Spring 6-29-2022

A Proposal for Social Ethical Hacking Framework for Detecting and Managing Human-Induced Vulnerabilities in Organizational Cybersecurity

Maharazu Kasim
American University of Nigeria, maharazu.kasim@aun.edu.ng

Mohammed Bashir Saidu
American University of Nigeria, mohammed.saidu@aun.edu.ng

Abdullahi Isa
American University of Nigeria, abdullahi.isa@aun.edu.ng

Samuel C. Avemaria Utulu
American University of Nigeria, samuel.utulu@aun.edu.ng

A Proposal for Social Ethical Hacking Framework for Detecting and Managing Human-Induced Vulnerabilities in Organizational Cybersecurity

Maharazu Kasim
Department of Information Systems,
School of Information Technology and Computing,
American University of Nigeria, Yola, Nigeria.
Maharazu.kasim@aun.edu.ng

Mohammed Bashir Saidu
Department of Information Systems,
School of Information Technology and Computing,
American University of Nigeria, Yola, Nigeria.
Mohammed.saidu@aun.edu.ng

Abdullahi Isa
Department of Information Systems,
School of Information Technology and Computing,
American University of Nigeria, Yola, Nigeria.
Abdullahi.isa@aun.edu.ng

Samuel C. Avemaria Utulu, Ph.D.
Department of Information Systems,
School of Information Technology and Computing,
American University of Nigeria, Yola, Nigeria.
Samuel.utulu@aun.edu.ng

Abstract

Organizations carry out an ethical hacking approach to combat cybersecurity challenges, focusing on the technical aspects of cybersecurity vulnerabilities. The practice persists despite evidence that shows that human-induced cybersecurity vulnerabilities constitute a significant threat to organizational cybersecurity. To address this gap, we propose the social-ethical hacking framework to deal with human-induced cybersecurity vulnerabilities in organizations. We adopted the interpretive case study research method, the community of practice theory as the theoretical study lens, and university undergraduate students as the study context. Research data was collected through interviews and participatory observation. The study reveals how the communities of practice undergraduate students established in the study context enabled the institutionalization of social actions and behaviors that constitute cybersecurity vulnerabilities. Organizational actors jointly create the social behaviors and actions that make organizations vulnerable to cybersecurity challenges and should focus on social-ethical hacking practices. The result shows the crucial role of competence in degenerating similar behaviors among undergraduate students; and how their social behaviors make their institution susceptible to cyber security threats.

Keywords: Social-Ethical Hacking, Penetration Testing, Cybersecurity Vulnerabilities, Community of Practice Theory, Universities, Undergraduate Students

1.0 Introduction

It is almost common knowledge globally that the benefits of using information and communication technologies (ICTs) are unprecedented. Despite the benefits, ICT users are still obliged to deal with various issues related to cybersecurity vulnerabilities. Cybersecurity vulnerability has to do with the security gaps that allow criminals that perpetrate cybercrimes to have unauthorized access to an organization's cyberspace. It results in intended distortion and unauthorized access to and modification of information, making information lose its value and integrity (Zwilling et al., 2020). Cybersecurity breaches may lead to financial loss, loss of an organization's reputation and integrity, and in some cases, total bankruptcy (Abawajy, 2014). Cybersecurity breaches manifest in different ways, including hacking, phishing, taken-for-granted actions and behaviors, unnecessary trust, and sharing passwords. Even though ICTs are prone to vulnerabilities that may lead to any of these cybersecurity breaches, scholars have persistently argued that human factors are the leading causes of cybersecurity breaches (Abawajy, 2014; United Nations Institute for Disarmament Research, 2017). In the context of this study, human factors refer to human behaviors and actions that people enact within organizations and other forms of defined social groups. Human factors evolve from users' ignorance, careless behaviors, and actions that expose organizations to unintentional vulnerabilities that are likely to lead to colossal cybersecurity breaches (Abawajy, 2014; Kortjan & Von Solms, 2014). Human factors enable attackers to exploit loopholes in organizations' cybersecurity programs softly and promote the use of social engineering by culprits (Hatfield, 2018; Salahdine & Kaabouch, 2019).

Most people who use ICT either lack sufficient knowledge of cybersecurity threats or deliberately do not pay attention to issues that promote cybersecurity threats. Most cyber attackers search for vulnerabilities connected to human actions and behaviors. Although technical issues are connected to ICT that enables cybersecurity threats, often technical issues are further exacerbated by human actions and behaviors (Ovelgönne et al., 2017). People enact questionable behaviors such as password sharing, opening spam emails, eavesdropping, opening untrusted sites, and downloading games. The behaviors expose them and the organizations where they work to cybersecurity threats. Cyber attackers are well aware of this and exploit people's negligence to their advantage. Often, attackers tap into the opportunities people unknowingly provide to them due to questionable actions and behaviors and, as a result, hit the target they least expected. Organizations adopt a primary strategy to avert cybersecurity threats by implementing ethical hacking. Ethical hacking is deliberate hacking into organizations' systems to detect cybersecurity vulnerabilities that may result from how the systems are designed and implemented (Hartley, 2015). This process is traditionally technical. Thus, cybersecurity experts, otherwise called White Hats, are hired to attack the system's hardware deliberately, not to damage or expose the system to danger, but to detect, understand, and strengthen the system's security against cybersecurity threats (Farsole et al., 2010). In other words, the hacking tests the technical strength of the system. Ethical hacking only tests the integrity of a system's security based on technical (hardware and software) requirements. Unfortunately, ethical hacking is designed and implemented to help organizations detect the potential areas for an attack on their systems; it rarely considers human factors connected with human behaviors and actions that enable hacking.

However, ethical hacking has proved to be a critical strategy for cybersecurity threats against organizations (Hartley, 2015). However, we thought that it is equally essential for organizations

to conduct a deliberate test of the integrity of organizational actors' social behaviors and actions to understand how the social behaviors and actions may impact organizational cybersecurity strength and integrity. We are of this opinion because no evidence in the literature reports how experts carried out a program meant to deliberately breach an organization's cybersecurity to identify cybersecurity vulnerabilities caused by human behaviors and actions. We are not ignorant of studies that deal with social engineering e.g. (Hatfield, 2018; Salahdine & Kaabouch, 2019). We argue that there is no attempt to produce a framework for testing the integrity of organizational actors' behaviors and actions to understand how they impact organizational cybersecurity integrity. Our observation during the study also shows that organizations do not pay enough attention to designing and implementing practices geared toward identifying, assessing, and understanding cybersecurity vulnerabilities caused by organizational actors' behaviors and actions. In other words, we identify the need for a concerted effort to develop a variation of ethical hacking targeted not on the technical strength of organizational cybersecurity but the social strength of organizational cybersecurity. We argue for a *social-ethical hacking* framework to augment the role ethical hacking plays in ensuring organizational cybersecurity strength and integrity. In the context of our study, social-ethical hacking has to do with deliberately spurring organizational actors to behave and act in ways that could lead to cybersecurity attacks. Social-ethical hacking aims to enable organizations to identify how knowledgeable organizational actors are regarding behaviors and actions that could lead to cybersecurity breaches. We present social-ethical hacking as an act that involves deliberately designing a program through which certain social behaviors and actions are spurred among organizational actors. Social-ethical hacking presents real-time situations to know how organizational actors understand the implications of their behaviors and actions on organizational cybersecurity integrity.

Therefore, an appropriate social-ethical hacking framework can only be designed if social actors' social behaviors and actions are exposed and understood. Interestingly, there is a deluge of theoretical notions on how social behaviors and actions evolve and get institutionalized. The theoretical notions explicate why and how social actors or organizations behave and act in similar ways and, over time, get the behaviors and actions institutionalized (Csordas, 2008; Schütz & Luckmann, 1989; Tolbert, 1999; Wenger, 2000, 2010). One important lesson we learned from the theoretical notions is the possibility that social actors can develop and institutionalize behaviors and actions that can make their organization's cybersecurity vulnerable. Consequently, we adopted the community of practice theory as a lens to guide the exposition and understanding of social actions and behaviors that must be understood if we are to propose an appropriate social-ethical hacking framework. The community of practice theory provides the basis for seeing universities as communities where behaviors and actions are shared and situated within specific communities of practice (Wenger, 2010; 2000; Li et al., 2009). Community of practice theory provides the basis to identify how organizational actors within universities develop competencies through which they define their identity, ascribe meanings to behaviors and actions, and institutionalize behaviors and actions that may unknowingly cause cybersecurity threats. The implication is that the study is driven by the notion that organizational actors' behaviors and actions develop through institutionalized social learning and knowledge-sharing practices enacted within communities of practice. The social-ethical hacking framework proposed in the study is designed for universities and complements existing cybersecurity frameworks (Badamasi & Utulu, 2021; Crick et al., 2019; Fatokun et al., 2019) and for other organizations; if only we could have proof of the existence of communities of practice. This suggests that the framework can be employed to carry out social-

ethical hacking in other organizations. We focused on undergraduate students because they are more vulnerable to cybersecurity threats than other university groups. The following research question drove our study: How can understanding undergraduate students' everyday life experiences and cyber activities contribute to developing a social-ethical hacking framework?

