Integrating Cybersecurity in the Classroom: Behavioural Modelling and Transformations

Betty Ogange, Commonwealth of Learning. E-mail: bogange@col.org

Walter Buyu, DSEC Consulting. E-mail: walter@dsec.co.ke

Abstract

Recent cybersecurity incidents have underscored the need for educators to upskill in cybersecurity to protect sensitive information and ensure uninterrupted learning. To help bridge this gap, COL offered the Cybersecurity Training for Teachers course series from 2020 to 2024, attracting more than 19,000 participants from 110 countries. During the training, teachers and other education practitioners acquired knowledge, skills, attitude, confidence, and commitment to help them protect themselves, their learners and institutions online. To evaluate the effectiveness of the programme, it was important to find out the degree to which participants applied what they learned in their jobs. To achieve this, surveys were administered, and one of the questions was about how the participants had used the knowledge, skills, and resources gained from the course in their daily practice. Drawing from 511 responses, this paper presents an assessment of the cybersecurity behaviours adopted by educators, behavioural modelling for students, and the transformations. We adopt thematic analysis and the New World Kirkpatrick Model to analyse and gain insights from the data. Finally, we propose the required drivers and an ecosystem to promote critical behaviours to achieve the desired results and minimise the impact of cyber threats on online teaching and learning.

1 Introduction

Even though Covid-19 spurred the adoption of online learning, virtual education continues to be integrated by schools post-Covid-19 (Chipangura & Dtendjo-Ndjindja, 2022). There is an increasing adoption of ICT by learning institutions (Fouad, 2021) and a growing number of students using digital devices for learning both at school and at home (Mehta, 2024). This progressive use of ICT in the education sector is expected to continue with more investments in education technology (Li & Lalani, 2020). Online teaching and learning introduce several risks to educators, learners and their institutions. Such threats include malware, ransomware, phishing, and privacy (Impact Networking, 2021). Learners can be exposed to dangers such as cyberbullying, online fraud, content risks and addiction (Chipangura & Dtendjo-Ndjindja, 2022). With increasing malware incidents in the education sector (Mehta, 2024), rapid technological advances introduce new risks which educators and learners might be unable to keep up with (Rahman et al., 2020). Therefore, it is imperative to empower learning institutions to integrate cybersecurity into their operations and curriculum (Mehta, 2024).

Schools are limited in teacher expertise, funding and resources to implement cybersecurity education (Rahman et al., 2020). The Commonwealth of Learning developed two cybersecurity courses – Cybersecurity Training for Teachers (CTT) and Advanced Cybersecurity Training for Teachers (ACTT) – to equip teachers, teacher educators and other education practitioners with the skills and knowledge that they need to protect themselves and their students online, as well as create awareness for parents and other stakeholders in digital learning. The CTT and ACTT courses were each offered for free in four iterations from October 2020 to July 2024. Each offer lasted a period of four weeks, save for the fourth offer of CTT, which ran for five weeks. The course series attracted over 19,000 participants from 110 countries, with 36.35% female and 62.41% male representation. The remaining 1.24% did not disclose their gender.

The CTT course comprised five modules: Introduction to Cyber Security, Cyber Threats, Defending Against Cyber Threats, Securing Online Learning Platforms, and Cyber Safety for Students. The ACTT course covered four modules: Advanced Cyber Attacks, Data Security, Advanced Personal/Host Security, and Cybersecurity Concerns in Emerging Technologies. Teachers need to be properly trained to effectively equip students with knowledge in cybersecurity (Mehta, 2024). Both courses considered the pressing cybersecurity challenges, skills needed by educators, and their knowledge level (Buyu & Ogange, 2022). Practical activities were included in each module for a hands-on experience. Furthermore, webinars were held each week during which industry experts shared their knowledge and insights from the field.

