
		37.5	12.5	7.5	25	17.5	
9	The program addressed real-life scenarios that I might encounter in my daily online activities.	23	10	3	4	0	4.3
		57.5	25	7.5	10	0	
10	Overall, I found the cybersecurity program to be a valuable and worthwhile experience.	35	5	0	0	0	4.8
		87.5	12.5	0	0	0	

Result: The overall intensity was 4.3, which shows the favourable reactions of the respondents towards the intervention programme.

Statement 1: The program increased my understanding of key cybersecurity concepts.

Interpretation: 100% of respondents agreed that the program enhanced their understanding of cybersecurity concepts (75% strongly agreed). With an intensity score of 4.7, the program effectively achieved this objective.

Statement 2: I feel more confident identifying and avoiding phishing emails after attending the program.

Interpretation: 95% of respondents felt more confident in identifying phishing emails, with 70% strongly agreeing. The intensity score of 4.6 reflects the program's success in boosting confidence in this area.

Statement 3: The program provided practical and actionable tips for securing my digital devices.

Interpretation: 75% of respondents agreed the program offered practical tips, but 12.5% expressed neutrality and another 12.5% disagreed. The intensity score of 4.1 indicates moderate effectiveness in this area, with room for improvement.

Statement 4: The content of the program was engaging and easy to understand.

Interpretation: 100% of respondents agreed the content was engaging and comprehensible (62.5% strongly agreed). The high-intensity score of 4.6 suggests excellent delivery of content.

Statement 5: The hands-on activities and demonstrations were effective in enhancing my learning.

Interpretation: 82.5% agreed on the effectiveness of hands-on activities, though 5% were neutral and 12.5% disagreed. With an intensity score of 4.1, this aspect was effective but may need refinement for better engagement.

Statement 6: I feel more aware of the potential cyber threats in my personal and academic life.

Interpretation: 95% of respondents felt more aware of cyber threats, with 75% strongly agreeing. The intensity score of 4.7 highlights a strong impact in raising awareness.

Statement 7: The program has motivated me to adopt safer online practices (e.g., stronger passwords and two-factor authentication).

Interpretation: 87.5% agreed that the program encouraged safer online practices, but 12.5% disagreed. The intensity score 4.5 indicates a positive motivational impact with slight room for improvement.

Statement 8: The duration of the program was sufficient to cover the intended topics effectively.

Interpretation: Only 50% of respondents agreed that the program's duration was sufficient, while 42.5% expressed dissatisfaction (25% disagreed, and 17.5% strongly disagreed). The low-intensity score of 3.2 indicates this is a significant area for improvement.

Statement 9: The program addressed real-life scenarios that I might encounter in my daily online activities.

Interpretation: 82.5% agreed the program addressed relevant scenarios, but 10% disagreed. The intensity score 4.3 suggests good relevance overall but highlights minor gaps in connecting with real-life applications.

Statement 10: Overall, I found the cybersecurity program to be a valuable and worthwhile experience.

Interpretation: 100% of respondents found the program valuable, with 87.5% strongly agreeing. The highest intensity score of 4.8 underscores the program's overall success.

Overall Interpretation:

High effectiveness in increasing understanding, confidence, and awareness of cybersecurity.

Overall, the value and engagement of the program were highly appreciated. However, respondents suggested that programme duration should have more duration.

Discussion

The study results indicate that the intervention program was highly effective in enhancing cybersecurity literacy among university students. The findings align with previous literature and underscore the necessity of structured educational programs for bridging gaps in cybersecurity awareness, knowledge, and behaviour. Similar to Jonathan et al. (2021) and Bhate (2023), who observed positive outcomes from targeted awareness sessions, this study demonstrates significant improvements in students' understanding of cybersecurity concepts and confidence in mitigating threats like phishing. The program’s high-intensity scores (e.g., 4.7 for knowledge enhancement and 4.6 for content engagement) confirm its relevance and impact, consistent with recommendations by Oluwatosin (2024) for integrating cybersecurity training in higher education.

However, the results also reveal challenges. A relatively lower score of 3.2 for program duration sufficiency suggests the need for extended sessions to cover topics comprehensively. These findings are echoed in studies like Sahu and Shukla (2024), highlighting the importance of adequately timed interventions for fostering deeper learning. Moreover, the moderate effectiveness in practical application (e.g., securing digital devices) suggests room for refining hands-on activities.