2.0 Literature Review

Organizations have identified the importance of cyberspace to their core business functions. This has made it one of the critical assets of organizations. Cyberspace comprises ICT and is a virtual world for social, economic, and political interactions. Cyberspace constitutes an organizational information environment (Singer & Friedman, 2014). Even though some commentators confuse cyberspace for the internet, the internet encompasses all networks that are put together to interact.

On the other hand, cyberspace includes the internet, the people behind those innovations, and the physical infrastructures that enable the platform (Ottis & Lorents, 2010; Strate, 1999). Nevertheless, there are so many challenges threatening the existence of cyberspace, specifically, the people who operate in the virtual world. Many people have been doped in cyberspace. Some have been exposed to new ways of living and carrying out businesses that are contradictory to those they are familiar with. Some have developed multiple questionable and fake identities, leading to serious cybersecurity concerns. Organizations need to implement specific cybersecurity measures to curtail the growing concern about cyberspace's security of information and resources. One measure that is already in use is ethical hacking. Ethical hacking refers to putting forward specific hacking skills to deliberately hack into an organization's systems to identify vulnerabilities in the systems and take precautionary measures against hackers. Ethical hackers are hired to break into an organization's system to detect any potential cyberattack (Engebretson, 2013; Farsole et al., 2010; Hartley, 2015).

It is said that paranoid organizations offer incentives to hackers to break into their systems and report traces of vulnerabilities (Maillart et al., 2017). Deliberately hacking is called bug bounties (Maillart et al., 2017; Sridhar & Ng, 2021) or legitimate use of social engineering techniques (Steinmetz et al., 2021). This exercise is a proactive measure aimed at detecting vulnerabilities and developing programs to counter them. Ethical hacking is carried out to keep organizations a step ahead of hackers. Scanning ports and snipping vulnerabilities, examining patch installation, social engineering techniques (such as pretending to be friendly with employees, shouldering, etc.), sniffing through networks, and unlocking stolen devices, among other things, may be done by an ethical hacker (Chakraborty et al., 2020; Sahare, 2014). Even though there is a casual mention of specific social engineering techniques in the work of (Steinmetz et al., 2021), social engineering differs from the social-ethical hacking framework we are proposing. A critical look at the basis of ethical hacking activities shows that activities completed during ethical hacking are more technically oriented. Although ethical hacking sometimes involves social engineering techniques that test behaviors and actions, they are usually relegated to the background during ethical hacking for more technically oriented cybersecurity integrity tests (Maillart et al., 2017). Apart from the fact that social engineering techniques are relegated to the background during ethical hacking processes, social engineering has to do with deliberately twisting peoples' behaviors and actions to behaviors that will enable cybersecurity attacks. There are also the key issues that have to do with the non-existence of a framework for carrying out social engineering. For example, an ethical hacker socializing with employees to make them release their passwords or other sensitive

information shows elements of socialization before the action. The hacker had to trick them into releasing their password. However, the result is detecting the vulnerability, not how the behavior led to the attack.

A review of literature on ethical hacking reveals that the number of research studies carried out on the subject, particularly those in Africa, is still very much scanty. Disappointingly, the few studies mainly focused on reinventing efforts required to understand technically orchestrated hacking into cyberspaces (Chhillar & Shrivastava, 2021; Cisar & Pinter, 2019; Hawamleh et al., 2020; Patil et al., 2017; Pienta et al., 2020; Pike, 2013; Tabassum et al., 2021; Trabelsi & Ibrahim, 2013). For example, a study by Pike (2013) focused on developing ethics guiding the practice of ethical hacking among students. The study was concerned with developing mechanisms to minimize the chances of committing criminal acts with the hacking skills paramount among students in contemporary educational institutions. This is because many students have been convicted of illegally practicing the hacking skills they learned. Thus, the ethics are vent on neutralizing the technical ethical hacking rather than social issues connected to the misuse of hacking skills. Hawamleh et al. (2020) suggested using ethical hacking as a security analysis tool to minimize cybersecurity risks. Their study was also mainly centered around technical ethical hacking. Distinctly, Steinmetz et al. (2021) conducted a study to determine the attributes that social engineers employ to successfully and effectively achieve their social engineering deceptions. One important finding in the study is how critical 'social context' and 'perception about human nature' are to successful social engineering. The problem with the study is that it underscored human actions and behaviors that enable those carrying out social engineering to carry out their malicious intents successfully. We can confirm that no study has been devoted to conceptualizing a social-ethical hacking framework. There are also no studies devoted to developing a framework that will enable organizations to practically assess how human vulnerabilities may promote cybersecurity vulnerabilities in organizations. It is problematic that existing studies ignore social-ethical hacking but only focus on ethical hacking, given that it pays strong attention to technical factors.

2.1 Theoretical Context of the Study

Community of practice is a social learning theory emphasizing that learning and knowledge creation are journeys into a community with shared characteristics (Li et al., 2009). The term 'community' does not always imply co-existence, a well-defined, identifiable group, or socially visible boundaries; instead, it refers to participation in an activity system in which participants share understandings about what they are doing and what it means for their lives and communities (Cox, 2005). A community of practice denotes a group of people, whether physical or virtual, that have shared certain competence that every member must identify with. Competence in the context of the study is part of the undergraduate students of the case university given factors such as educational qualifications, a registered student of the case university, age, and social status, including religious affiliations. Competence provides members with the qualifications for identity, enhancing mutual taken-for-granted and almost entirely informal engagements among members. Thus, it is argued that learning is a social process among members of a particular community of practice rather than an individual situated around cultural and historical context (Cox, 2005; Li et al., 2009). Community of practice does not mean a team, given that a team has a target they must achieve. In a team, the target can be monitored and influenced by those who coordinate and control team activities (Farnsworth et al., 2016). Members of a team must agree. However, a community of practice is not a community of agreement (Li et al., 2009). A community of practice involves people who voluntarily become members, given that they possess the shared competence that glues

the community together. Members move into or out of the community without being forced. Moreso, each member has the chance to change the competence of the community with new ideas or be changed by the community.

Competence evolves if there is an element of joint enterprise or domain (Li et al., 2009), engagement, and shared repertoire (Wenger, 2000). These three concepts are the ingredients for developing competence within a particular community of practice. Domain is a concept used to describe the area where a community claims to have the authority to define competence. Whereas a team is a task-driven partnership characterized by a shared goal, a community of practice is a learning partnership enabled by a certain domain of practice (Li et al., 2009). In this study, the domain of practice of the research participants is the university, which provided them with an enabling environment to connect and enhance new practices. The domains include the various activities the students engage in with other members of the same community and the connections in classes, hostels, events, and many other related activities. It is pertinent to note that a community risks the danger of non-existence if there are no elements of events, leadership, connectivity, memberships, projects, and artifacts (Wenger, 2000). This has led to the development of smaller communities of practice from the broader one. When the domain of practice is enabled, mutual engagement becomes at the center of any community of practice. Members of the community of practice build the community through mutual engagement with one another (Wenger, 2000). Mutual engagement has been equated with network establishment in the work of (Li et al., 2009).

For a community of practice to exist, there must be interrelationships among people in physical or virtual contexts. The possibility for people to share their everyday life in virtual contexts has been underscored in the extant literature (Spracklen, 2015; Zhao, 2004) and confirms the possibility that a community of practice can exist online. Interrelationships enable the community to share experiences and negotiate competencies and meanings. Members interact, resulting in the mutuality of norms and social connections in situated contexts. Competence in a community of practice is demonstrated by the ability to interact with the community and be trusted as a participant in these interactions. In the study's context, mutuality has been established, given that most activities in the community involve collective effort. Students have been grouped into classes, hostels, collective events, and community-based projects. These have collectively made the earlier strangers develop into a community with similar interests and styles of action and behavior. After the institution of mutual engagement among members of communities of practice, the next concept is shared repertoire. Shared repertoire involves producing communal resources (Wenger, 2000) needed for every community member. Thus, members develop communal resources such as community tools, artifacts, language, routines, etc. To fit in, members must know how to operate these shared repertoires appropriately. In our study, the shared repertoire is embedded in the collective engagement of students in most of their activities at the university. They mainly eat together, play together, read within a confined space that serves most academic activities in the university, sleep in the same domain, and or spend most of their time together if they do not live on the campus, which develops into normal routines within the community. All these ganged up to develop the competence the students see themselves as. This competence is being undergraduate students with the same social and academic status. Thus, a community of practice evolves out of the "convergent interplay of competence and experience that involves mutual engagement. They offer an opportunity to negotiate competence through an experience of direct participation" (Wenger, 2000, p. 229).