The main objective of the course was to empower participants with cybersecurity knowledge and skills to protect themselves, their learners and institutions, as well as other stakeholders in the learning ecosystem. It has been observed that while institutions spend resources to train their staff, most training often does not achieve the intended result of improving the performance of the employee and organisation. However, when employees adopt the desired behaviour post-training, their performance and that of the organisation are likely to improve (Diamantidis & Chatzoglou, 2014). Therefore, it was necessary to interrogate the changes in participants' behaviour to determine the final results of the training.

2 Integrating Modelling in the Cyber Security Training for Teachers Course

Salisu & Ransom (2014) describe modelling as “The process of learning or acquiring new information, skills, or behavior through observation, rather than through direct experience or trial-and-error efforts.” The CTT course incorporated modelling in the course design, gender, technical skills, integrating cybersecurity in the classroom, and community.

2.1 Course Design

The MOOCs were offered on mooKIT and Moodle. A mobile app, MOOC4D, was also available for participants to access the course on both Android and iPhone smartphones. Zoom was used to host webinars, while Telegram and WhatsApp were used to support learners and promote peer learning. The security features of these platforms were explored in the course. The course materials were made in different formats, including audio, video and text. Webinars were held each week during which industry practitioners shared their expertise with the participants. The design of the course, therefore, served as a model that learners could adopt in delivering cybersecurity education. Feedback from participants validated this:

“This course delivery was excellent. I must say it is one of the best deliveries I have received in a MOOC.”

“Combining the teaching-learning activities facilitated via the LMS with Zoom sessions and Telegram chat is a splendid idea.”

2.2 Gender

The representation of women in cybersecurity remains a challenge, with females forming only 25% of the cybersecurity workforce (Hoteit Leila, 2022). Interventions were made to increase the number of women in the course. An image of a lady and gentleman was used in the LMS landing page banner. Feminine promotional materials were used, and women-based networks were targeted during the registration drive. This led to an increase in the number of females enrolled in the course in the third offer, from 640 in CTT3 to 995 in ACTT3, a jump of 355. The course facilitators were all female, thus reassuring participants that women can lead cybersecurity initiatives. The guest speakers were a mix of men and women, demonstrating to learners the presence of female experts in cybersecurity.

2.3 Technical Skills

In each module, participants were guided through the implementation of technical, administrative and physical cybersecurity controls. Subsequently, learners were required to complete related practical activities. Example activities included:

- Using password managers, VPNs, two-factor authentication, encryption, and file access permissions.
- Assessing security features of online learning platforms.
- Evaluating third-party vendors for cybersecurity practices and regulatory compliance, ensuring that educational institutions partner with secure and compliant service providers.
- Identifying, assessing, and mitigating cybersecurity risks associated with emerging educational technologies.
- Developing cybersecurity guidelines and risk management plans.

Additionally, guest speakers demonstrated various tactics, tools and techniques during the webinars to further solidify what participants had learnt that week.

2.4 Incorporating Cybersecurity in the Classroom

Learners experienced first-hand the security put in place on the platforms used during the training. Safeguards were implemented on the learning management system, as well as on Zoom, Telegram, and WhatsApp. Security guidelines and etiquette were shared on Telegram and WhatsApp to guide engagements and promote safety on the platforms. To practice what they had learned, the participants were required to block access to social media sites and set up parental access controls. Furthermore, they were exposed to software for managing student devices, ensuring students were on track, and rewarding positive behaviour.

2.5 Community

Communities of practice promote collaborative learning where learners exercise shared knowledge, language, and activities (Lave & Wenger, 1991). To promote CoP, Telegram and WhatsApp groups were created for participants to share knowledge and interact with one another and the facilitators. Beyond learning, cybersecurity CoP is critical for enhancing cyber expertise and can open opportunities for funding, getting cybersecurity experience, and shaping cybersecurity culture (Fisk et al., 2023).