Overall, the study reinforces the literature's call for incorporating cybersecurity literacy as a curricular component, emphasizing experiential learning for fostering actionable knowledge and behavioural change.

Conclusion

The study highlights the effectiveness of a structured intervention program in enhancing cybersecurity literacy among university students. The program significantly improved students' understanding of cybersecurity concepts, confidence in identifying threats, and motivation to adopt safer online practices. These findings align with existing research that emphasizes the importance of targeted educational initiatives in addressing gaps in cybersecurity awareness, knowledge, and behaviour. This research advocates for the inclusion of comprehensive cybersecurity training as an essential component of academic programs, ensuring that students are equipped to face the challenges of the digital age.

References

Bhate, K. (2023). A study on awareness about cyber security among the female university students. *International Journal on Emerging*

Technologies, 14(2), 13–19. ISSN 0975-8364.

Binh, T., Benson, K, Jonassen, L. (2023). Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce. *Journal of Cybersecurity Education, Research & Practice.* doi: 10.32727/8.2023.19

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky online behaviours. *Heliyon, 3*(7), e00346.

Haque, A., Ahmad, S., Haque, S., Jeswanth, K. R., Mishra, K., and Mishra, B. K. (2023). Analyzing University Students' Awareness of Cybersecurity. doi: 10.1109/etncc59188.2023.10284971

Khan, Z., & Afrozulla. (2018). Cybercrime awareness among MSW students, School of Social Work, Mangaluru. *Journal of Forensic Sciences & Criminal Investigation, 9*, Article 555757. https://doi.org/10.19080/JFSCI.2018.09.555757

Kumar, S., Grewal, D., & Khosla, M. (2021). Cybercrime awareness among teacher trainees. *IARJSET, 8*(6), 471–473. https://doi.org/10.17148/IARJSET.2021.8683

Lee, C. S., Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency.* doi: 10.1177/00111287231180093

Lim, J., & Thing, V. (2022). Towards effective cybercrime intervention. *arXiv.* https://doi.org/10.48550/arXiv.2211.09524

Livingstone, S., & Haddon, L. (2012). *Theoretical framework for children's internet use: Risk and opportunities.* London School of Economics and Political Science.

Malhotra, T., & Malhotra, M. (2017). Cybercrime awareness among teacher trainees. Retrieved from https://api.semanticscholar.org/CorpusID:212471143

Manral, S. M. (2023, December 4)24% rise in cybercrime in 2022, 11% surge in economic offences: NCRB report. *The Indian Express.* https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/

Miller, S, and Bossomaier, T., (2024). 'Cybersecurity: Threats, Countermeasures, and the Institutional Landscape. In Miller, S, and Bossomaier, T., (Eds), *Cybersecurity, Ethics, and Collective Responsibility*. New York, online education, Oxford Academic. https://doi.org/10.1093/oso/9780190058135.003.0002

Narahari, A. C., & Shah, V. (2016). Cyber crime and security – A study on awareness among young netizens of Anand (Gujarat State, India). *International Journal of Advance Research and Innovative Ideas in Education, 2*(6), 1164.

National Crime Report Bureau (2024, Feb 6). Press Release. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003158

Oluwatosin, I. Y. (2024). Bridging the Gap: Aligning Cybersecurity Education with Industry Needs. *International journal of information technology* *and computer engineering*. doi: 10.55529/ijitc.43.1.8

Rajani, M., and Thakur, N. (2024). Cyber Security. *International journal of science and research.* doi: 10.21275/mr231228122722

Rajasekar S. (2011). Cyber Crime Awareness Scale, National Psychological Corporation, Kacheri Ghat, Bhargav Bhawan4/230, Kacheri Ghat, , Agra282004 (India)

S, Jagadeesan., S., Singh, S. D., Ojha, R., Ibrahim, R. K., Alazzam, M. A. (2023). Implementation of an Artificial Intelligence with Cyber Security. *E-Learning-Based Education Management System*. doi: 10.1109/iccakm58659.2023.10449611

Sahu, & Shukla. (2024). A Study on Cyber-Crime Awareness Among Students in Chhattisgarh. *Journal of Ravishankar University (Part-A: SOCIAL-SCIENCE)*, 30(1), 54-60.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security*, *38*, 97-102.