3.0 Methodological assumptions

We adopted the qualitative research design. Elliott & Timulak (2005) state that qualitative research permits researchers to seek verbal narratives or descriptions in words and also attempts to convert observation into words. We employed the deductive research approach. Deductive research allows researchers to collect data based on propositions in formal theories and theoretical perspectives. Hassan et al. (2018) argue that deductive reasoning allows the use of existing knowledge, usually in the form of theories, to serve as the basis for developing new theories and models or testing existing theories. The philosophy adopted in the study is the interpretivism paradigm. Interpretivism holds that human knowledge of reality is only held through social construction and humans understand a phenomenon from the meaning people ascribe to it (Klein & Myers, 1999). The paradigm enables researchers to view research participants' underlying social behaviors and actions as situated and embedded in taken-for-granted social contexts (Utulu & Ngwenyama, 2017). This implies that we view the underlying behaviors and actions that may render universities vulnerable to cyber security attacks as socially constructed and embedded in the case university. The method adopted is the interpretive case study. The interpretive case study enables researchers to understand phenomena from the viewpoint of the participants directly involved with the phenomenon under study (Cavaye, 1996). We used semi-structured interviews and participant observation to collect data from undergraduate students in one of the three universities in Adamawa state, Nigeria. Walsham (1995) argues that interviews are an essential data source in conducting interpretive case studies because they allow researchers to step back and study the interpretations of their fellow participants in-depth.

We adopted the convenient sampling technique to select the case university, given that it enables us to choose research contexts without credence to complex statistical requirements used to validate the selection of cases in positivism-based case studies (Alvi, 2016). We adopted the snowball sampling technique to select the undergraduate student that took part in the study. The snowball sampling technique was considered relevant given the need to sample participants within different communities of practice. The snowball sampling technique occurs when study participants lead a researcher to participants that they feel are relevant to achieving the objectives of the research study. We adopted the thematic analysis data analysis technique, which involves identifying, analyzing, and reporting patterns inherent within the research data collected for a study. The thematic data analysis technique focuses on discovering and making sense of themes inherent in raw qualitative data and helps researchers describe data in rich detail (Braun & Clarke, 2006). Many scholars, including Guest et al. (2012) and Utulu & Ngwenyama (2021), have adopted the thematic data analysis technique. The Atlas Ti software was used to facilitate the thematic data analysis procedure. To adequately and appropriately carry out the thematic data analysis technique in the study, we transcribed and typeset recorded interviews into Microsoft Word documents, printed them, and read them several times. Multiple readings allowed us to familiarize ourselves with the material and organize the interviews into themes that showed the behaviors and actions of the study participants, providing the possibility of coming up with a social-ethical hacking framework. We also read data from field notes multiple times to develop pertinent themes that we used to supplement narratives obtained from the in-depth interview themes. We grouped and used similar themes to create variables that helped us to develop the social-ethical hacking framework proposed in the study.

We completed the study process in the empirical situation for six months. Before the study, one of the researchers had contact with the university. He served in the research context for more than a year. The researcher was instrumental in gaining access to the university and also helped minimize the efforts required to gain participants' confidence and agreement to participate in the study. We got official permission to carry out the study from the case university. During the study, we observed the day-to-day activities of the undergraduate students in the case university. This afforded us the privilege to identify and understand the communities of practice within the study context and how the communities of practice impact social behaviors and actions that promote cyber security threats and, in effect, could be used to come up with a proposed social-ethical hacking framework. We observed how the students used their mobile phones in different locations across the research context. The locations include the students' center, classes, library, cafeteria, bus stops within the university, snacks bar, etc. We also got involved in informal and formal discussions on issues related to how the students' communities of practice impact the behaviors and actions they enact and how these can promote cyber security threats and their daily activities. In all, we conducted twenty-one interviews. We recorded the interviews using mobile phone-based recording devices. We recorded all the interviews, given that the study participants agreed that the interviews could be recorded. We used field notes to record our observations during the participant observation. Before the interview, we explained to the participants that they might participate or withdraw from the study whenever they chose to. We also made participants fill out and sign consent forms.

4.0 Presentation of Study findings

The objective of the study is to assess and understand the everyday life practices and actions of undergraduate students at the case university. We assume that assessing and understanding undergraduate students' everyday life practices and actions, particularly touching on how they use cyberspace, will likely enable us to propose a social-ethical hacking framework. The social-ethical hacking framework will help detect and manage human factors that enhance cybersecurity vulnerability in universities and other similar organizations. The study defines social-ethical hacking as a variation of ethical hacking. Its objective is to underscore and test human behaviors and actions that make universities vulnerable to cybersecurity threats. In this segment, we provide the data gathered through the interviews and participant observation of students' everyday life practices and cyberspace use. The study findings reveal how human factors make universities vulnerable to cybersecurity threats due to undergraduate students' everyday life practices and the use of cyberspaces. The findings also reveal how the human factors evolved and become taken-for-granted within the communities of practice undergraduate students formed in the case university. The study reveals how concepts underpin the community of practice theory, namely, competence, domain, mutual engagement, and shared repertoire, provided the basis for explaining the ways undergraduate students' everyday life and use of cyberspaces lead to cybersecurity vulnerabilities. We present the findings below:

4.1 Competence and Cybersecurity Vulnerability

Competence in the context of the study includes factors such as educational qualifications, age, and social status. These attributes of competence made it possible for the study participants to be enrolled as undergraduate students in the case university. In the research context, religion is also a critical attribute of competence as it determined to a large extent the clichés of communities of practice that existed within the study context. The study findings show that most participants have

no connections with people outside their families. They were young people aged between 16 and 19 whose life revolved around staying indoors at home when they were not on campus. Their religious affiliations also played a crucial role in their restricted movement at home.
On the university campus, they easily identified and made friends with other students with whom they shared competence. This made them easily trust one another as undergraduate students and establish communities of practice. The acquaintances on campus and the demands of their everyday life as undergraduate students transformed them into various communities of practice. The communities of practice flourished because it allowed them to connect around mostly informal activities (friendship) and, on some occasions, activities connected to their studies. They, however, enacted the activities in physical and cyber contexts. This is evident in the interview with Participant 3 "*My friendship with my friends ends in school. I do not have friends at home. It is only my sister*…." Participant 3 position implies how conditions on campus provided him with the social context to belong to any evolving communities of practice. The community of practice provided him with the grounds to negotiate a unique identity on campus.

Participant 1's claims also show how contexts on campus provided the opportunity for the formation of different communities of practice in the research context. He posits that "*at home, I always sleep, watch movies, play video games. I do not go out unless if I want to go and pray. That's all I do and by 4 [4:00 pm]. That's all, I don't use to see my friends and my area is quiet already (sic)".* Participant 2 stated that *"…there's nothing much to do after going back [home]… I spend most of my time in school."* Participant 2's claim resulted from the non-existence of opportunities to interact with friends at home and how everyday campus life enabled him to make friends. It is important to note that it is not only the availability of people to befriend that resulted in the ease of forming communities of practice on campus but also the social challenges of learning, living out everyday life realities, and the social contexts that were on campus. Competence determined the category of people on campus, the social challenges they are likely to face, everyday life realities, and the nature of socially constructed contexts. The socially constructed contexts were also influenced by competence factors, including study participants' culture, religion, and tribe. The study participants were conscious that their status as undergraduate students was the primary competence factor that enabled them to become members of communities of practice in the case university. Competence factors, including tribe, religion, and sometimes social status, also played vital roles in determining their membership in communities of practice. We observed that groups of friends of about four to seven were formed mainly based on tribe, culture, and region. In other words, participants seem to develop close friendships with those that share the same culture, religion, and tribe. This also manifested in the ways they dress and the kind of conversation they want to participate in.