3 Methodology

To help evaluate the training programme, three surveys were administered in each offer: pre-course, end-of-course and tell us your story. Tell us your story survey provided an opportunity for participants to share their stories, experiences and reflections. Though the survey had 17 questions, of interest to this research was the question, *"Has any of the skills and knowledge gained / resources accessed been helpful? How have you used the knowledge gained in your daily practice? Give an example."* The question was designed to evaluate Level 3 of Kirkpatrick's Four Levels of Training Evaluation: Behaviour. Behaviour is "The degree to which participants apply what they learned during training when they are back on the job" (Kirkpatrick & Kirkpatrick, 2016). The number of respondents were as shown in Table 1.

Table 1. Tell Us You Story Survey Respondents

Offer	CTT1	CTT2	CTT3	CTT4	ACTT1	ACTT2	ACTT3	ACTT4
Respondents	80	57	49	96	79	12	59	79

Inductive thematic analysis was used to identify the themes emerging from the data set (Braun & Clarke, 2006). Semantic themes were developed by drawing themes from the data provided by the respondents. Data familiarisation was done by reading through the dataset, noting ideas and taking notes. Initial codes were generated by tagging and naming sections of text within the data item. Subsequently, themes were generated by collating and analysing the codes.

Even though the course was primarily for educators, it attracted participants outside the academic space. This was also a strength, as successful implementation of cybersecurity requires a robust ecosystem, including technology providers, parents, etc. Such learners, especially those in IT, also brought their experiences, which helped improve discussions and the overall quality of the course. Having their views in the surveys was helpful as it contributed to cyber resilience in education. Participation in the survey was voluntary and the data collected was used per the prescribed purpose.

4 Findings and Discussion

4.1 Behavioural Adoption and Application

Shift to strong passwords and password managers

Strong passwords are difficult to crack and easy to manage with password managers. Participants changed weak passwords to strong ones and used password managers to manage them. They applied the use of strong passwords to their email accounts, social media accounts, LMS, computers, and smartphones.

"I am using password management systems to secure my password instead of recording it somewhere; I have created strong passwords; I am not reusing passwords; my laptop is well secured with a strong password."

Adoption of strong authentication

Beyond passwords, the educators incorporated multifactor authentication such as biometrics and one-time passcodes, providing an extra layer of security.

"I implemented a two-factor authentication system for our school's online learning platform, significantly enhancing its security."

Protecting confidential information

Mechanisms such as encrypted storage, file permissions, and password-protected documents were employed to protect sensitive information.

"I have started to protect my documents with passphrases and read-only access (e.g. marksheets and documents shared with students so that they are unable to alter or delete the content)."

"In the past, I always have problems securing my exam questions. But now, with the knowledge gained, I can encrypt my files to avoid leakages."

"I am getting familiar with using VeraCrypt to encrypt data stored in my storage media."

Vigilance in the cyberspace

Participants became careful with the information they shared online and inspected links, websites, and emails for any phishing signs. Additionally, they avoided using public WiFi or employed security measures like VPNs.

"Recently, I received an email that appeared legitimate but had suspicious elements. Remembering the course's teachings, I immediately identified it as a potential phishing attempt. Instead of clicking any links, I verified the sender's identity through official channels and reported the incident to our IT department."

Harnessing security features on learning platforms

The exposure to security features on learning platforms resulted in their use to secure online teaching and learning.

"I think this course has been helpful especially on using Zoom. I didn't know about the security features but after this course I was able to set the security features when having zoom classes with my pupils."

Confidence in online teaching and learning

The knowledge of online threats and the countermeasures resulted in confidence to operate on the internet.

"At the beginning of Covid I felt lost as a teacher. Teaching in the classroom was a practice but now teaching online has replaced that practice. This course allowed me to continue teaching my students with confidence online knowing that cybersecurity treats can be managed."

4.2 Behavioural Modelling for Students

Integrating cybersecurity concepts into lessons

Teachers reported dedicating sessions to take students through cybersecurity or interweaving cybersecurity as part of a broader class. Some of the educators used the CTT resources to teach their students.

"The knowledge gained was exceptionally useful as I was able to teach my students on cyber threats and how to protect themselves daily. For example, many students admitted that they did not update their devices as this took too much time. I educated them on the danger of doing this and what can be the consequences of such an act. The students were quite intrigued and were able to understand and right in my presence, update their devices."