Participants who wore religiously-themed clothing were closely related and bonded. This is also the same with participants whose dresses are regarded as socially 'indecent.' The study participants' socio-cultural and religious ideologies influenced the communities they are likely to form or belong to. There were times, however, that the participants transcended the socio-cultural and religious boundaries to create communities of practice based on the reality that they were enrolled in the same academic programme. Enrollment in the same academic program, therefore, becomes a very crucial attribute of competence. Academic and school issues determined friendship, intimacy, and bonding under this circumstance. Irrespective of the attribute of competence that is in play, shared history, informalities, and social learning and knowledge sharing in situated

contexts led to the emergence of communities of practice in the research context. It also made the undergraduate students exhibit similar behaviors that could expose them and the case university to cybersecurity threats. The study findings revealed two types of activities enacted by all the undergraduate students due to competence. First, they use their mobile phones more for non-academic activities than academic ones. For example, Participant 5 stated: *"I use my phone even in class because some classes are boring."* Our observations of the study participants show that most of them used their mobile phones for social activities than for academic activities. Our study findings show that the study participants mostly use their mobile phones for social media. Social media uses that are prevalent among them include chatting with friends, sharing and watching short videos, and sharing and viewing photographs uploaded on social media. Participant 6 posited that "*…I communicate with my friends via phone call, or through social media, or search something on the internet"*. Also, participant 8 shared how social media became part of her routine. He stated, "*Most times, I go on social media with my phone…"*. Participant 9 concurred that *"...I chat. I normally do Instagram, WhatsApp, Snapchat, etc. I browse mostly on my phone..."* Similarly, participant 19 said, *"Most of my social activities are online, yeah. I chat with my friends, family, my girlfriend, etc. I'm on every social media platform. I use it. I do not post, but I watch a lot of things online. I can't do without [the] internet"*. Information on how cyber attackers capitalize on the number of people that use social media. Through social media, attackers might be waiting for one mistake to attack a system or organization. Supporting the above assertion, participant 19 said, *"...I learn how to break a password, hack into somebody's computer, learn how to fix it. I just like. I mean things I cannot tell you exactly, it can be done on social media"*.

The students also use their mobile phones to watch movies, download movies, play online games, and do online business/shopping. This has been evident in the interview sessions held with the participants. Participant 6, for instance, revealed that *"Sometimes I download [academic] files from the canvas. Sometimes downloading series and movies, I used to think about virus because it is always there when you are downloading…. I do play games. I mostly download them, because I mostly spend most of my time playing them. I hardly spend time on social media"*. Participant 7 also said, *"I play video games online and offline."* Participant 8 shared that *"...I occasionally play a game called 'call of duty. It is a video game. I usually go to my friend's room to play it. Most times, I go on social media with my phone. I search for materials. I download movies"*. Students do all these non-academic activities that could expose them to cyber security threats.

It feels okay to know that some of the activities that the students do are academic activities. However, educational materials downloaded on the internet might not be free from threats capable of undermining the individual's cyber security and the institution's. Participant 9 said, "*I mostly use the internet for academic purposes. I do assignments. Like right now I am doing my project"*. Participant 17 said, *"So, I use my phone to read because I read many novels. Yes, and I write also. And then I access them offline. There is an app you download, and then that app gives you free books to understand. So, I read on it, and sometimes I write"*. This is evidence that the students use some of their time online to check for academic information. However, they seem not concerned about what sites they follow and what are the implications of their actions. In this regard, participant 19 buttressed the point further, "*I can make you download an app, make you download it, or I borrow your phone. I download the app without you knowing and as it is holding your phone every password that you ever put captures it*". Attackers might take a long time spying on

one's favorite activities. They hit them where they least expected—for example, downloading apps without considering the implications.

The study findings show that unique patterns of action among the study participants could expose them and the case university to cybersecurity threats. They mostly get involved in social and non-academic activities and not educational activities, even though the IT infrastructures in the case university were put in place to support and enhance their learning. A critical assessment of how study participants' everyday life activities unfolded in the case university, as revealed above, establishes the notion that the concept "practice," which is one of the concepts of the community of practice theory, evolves uniformly among the study participants due to their shared competence. It is evident in the study findings that everyday life practices among the study participants, particularly regarding how they used their mobile phones and what they used them for, have been institutionalized. Observation shows that most students use their phones for social media and other non-academic uses during classes. They do this with the university's Wi-Fi or subscription-based internet services, which they pay for with their own money. The bottom line is that the study participants have taken it for granted that it is right for students to use their mobile phones for social media and other non-academic purposes during classes.
Consequently, they unconsciously get involved with activities that may expose them and the case university to cybersecurity threats. Although some of the study participants indicated that they were aware that hackers could attack at anytime, they did not see their use of mobile phones where they should not be used, particularly during classes, as avenues that hackers could capitalize on. Participant 19, for instance, opined that *"hackers use emotions to attack their prey*." He stated, *"So, I feel the social closeness, the sharing of computers [that students do]"* exposes them to cybersecurity threats. Despite this assertion, the study participants did not indicate that people within their communities of practice could pose cyber security threats. Our observation showed that students fall for social tricks such as love, pity, and empathy, among others.

Moreover, one interesting thing about these findings is that the study participants did not exercise any care on how they allowed members of their communities of practice to access their mobile devices. The trend is reinforced among the study participants by competence being undergraduate students at the university, studying in the same department and courses, and sharing the same cultural, religious, and tribal backgrounds. Study participants seem to easily allow those that belonged to the same communities of practice the privilege of having unchecked access to their mobile devices. To them, it seems okay, but to cyber security-aware people, it seems weird. Thus, it exposes them to a variety of cyber security threats. This has been established in the interview with the participants. Participant 3 states, *"I have a password on my phone. Yeah, but all of my family members and friends know my password. I don't mind".* Also, participant 9 has the same experience, *"My friends access my phone, especially my best friend. She is not in this school. I have a password on my phone. [if they want to use it], I unlock it for them. Even when I open the phone for them, and they mistakenly let it close, they have to wait for me to return and open it for them because I don't share my passwords with them".* Although the person was trying to put some restraints on the access, the participant failed to understand that attackers might not need your password to attack. They might use social closeness to gain access to the phone and strike in the least expected time. A careful look at these quotations shows a pattern of actions among the participants. This is evidence that the participants are working toward negotiating competence among their members.

4.2 Domain and Cybersecurity Vulnerability

Domain is another important component in the community of practice theory that plays out in everyday life experiences and practices of study participants. Domain also provided avenues for understanding cyber security threats and developing a social-ethical hacking framework for identifying and managing them. Competence enables members of communities of practice, in the case university, to develop enabling environments where their everyday life experiences and practices are situated. Although competence leads to the formation of domains as explicated in the community of practice theory, domains are situated contexts and competence playout within them. This domain of practice could be physical or virtual. In the context of our study, we observed that most academic and social activities were done in the case university's library. This has made it easier to set up different domains, including the library, students' residence, and a multipurpose hall for sports and other social activities. Most students carry out their academic activities, including classes, reading, relaxing, socializing, and partaking in special activities. Special activities include participating in writing classes, meeting with advisors, and group-based learning in a private meetings and reading rooms in the library. Sitting arrangements in the library indicate that the university deliberately promotes collective and group learning among the students. The implication is the development of clichés of communities of practice with more specific competencies. For example, participant 1 said that *"It depends on what I do if it's YouTube, sometimes I use [university's] Wi-Fi because this [the library] is the only place I can say [the Wi-Fi] is fast… the ones in the dorm is not that fast."* Since study participants are usually in the library, the library serves as one of the major domains where their everyday experiences and practice play out.

Observation confirmed that the university's internet is faster in the library than in every other domain, including students' residences. It follows that this may have been done deliberately to force students to use the library more than they want to use their residences. The 'forced' use of the case university's library may have been implemented to increase the time study participants spend dealing with academic and learning-oriented uses of the internet. If this played out as expected, the library as a domain would have provided the avenue for competencies such as membership in the undergraduate body, academic departments, and courses to play out. Unfortunately, competence such as culture, religion, and tribe evolved and were used to establish clichés of communities of practice. Aside from this, observation shows that study participants also used the library more for non-academic purposes, both on the internet and physically. This outcome shows how crucial competence is to the formation of communities of practice. It follows that most activities the study participants socially constructed could expose them and the case university to cybersecurity threats were mainly carried out in the library. This also shows how communities of practice, though informalities, history, and shared situated contexts, socially construct the domains where members experience their everyday life experiences and practices. Over time, due to shared experiences, study participants took for granted actions and behaviors that exposed them and the case university to cybersecurity threats. For example, observation recorded in our field notes shows how study participants carelessly drop their mobile devices on tables, chairs, and other furniture in the library. During the cause of the study, we observed that study participants also left their mobile devices in the care of other members of their communities of practice without second-guessing that they could be threats to their cybersecurity. The fact that there were no close circuit television cameras in the case university library also indicates that study participants risk losing

their mobile devices to thieves and people who pose cybersecurity threats. It follows that study participants felt comfortable and secure in the library and were usually around members of their communities of practice. The domain provided them with the avenue to develop habits allowing others un-checked access to their mobile devices despite the devices containing sensitive information and providing access to the case university's internet network and virtual resources. This behavior provides avenues for impersonation, stealing personal data, distortion of information, and access to personal academic, financial and other records.

Participant 18 narrated a scenario in the case university where a student was caught hacking into the university's network using another student's user name and password. The outcome is that the student whose account was used paid for the damages. According to Participant 18:

> *"They [the case university] traced it down to the room number and cut the person (sic). They caught the student, but he said he was not the one, but the hacker used his laptop. They asked him who used his laptop, but he said no one. So, they started believing him and keeping a close eye on him. Later, he reported that his friend used his laptop at night around 1 am, and he returned it after some days. When they investigated, they found out that the friend was the TKN. They found from the laptop that the meaning of TKN is 'The Knight King' [a term derived from the film] game of thrones."*

The scenario above is a typical example of why mobile devices are not supposed to be kept with anyone, irrespective of membership in communities of practice. Another scenario was provided by participant 19:

> *"I got close to those people that I have to fix their computers (sic). I got close to them. And you know they trusted me in their mind. They were like, okay. He wants to set up my computer, so it does not matter that I give him my email and my password. So, that is it. I now create the email address on their computer, you know to set up. Now you know Windows 10… Users unintentionally fall for such…"*

Scenarios provided by Participants 18 and 19 indicate why close friends, including those with membership in the same community of practice, should second guess their trust in one another. The scenarios show that trust is a significant cybersecurity factor.

4.3 Mutual Engagement and Cybersecurity Vulnerability

Mutual engagement is another concept of the community of practice theory. Mutual engagement has to do with members of communities of practice establishing a mutual relationship with one another. Competence and domain provide an avenue for the evolution of mutual engagement among members of communities of practice. Mutual engagement evolves, given the existence of competence and domain. And unless there is mutual engagement among the members of communities of practice, it will be difficult for communities of practice to exist. The social learning and knowledge sharing that characterize communities of practice are made possible by mutual engagement. Observation done in the cause of the study shows how study participants engaged in a mutual engagement at different levels. For example, most academic activities in the school involve mutual engagement. Observation shows that study participants rarely engage in individualized learning activities. It follows that group-based learning culture is entrenched in the case university. Study participants were frequently involved in group-based take-home assignments and social activities, including group sports and social activities.

Aside from academic-based mutual engagements, study participants also engaged in mutual social engagements. Study participants share highly personal everyday life experience and practice with members of the communities of practice they belong to. Some share information about their love relationships, relationships with parents and guidance, love affairs, and other related personal activities. For instance, Participant 5 reveals: *"Like among us, if they've got problems with their boyfriends…in school, they just called me and asked me. They can share anything with me, be it school or personal activities."* Participant 5 surprisingly points out that *"I have access to their phones. But for me, only one can access my phone. They can at least access some of my phone activities, but not what I do like chatting or anything regarding that."* This type of behavior is rampant among study participants. Some students take up leadership responsibilities and tend to take them far beyond expectation. Aside from the cagy behavior resulting from trust gained by acting as a caring leader, study findings also showed that study participants got involved in mutual engagements by relying on members of the communities of practice they belonged to who had technical capabilities to repair mobile devices. Participant 19 provides a narrative of how he plays this out. He said he makes friends with students to access their electronic devices, and if this is difficult to do, he uses his technical skills to cajole them into trusting him. His claims: *"I got close to those people that I have to fix their computers. I got close to them. And you know they trusted me in their mind. They were like, okay. He wants to set up my computer, so it does not matter that I give him my email and my password. So, that is it. I now create the email address on their computer, you know to set up. Now you know Windows 10… Users unintentionally fall for such…".* While mutual engagement might help enhance learning and knowledge creation and sharing among members of communities of practice, it also provides unintended avenues for culprits to carry out activities that pose cybersecurity threats.

4.4 Shared Repertoire and Cybersecurity Vulnerability

Shared repertoire stands for the unique languages, norms, values, meanings, and practices, which otherwise could be termed social fabrics, that distinguish a community of practice. Shared repertoire evolves within communities of practice given competence, domain, and mutual engagement. Members of communities of practice develop and take for granted shared languages, norms, values, meanings, and practices that become peculiar to the community of practice. The shared languages, norms, values, meanings, and practices serve as bonds in communities of practice. Members of communities of practice remain part of the communities in as much as they continue to the social fabrics. The role shared repertoire plays in the evolution of communities of practice was established in the study. Observation carried out during the cause of the study shows that each community of practice, in the case university, had a shared repertoire that they used to distinguish members from non-members. Shared repertoire determines those with access to information, experiences, and knowledge and the meanings ascribed to the information, experiences, and knowledge within communities of practice. For instance, the practice that made study participants keep their mobile devices unchecked has become a norm in the communities of practice. This is the same with allowing friends to use their mobile devices unchecked. Most practices we observed as potential cybersecurity threats have evolved into norms whose meanings are perceived positively and hence, not seen as potential cybersecurity threats. We also observed practices connected to the use of mobile devices for internet access which members of communities of practice in the case university value and ascribe positive meanings to even though the practices were potential cybersecurity threats. These were mainly connected to the use of social media, downloading internet-based applications, videos, and audio files and games. We observed

that shared repertoire was made up of practices that have been institutionalized given their historical antecedents, informalities, and situated nature. The practice of enacting social activities more than academic activities in the university library had been taken-for-granted and rooted in the study participants' everyday life experiences and practices. Study participants enacted social engagements in physical and virtual spaces, watched films downloaded on their mobile devices and directly from the internet, communicated with friends through text-based and video-based chatting, accessed banking services, and other online-based engagements within the library. During the interview held with Participant 6, he revealed that: *"Sometimes I do bank transactions. Sometimes I download files from the canvas. Sometimes download series and movies while in the library and classes."*. Participant 17 posits that: *"The only time I use it is maybe my laptop is dead, and I have to use my phone for my canvas work or something like that. And then I use my phone and maybe communicate to some people I know that are into something like this."* Participant 17 further noted, "*There's an app you download, and then that app gives you free books to understand. So, I read on it, and sometimes I write."* One of our participants is into coding and hacking people's computers and mobile devices. He stated thus, "*Some people can hack through iPod. Yes, sometimes I can send you a spam file. So, I can make you download an app, make you download it, or I borrow your phone. I download the app without you knowing, and as it is holding your phone, every password that you ever put captures it."* The claims derived from interviews as exemplified above reveal the taken-for-granted norms and practices of using internet and Wi-Fi resources provided by the case university in ways that pose cybersecurity threats. Participant 19 claimed, *"So, I feel the social closeness, the sharing of computers [that students do] expose students to cyber threats.* Given that the shared repertoire had been institutionalized, the study participants seem not to know the cybersecurity risks they exposed themselves to.

5.0 Theoretical Elaboration of the Study Findings

The study aims to understand undergraduate students' everyday life experiences and practices to develop a social-ethical hacking framework. We consider the social-ethical hacking framework necessary for contemporary organizations because it has been underscored in the extant literature that human factors pose more dangerous challenges to cybersecurity than technical ones (Abawajy, 2014). Consequently, the social-ethical hacking framework is expected to provide organizations with the framework required to understand and manage social factors that pose challenges to organizational cybersecurity. Social-ethical hacking is the direct variation of ethical hacking, primarily based on assessing and testing the strength of organizations' cybersecurity based on technical factors (Farsole et al., 2010; Hartley, 2015). The study used the community of practice theory as the lens to understand human factors and how to come to bear on the social factor-oriented cybersecurity challenges organizations face. The community of practice theory outlines competence, domain, mutual engagement, and shared repertoire as the key factors that come to bear in the evolution, over time, of communities of practice (Farnsworth et al., 2016; Wenger, 2010, 2011).