"Additionally, the resources accessed during the course have provided valuable materials for developing cybersecurity awareness campaigns within the institution."

Demonstrating safe practices in classrooms

Some of the safe practices demonstrated to learners covered phishing, updating software, and protecting their information online.

"This has been a great and memorable experience. As I'm going through the examples, one of my students suddenly pipes up and says, 'Hey, I think I got an email like that last week!' Talk about a teachable moment! I seize the opportunity to delve deeper, guiding the class through a discussion on how to spot phishing red flags and what steps to take if they ever encounter a suspicious email."

Student awareness and behavioural change

Creating awareness amongst students has the benefit of collective immunity against cyberattacks.

"Recently, a student reported a suspicious email attempting to phish login credentials. I quickly identified it as a potential phishing attack and reported it to our IT department. We promptly sent a notification to all students and staff, warning them about the email and providing guidance on how to avoid similar scams. Thanks to the knowledge gained from the CTT course, we were able to respond swiftly and effectively, preventing any potential damage."

4.3 Institutional and Pedagogical Transformations

Pedagogical Transformations

Teaching cybersecurity has the potential to enhance digital literacy and cybersecurity awareness among students.

"One example of how I've used this knowledge is by incorporating cybersecurity awareness into my classroom activities. For instance, during a lesson on internet research, I dedicated a portion of the class to discussing online safety practices with my students. Drawing from the principles learned in the CTT course, I emphasized the importance of critically evaluating online sources, avoiding suspicious links and downloads, and safeguarding personal information. Additionally, I integrated practical exercises into the lesson, such as analyzing website URLs for authenticity and identifying common indicators of phishing attempts. By actively engaging with these concepts, my students not only improved their digital literacy skills but also developed a heightened awareness of cybersecurity threats and how to protect themselves online. Furthermore, I regularly reinforce these lessons by incorporating cybersecurity discussions into classroom discussions and providing resources for further exploration. By leveraging the knowledge gained from the CTT course, I'm better equipped to educate and empower my students to navigate the digital landscape safely and responsibly."

Development or enhancement of digital safety policies

Participants created policies to help protect their institutions.

"Yes, the skills and knowledge gained from the Advanced Cybersecurity Training for Teachers (ACTT) course have been extremely helpful. For example, I utilized the knowledge of risk assessment and mitigation strategies to develop a comprehensive cybersecurity policy for our institution. This included creating guidelines for secure password practices, safe online behaviour, and protocols for responding to potential security incidents. By implementing these practices, I have enhanced the institution's overall security posture and increased awareness among both staff and students about the importance of cybersecurity."

Cross-collaboration among educators and IT staff

Knowledge of cyberthreats enhanced collaboration between educators and IT staff in implementing technical controls and complying with cybersecurity industry standards.

"I've worked closely with our IT department to ensure that our school's cybersecurity measures are aligned with industry best practices and that we're prepared to respond to potential incidents effectively."

"I have also requested that the school's IT Technician review the firewall setting to ensure that students continue to browse the Internet as safely as possible."

5 Recommendations

- Cybersecurity should be viewed as an enabler of education and not something to simply protect school data, systems and networks. A shift in this perspective ensures cybersecurity is integrated as a core component in achieving teaching and learning outcomes.
- Continuous training for educators is necessary to keep up with evolving threats, especially in the present era, where there is unprecedented growth of emerging technologies such as AI and quantum computing, which have increased the speed, scale and sophistication of cyberattacks. Cybersecurity training should begin pre-service and continue in-service with follow-up modules, refreshers, and self-directed learning.
- Leadership support is crucial for the success of cybersecurity programmes. The management of learning institutions should support cybersecurity capacity building in knowledge, skills, and tooling. They should also establish a clear mechanism for monitoring, reinforcing, rewarding and encouraging critical behaviours post-training.
- Educators should join cybersecurity CoPs in their countries and globally to enhance their cybersecurity expertise. Through CoPs, educators can gain world-class competence which can be used to build local cyber capacity, leading to sustainable development of cybersecurity programmes.
- Gender disparity in cybersecurity is evident, with women underrepresented in both training and the industry (Peacock & Irons, 2017). Interventions should be made to eliminate barriers such as low enrolment in STEM disciplines, awareness of cybersecurity, the masculine perception of cybersecurity, and the lack of female role models, mentors, and sponsors (Hoteit Leila, 2022).
- Schools should have a team of first responders for cyber threats. This team should comprise staff trained to address the needs of students and staff during a cyber incident. Community volunteers such as parents skilled in this area could also be valuable (Nason, 2024). Teachers who went through CTT could be part of the incident response teams since they learnt risk management and developed a cybersecurity preparedness plan for their institutions as part of the practical activities (Buyu & Ogange, 2022). It would also be imperative to upskill the school management and IT teams in cybersecurity to help them provide strategic direction and effective technical support during a crisis.

- Education institutions should be empowered to independently incorporate cybersecurity into their operations and curriculum (Mehta, 2024). This requires government and industry to work together to realise the necessary policies, subsidies and investments to drive cybersecurity programmes in educational institutions (Amankwa, 2021). Cybersecurity education should be introduced at an early age as learners are already using digital devices from kindergarten.

6 Conclusion

Upskilling educators in cybersecurity remains a key pillar in protecting learners and schools against cyberattacks. Incorporating behaviour modelling in cybersecurity training for teachers makes it easier to understand and apply the concepts taught. Teachers can replicate these models in the classroom, leading to increased cybersecurity resilience. Safety in online learning environments is a fundamental issue warranting safeguards to be incorporated into the learning design.

Disclaimer

References

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, *12*(4), 233–249.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Buyu, W., & Ogange, B. (2022). *Cybersecurity in Online Learning: Innovations for Teacher Training and Empowerment*.

Chipangura, B., & Dtendjo-Ndjindja, G. (2022). Securing the cybersafety of South African online high school learners beyond COVID-19. *The Journal for Transdisciplinary Research in Southern Africa*, *18*(1), 1256.

Diamantidis, A. D., & Chatzoglou, P. D. (2014). Employee post-training behaviour and performance: evaluating the results of the training process. *International Journal of Training and Development*, *18*(3), 149–170.

Fisk, N., Kelly, N. M., & Liebrock, L. (2023). Cybersecurity communities of practice: Strategies for creating gateways to participation. *Computers & Security*, *132*, 103188. https://doi.org/https://doi.org/10.1016/j.cose.2023.103188

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Hoteit Leila. (2022, September 9). *Empowering women can help fix the cybersecurity staff shortage*. World Economic Forum. https://www.weforum.org/stories/2022/09/cybersecurity-women-stem/

Impact Networking. (2021). *15 Cybersecurity In Education Stats You Should Know*. https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/

Kirkpatrick, J. D., & Kirkpatrick, W. K. (2016). *Kirkpatrick's Four Levels of Training Evaluation*. Association for Talent Development.

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge university press.

Li, C., & Lalani, F. (2020). *The COVID-19 pandemic has changed education forever. This is how*. Word Economic Forum. https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/

Mehta, K. (2024, September 10). *Should cybersecurity be made part of the school curriculum?* World Economic Forum. https://www.weforum.org/stories/2024/09/de059443-c00c-4b15-94c0-5a367c94d31b/

Nason, A. (2024, February 27). *Why School Districts Should Consider a Team of First Responders for Cyber Threats*. CORO. https://www.coro.net/blog/why-school-districts-should-consider-a-team-of-first-responders-for-cyber-threats

Peacock, D., & Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology*, *9*(1), 25–44.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382.

Salisu, A., & Ransom, E. N. (2014). The role of modeling towards impacting quality education. *International Letters of Social and Humanistic Sciences*, *32*(1), 54–61.