5.1 Competence and Cybersecurity Vulnerability

Competence has helped us generate certain behaviors that students exhibit, making them prone to cybersecurity threats. Understanding competence, domain, mutual engagement, and shared repertoire helped our study understand that students do educational and non-educational activities

that could expose them to cyber security threats. Although the two concepts might seem relevant, attackers can be snipping through social context to achieve technical hacking. Many studies have used community of practice to enhance collective learning rather than individualistic learning. Studies on how the community of practice helps provide complex explanations regarding learning have been underscored in the literature. Community of practice has helped generate an understanding of how online CoP can enhance teaching productivity (Wang & Lu, 2012), promote virtual learning environments (Ellaway et al., 2004), and enhance learning among therapists' communities (Hoffmann et al., 2011), establish an online community of practice to enhance student-teachers learning (Hou, 2015), and many other efforts. Each of the studies has specifically identified how they view competence and how it was critical to the success of the online community of practice. For example, Wang & Lu (2012) has not explicitly identified the competence of their study. However, it was implied as teachers who teach the same subject. This has helped in the establishment of the community. It has proved invaluable to the existence of the community and to promote collective learning. Ellaway et al. (2004) identified their competence as pre-existing students, teachers, and support teachers grouped under a particular course. The competence needed to qualify as a community member is being a student, tutor, or supporting staff. This has helped develop a virtual learning environment framework to enhance learning among members of the community of practice.

Hou (2015) has established final year students as the competence needed to qualify for participation among group members. This has helped them develop the community and shape the students' perception of the high possibility of learning within the online community of practice. Our study has tried to use community of practice to understand how students' everyday life practices and cyber activities contribute to developing a social-ethical hacking framework. Our study was able to stress the role that competence of undergraduate students plays and results in the enactment of behaviors and actions capable of exposing them to cyber security threats. The finding of the study has revealed a pattern of negligent actions and behaviors that the study context enact, which make them prone to cyber security threats (S. C. A. Utulu, 2014). Also, a study conducted by (Gallivan, 2000) used a community of practice to determine technology usage among employees in an organizational setting. However, the study has not provided evidence for how the principles of the community of practice played a crucial role in understanding technology usage. At the same time, competence is the key driver to the three concepts mentioned above, given that it is the competence that negotiates community, practice, and domain of practice (Farnsworth et al., 2016; Smith et al., 2017). Thus, one of the key contributions of this study is the explicit recognition of competence as key in a community of practice and how it oscillates between domain, mutual engagement, and shared repertoire and its impact on the taken-for-granted actions and behaviors of people.

5.2 Domain and Cybersecurity Vulnerability

Another key concept in a community of practice is how members converge in a domain of practice to learn among members. This domain shapes how members contribute, speak, and behave with one another (Gherardi, 2009). Most studies that use community of practice have to first establish the domain of practice for the community of practice to stay. Although, domain is determined by the competence of the members of the community of practice. Some studies have viewed domain as a common vision, focus, and direction (Ellaway et al., 2004)**.** others have viewed it in terms of physical structure that enhances learning among members. For example, the literature has

established social media as a domain in which community of practice members of health care groups learns from one another (Gilbert, 2016). The authors emphasized how the domain created enhanced learning and the readiness to participate actively as a member of the community with Twitter as a domain. Similar to this effort is evident in the work (Yang, 2009). The author establishes the relationship between the critical reflection of student teachers and the community of practice. The study used a blog to serve as a domain of practice to understand the relationship. A positive outcome was realized. Students have found discussions on the blog with fellow community members relevant and helpful in time management, resource accessibility, and job deliverance. Another giant effort in enhancing learning through the domain of practice is evident in the work of (Hoffmann et al., 2011). The authors have established how members feel work has been much easier for them while trying to access materials and rub minds among a community of therapies. This is quite encouraging and in line with what domain is expected to play in the community of practice. Domain has also helped establish a student learning community by creating an online community of practice (Hou, 2015). Thus, the domain has helped in the generation of optimism about the establishment of the community and how members became ready to participate in the group. However, our paper used domain as a physical structure provided by the study context (the university), where students are made to do about 80% of their activities. Thus, this has enhanced knowledge sharing among the students and established similar patterns of actions prone to cyber security threats. This paper has contributed to the fact that the domain can determine the enactment of similar behaviors and actions prone to cyber security threats.

5.3 Mutual Engagement and Cybersecurity Vulnerability

Another great contribution of this paper is how mutual engagement proved invaluable for determining the enactment of actions and behaviors capable of exposing students to cyber security threats. Mutual engagement has been stressed in the literature as an important tool for chasing frustration among community members and establishing the benefits enshrined in the community of practice (Hou, 2015). Thus, studies engage members of the community of practice in a series of programs to familiarize them with the new learning environment and help achieve the aim of the study. Students have used mutual engagement to develop a virtual learning environment framework (Ellaway et al., 2004), enhance participation among therapies to share therapist information and experience (Hoffmann et al., 2011), and many other uses. Hoffmann et al. (2011)Hoffmann et al. (2011) used mutual engagement in the context of therapists through an online collaboration sharing information about therapy to enhance collective learning and generation of new experiences. This means advancing the course of therapists in discharging their responsibility even though they are dispersed across the globe. Mutual engagement has been explicitly and efficiently utilized in the work of Rogers (2000). The study used mutual engagement to enhance students' learning and help them establish an identity through workshops. This has proved invaluable as participants have shared how active engagement enhanced their learning capability. Mutual engagement has served as a ground for successfully sharing medical information among practitioners using Twitter (Gilbert, 2016). Mutual engagement has been used to establish virtual closeness among the participants and see how it enhanced their learning capability. This has helped in understanding how Twitter became a relevant domain to promote learning among the healthcare community. Mutual engagement has been stressed in the work of Yang (2009) as an important tool that helped identify blogs to promote student teachers learning. (S. Utulu & Alonge, 2012) is another example of work devoted to enhancing understanding of how mutual engagement induced through group-based learning resulted in expected learning outcomes

due to cooperative learning. The active participation has established a free flow of information to enhance the practice and to see the relevance of the community of practice in reducing teaching complications, enhancing sharing of information, discussing complex problems, and providing access to resources that are otherwise difficult to access. Mutual engagement helps generate the structure among the IT community of practice comprising senior and junior IT professionals (Squires & Shade, 2015). Although, the focus of the paper is tailored towards a fresh theoretical approach to cyber-security as a group phenomenon that is well suited to ethnography. This is an excellent effort at establishing the relevance of community of practice in the realm of cyber security. However, our study has made explicit use of community of practice and specifically used mutual engagement of the students to understand how their actions and behavior help establish a social-ethical hacking framework. While this study looks at cyber security broadly, our study narrowed the focus down to ethical hacking with a specific focus on social interactions influencing the enactment of actions and behaviors capable of exposing the students to cyber security threats.

5.4 Shared Repertoire and Cybersecurity Vulnerability

Shared repertoire is one of the components of a community of practice that is critical to the successful implementation of a community of practice. It is concerned about the shared norms, beliefs, languages, and practices that members of the community of practice do to maintain the competence inherent in their community of practice (Farnsworth et al., 2016). The literature has established how studies have applied Wenger's community of practice to understand online blended learning. However, it appears that most of the studies have either casually looked at the theory or adopted it but did not capture its actual meaning (Smith et al., 2017). Shared repertoire enables members of the community of practice to not only share resources among their members but also engage in developing the resources and renewing their relevance to the community of practice (Rogers, 2000). These resources might be tangible or intangible. In the literature, it was evident that shared repertoire results in forming shared points of reference and developing new ideas that might transcend the initial idea. In all the papers that discussed using the community of practice, specifically the domain, mutual engagement, and shared repertoire, only Rogers (2000) identified how shared repertoire played a significant role in his study. Most studies failed to identify how the principles of the community of practice play a role in the analysis of the studies. This assertion is similar to the claim made by Smith et al. (2017).

Their work has established that Wenger's theoretical assumptions regarding the community of practice form a complicated and rich theory that is difficult to comprehend and apply. As a result, the authors felt surprised to find only three papers (Brosnan & Burgess, 2003; Ellaway et al., 2004; Rogers, 2000) that provided practical implications of this theory among the definitive collection of 17 investigations from 60 publications they have analyzed. Brosnan and Burgess' research offered context for how the Wenger community of practice's core principles may be used to evaluate and guide the design and support of a Web-based continuing professional development course. Rogers' research provided guidelines and examples of how Wenger's mutual engagement, joint enterprise, and shared repertoire concepts may be used to establish cohesive communities in online learning settings. However, none of the above studies touched on how Wenger's community of practice can be used to understand behaviors and actions that could lead to cyber security threats. Albeit many studies on technology, none has considered using a community of practice to enhance the ethical hacking framework. Just like how Roger's study provided the guidelines for understanding how domain, mutual engagement, and shared repertoire can establish cohesive

communities in online learning settings, we used these three principles to develop an understanding of how a community of practice helps in generating actions and behaviors needed to develop an ethical hacking framework. Although (Duin, 2020) was able to conclude that social dynamics can be best used to develop a community of practice for cyber security resilience, the study was lacking in the use of a community of practice to develop actions and behaviors for enhancing ethical hacking. To the best of our knowledge, our study is the first to use the community of practice to develop the social-ethical hacking framework. The concepts of negligence, taken-for-granted actions, fear of missing out, and trust have been generated in our study as the actions and behaviors that could undermine the cyber security of the most sophisticated technical ethical hacking test. These concepts confirm the danger of the human enacted actions and behaviors that most organizations take for granted. Furthermore, we could generate these concepts through understanding students as a community of practice.

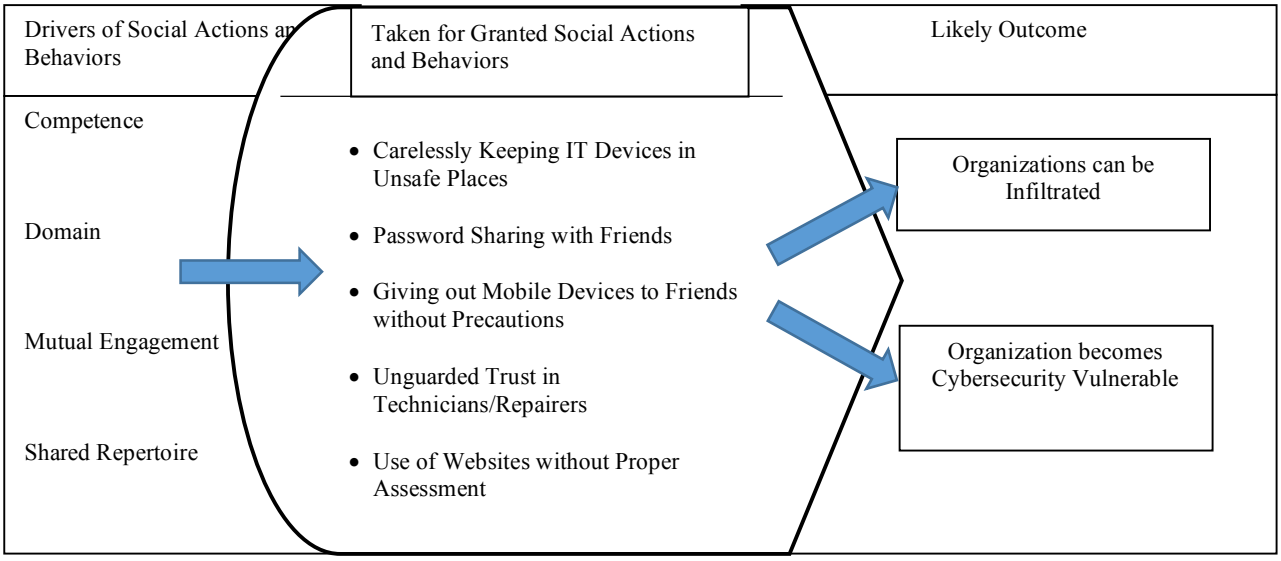

Figure 1: Components of Social Ethical Hacking Framework

The research proposes the social-ethical hacking framework to augment ethical hacking in detecting and protecting an organization's information security and the people in cyberspace. The

framework is aimed at assessing everyday social behaviors and the use of cyberspace that could expose organizations to cyber security threats. We used the community of practice theory to guide the development of the framework. The four elements of the theory are competence, domain, mutual understanding, and shared repertoire. These elements guide our understanding of how students' academic and non-academic activities could expose them to cyber security threats. The framework names the elements as the drivers of social actions and behaviors. They are the predictors of social actions and behaviors in context. The framework identifies the social actions and behaviors: Careless Handling of IT Devices, Password Sharing with Friends, Giving out Mobile Devices to Friends with Precautions, Unguarded Trust to Technicians, and Use of Websites with Proper Assessment. When organizational actors are fond of these social actions, they expose themselves to cyber threats. Meanwhile, their actions and behaviors can make the organization vulnerable to attack and can be infiltrated.

Careless handling of IT devices is a social behavior that takes place in a social context as a result of the existence of a community of practice. Our study has revealed that students have institutionalized leaving their IT devices with their friends while connected to the internet. The students do not mind giving their friends access to their PCs and handsets because of the trust they have for one another as undergraduates. The students also share their passwords with friends and family members because they think they have nothing to hide from them. Some do not give out the passwords, but they unlock their devices to their friends whenever the friends want to use their devices. It has also become a taken-for-granted behavior among the students to share the institution's Wi-Fi passwords because a password can work on multiple devices simultaneously. Another behavior that students take for granted is unguarded trust in technicians. Students give out their devices and share passwords with technicians in order to fix the devices for them. These actions provide the technicians with full access to the information and cyber resources of the students. These social actions and behaviors within communities of practice in organizations expose them to vulnerabilities and lead to infiltration.

6.0 Study implication

The study stems from the realm of information security. Specifically, the study aims to enhance the ethical detection of any vulnerability of vulnerabilities in organizations' systems. While many studies have provided an understanding of technical ethical hacking, this study has generated insight into the social context of ethical hacking. Our study was able to prove that these social factors can undermine the best cyber security protocol put in place in an organization. Thus, our study has practical implications. Organizations can deliberately enact these social behaviors among their social actors to detect the possibility of undermining their cyber security, provided that communities of practice have been formed within the context. Another implication of the study is developing a framework for social-ethical hacking. This framework is a move to strengthen the field of ethical hacking and to have an overall view of vulnerabilities leading to cyber security threats. Also, the study has theoretical implications. This theoretical implication is given that, to our knowledge, our study was the first to develop a framework for social-ethical hacking. Most studies have only implied the existence of social factors but have not gone further to explore them.

7.0 Conclusion and Limitations

Our study proved that social behaviors are the primary drivers of hacking success. While ethical hacking from a technical perspective is necessary, testing the social drivers leading to the hacking is quite necessary. The finding was able to identify the particular social intimacy that attackers create with their prey. Once you fall for it, it quickly turns serious. This is when we begin to use the famous phrase 'had I known. Thus, our study could answer how students' everyday life and cyber activities contribute to threats capable of undermining the operations of organizations. This is by developing a framework for organizations to use in detecting enacted actions and behaviors that employees exhibit that exposes the organizations to cyber security threats. The study has limitations. First, the study could only consider undergraduate students of a single university. Thus, the study considered a single case study to generate the framework. Other studies can explore multiple case studies to have a broader view of the phenomenon. The study also used interpretive research philosophy to explore the phenomenon. Other studies can look into other philosophical assumptions to generate a new understanding of the phenomenon. Having generated this framework, other studies can test the behaviors in another context to enrich the theoretical aspect of social-ethical hacking.

Reference

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Alvi, M. (2016). *A manual for selecting sampling techniques in research*.

Badamasi, B., & Utulu, S. C. A. (2021). Framework for Managing Cybercrime Risks in Nigerian Universities. *ArXiv:2108.09754 [Cs]*. http://arxiv.org/abs/2108.09754

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Brosnan, K., & Burgess, R. C. (2003). Web-based continuing professional development–a learning architecture approach. *Journal of Workplace Learning*.

Cavaye, A. L. (1996). Case study research: A multi-faceted research approach for IS. *Information Systems Journal*, *6*(3), 227–242.

Chakraborty, M., Chakrabarti, S., & Balas, V. E. (Eds.). (2020). *Proceedings of International Ethical Hacking Conference 2019: EHaCON 2019, Kolkata, India* (Vol. 1065). Springer Singapore. https://doi.org/10.1007/978-981-15-0361-0

Chhillar, K., & Shrivastava, S. (2021). *Vulnerability Assessment of University ComputerNetwork using Scanning Tools*. 13.

Cisar, P., & Pinter, R. (2019). Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical and Educational Sciences*, vol. 9. issue 4. ISSN 25605429. https://doi.org/10.24368/JATES.V9I4.139

Cox, A. (2005). What are communities of practice? A comparative review of four seminal works. *Journal of Information Science*, *31*(6), 527–540. https://doi.org/10.1177/0165551505057016

Crick, T., Davenport, J. H., Irons, A., Pearce, S., & Prickett, T. (2019). Maintaining the Focus on Cybersecurity in UK Higher Education. *IT NOW*, *61*(4), 46–47. https://doi.org/10.1093/itnow/bwz110

Csordas, T. J. (2008). Intersubjectivity and intercorporeality. *Subjectivity*, *22*(1), 110–121.

Duin, L. (2020). *Collaboration could improve cyber resilience: A Community of Practice approach in the Rotterdam port area*.

Ellaway, R., Dewhurst, D., & McLeod, H. (2004). Evaluating a virtual learning environment in the context of its community of practice. *Research in Learning Technology*, *14*(2). https://doi.org/10.3402/rlt.v14i2.11247

Elliott, R., & Timulak, L. (2005). Descriptive and interpretive approaches to qualitative research. *A Handbook of Research Methods for Clinical and Health Psychology*, *1*(7), 147–159.

Engebretson, P. (2013). *The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy* (Second Edition). Syngress, an imprint of Elsevier.

Farnsworth, V., Kleanthous, I., & Wenger-Trayner, E. (2016). Communities of Practice as a Social Theory of Learning: A Conversation with Etienne Wenger. *British Journal of Educational Studies*, *64*(2), 139–160. https://doi.org/10.1080/00071005.2015.1133799

Farsole, A. A., Kashikar, A. G., & Zunzunwala, A. (2010). Ethical Hacking Procedure 15, Sujay Nagar, Sewagram Road, Wardha. *International Journal of Computer Applications*, *1*(10), 7.

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*, *1339*(1), 012098. https://doi.org/10.1088/1742-6596/1339/1/012098

Gallivan, M. J. (2000). Examining workgroup influence on technology usage: A community of practice perspective. *Proceedings of the 2000 ACM SIGCPR Conference on Computer Personnel Research*, 54–66.

Gherardi, S. (2009). Community of Practice or Practices of a Community? In *The SAGE Handbook of Management Learning, Education and Development* (pp. 514–530). SAGE Publications Ltd. https://doi.org/10.4135/9780857021038.n27

Gilbert, S. (2016). Learning in a Twitter-based community of practice: An exploration of knowledge exchange as a motivation for participation in #hcsmca. *Information, Communication & Society*, *19*(9), 1214–1232. https://doi.org/10.1080/1369118X.2016.1186715

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). Introduction to applied thematic analysis. *Applied Thematic Analysis*, *3*(20), 1–21.

Hartley, R. D. (2015). *Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack*. *24*(4), 11.

Hassan, N. R., Mingers, J., & Stahl, B. (2018). *Philosophy and information systems: Where are we and where should we go?* Taylor & Francis.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102–113. https://doi.org/10.1016/j.cose.2017.10.008

Hawamleh, A. M. A., Alorfi, Almuhannad Sulaiman M, Jassim Ahmad Al-Gasawneh, & Ghada Al-Rawashdeh. (2020). Cyber Security and Ethical Hacking: The Importance of Protecting User Data. *Solid State Technology*, *63*(5), 7.

Hoffmann, T., Desha, L., & Verrall, K. (2011). Evaluating an online occupational therapy community of practice and its role in supporting occupational therapy practice: OCCUPATIONAL THERAPISTS' USE OF ONLINE FORUMS. *Australian Occupational Therapy Journal*, *58*(5), 337–345. https://doi.org/10.1111/j.1440-1630.2011.00954.x

Hou, H. (2015). What makes an online community of practice work? A situated study of Chinese student teachers' perceptions of online professional learning. *Teaching and Teacher Education*, *46*, 6–16. https://doi.org/10.1016/j.tate.2014.10.005

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, 67–93.

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber security awareness and education in SA. *South African Computer Journal*, *52*. https://doi.org/10.18489/sacj.v52i0.201

Li, L. C., Grimshaw, J. M., Nielsen, C., Judd, M., Coyte, P. C., & Graham, I. D. (2009). Evolution of Wenger's concept of community of practice. *Implementation Science*, *4*(1), 11. https://doi.org/10.1186/1748-5908-4-11

Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal of Cybersecurity*, *3*(2), 81–90.

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and implications. *International Conference on Cyber Warfare and Security*, 267.

Ovelgönne, M., Dumitraş, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *8*(4), 1–25.

Patil, S., Jangra, A., Bhale, M., Raina, A., & Kulkarni, P. (2017). Ethical hacking: The need for cyber security. *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, 1602–1606. https://doi.org/10.1109/ICPCSI.2017.8391982

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of Information Technology*, *35*(3), 214–231. https://doi.org/10.1177/0268396220918594

Pike, R. E. (2013). *The "Ethics" of Teaching Ethical Hacking*. *22*(4), 11.

Rogers, J. (2000). Communities of practice: A framework for fostering coherence in virtual learning communities. *Journal of Educational Technology & Society*, *3*(3), 384–392.

Sahare, B. (2014). *Study Of Ethical Hacking*. *2*(4), 5.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Schütz, A., & Luckmann, T. (1989). *The structure of the life–world. Volume II*. Northwestern University Press, Northwestern University, Evanston, IL.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know*. Oxford University Press.

Smith, S. U., Hayes, S., & Shea, P. (2017). A Critical Review of the Use of Wenger's Community of Practice (CoP) Theoretical Framework in Online and Blended Learning Research, 2000-2014. *Online Learning*, *21*(1). https://doi.org/10.24059/olj.v21i1.963

Spracklen, K. (2015). *Digital Leisure, the Internet and Popular Culture: Communities and Identities in a Digital Age*. Palgrave Macmillan.

Squires, S., & Shade, M. (2015). People, the Weak Link in Cyber-security: Can Ethnography Bridge the Gap? *Ethnographic Praxis in Industry Conference Proceedings*, *2015*(1), 47–57. https://doi.org/10.1111/1559-8918.2015.01039

Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties. *Journal of Cybersecurity*, *7*(1), tyab007.

Steinmetz, K. F., Pimentel, A., & Goe, W. R. (2021). Performing social engineering: A qualitative study of information security deceptions. *Computers in Human Behavior*, *124*, 106930.

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*, *63*(3), 382–412. https://doi.org/10.1080/10570319909374648

Tabassum, M., Mohanan, S., & Sharma, T. (2021). *Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework*. *2*(1), 14.

Tolbert, P. S. (1999). The Institutionalization of Institutional Theory: Studying Organization. *Theory & Method. London, Thousand Oaks, New Delhi*, *1*, 169–184.

Trabelsi, Z., & Ibrahim, W. (2013). Teaching ethical hacking in information security curriculum: A case study. *2013 IEEE Global Engineering Education Conference (EDUCON)*, 130–137. https://doi.org/10.1109/EduCon.2013.6530097

Utulu, S., & Alonge, A. (2012). Use of Mobile Phones for Project-Based Learning by Undergraduate Students of Nigerian Private Universities. *International Journal of Education and Development Using ICT*, *8*(1), 4–15. https://www.learntechlib.org/p/42296/

Utulu, S. (2014). Mobile Phone and Development: Synthesis on New Misuse Perspective. In H. Kaur & X. Tao (Eds.), *ICTs and the Millennium Development Goals: A United Nations Perspective* (pp. 101–125). Springer US. https://doi.org/10.1007/978-1-4899-7439-6_7

Utulu, S., & Ngwenyama, O. (2017). Rethinking theoretical assumptions of the discourses of the institutional repository innovation discipline. *African Conference for Information Science, Cape Town, South Africa*.

Utulu, S., & Ngwenyama, O. (2021). Multilevel analysis of factors affecting open-access institutional repository implementation in Nigerian universities. *Online Information Review*.

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems*, *4*(2), 74–81.

Wang, Q., & Lu, Z. (2012). A case study of using an online community of practice for teachers' professional development at a secondary school in China. *Learning, Media and Technology*, *37*(4), 429–446. https://doi.org/10.1080/17439884.2012.685077

Wenger, E. (2000). Communities of Practice and Social Learning Systems. *Organization*, *7*(2), 225–246. https://doi.org/10.1177/135050840072002

Wenger, E. (2010). Communities of practice and social learning systems: The career of a concept. In *Social learning systems and communities of practice* (pp. 179–198). Springer.

Wenger, E. (2011). *Communities of practice: A brief introduction*.

Yang, S.-H. (2009). Using blogs to enhance critical reflection and community of practice. *Journal of Educational Technology & Society*, *12*(2), 11–21.

Zhao, S. (2004). Consociated Contemporaries as an Emergent Realm of the Lifeworld: Extending Schutz's Phenomenological Analysis to Cyberspace. *Human Studies*, *27*(1), 91–105. https://doi.org/10.1023/B:HUMA.0000012246.33089.68

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 1–16. https://doi.org/10.1080/08874417.2020.1712269