Journal of Digital Educational Technology
2023, 3(2), ep2304
e-ISSN: 2752-5503
https://www.jdet.net/

Research Article

OPEN ACCESS

Key determinants and strategies for cybersecurity education in Yemen

Ismail Abdullah Hasan Humied [1]*

[1] Faculty of Police, Policy Academic, Ministry of Interior, Sana'a, YEMEN
***Corresponding Author:** dr.ismail_humied@yahoo.com

Citation: Humied, I. A. H. (2023). Key determinants and strategies for cybersecurity education in Yemen. *Journal of Digital Educational Technology, 3*(2), ep2304. https://doi.org/10.30935/jdet/13178

ARTICLE INFO

Received: 19 Mar. 2023

Accepted: 06 Apr. 2023

ABSTRACT

The availability of an education system capable of developing skills, and thus a trained workforce with cyber-competence, is a prerequisite for avoiding cyber-attacks on a country's critical infrastructure. Hiring foreign workers or outsourcing some operations is possible, but this is not a long-term solution and poses other problems. The available literature provides recommendations for creating a nationwide development, but little is known about the variables affecting the growth of ***cybersecurity education*** in developing countries like Yemen. Using data from 19 semi-structured meetings with academic officials from seven universities and academic entities, and then qualitative analysis these data, this article discusses the ***determinants*** of ***cybersecurity education***, and approaches to improve ***cybersecurity education***. To enhance current preparation, there is an urgent need for a national ***cybersecurity education*** strategy, which supports a number of initiatives and creates a multi-stakeholder space, where government, ***labor market***, and academia can actively work together to meet national ***cybersecurity education*** requirements. Also, there is needed to complete the preparations to promote research and development skills and cybersecurity ***awareness*** while enhancing educator training and academic cybersecurity programse.

Keywords: cybersecurity education, awareness, determinant, strategy, labor market, Yemen

INTRODUCTION

Due to the development of the internet, people may now enjoy both the real world and the virtual world (Lokman et al., 2019). With the advent of search engines such as Google and Yahoo, and video sharing sites such as YouTube, anyone can easily access information. However, the expansion of cyberspace can also harm Internet users, such as by encouraging crime. Therefore, such issues should be addressed promptly to prevent significant impact.

Cybersecurity education is essential because cybercrime incidents can occur anywhere, regardless of person, organization or location. Technical means that represent the joint efforts of the private and public sectors, local and international, aimed at protecting the national cyberspace, with a focus on ensuring the availability of information systems, strengthening privacy, protecting the confidentiality of personal information, and taking all necessary measures to protect citizens and consumers from the dangers of cyberspace, in addition to all legal frameworks and organizational workflow procedures, is the definition of cybersecurity. The ubiquity of various malicious activities has been highlighted in several recent cybersecurity attack reports, demonstrating the increasing sophistication of cyberthreats (Humied, 2022a). These dangers have a wide range of effects on international governments, organizations and people. A framework created to address cybersecurity issues at the national level highlights the need to develop cybersecurity skills to improve cyber preparedness. These theories identify development of development as an important prerequisite for the development of such talents. Addressing cyber challenges requires people who can detect and respond to cyber threats and protect critical infrastructure (Paulsen et al., 2012). As such, nations have devised ways to create critical human skills such as ***cybersecurity education***, training, and qualification. These tactics are aimed at addressing the current skills shortage.

Developing human capital requires the creation of operational and strategic institutions that are often lacking in underdeveloped countries like ***Yemen***. Recognizing the limitations faced by such countries is therefore an important first step in determining how cybersecurity can be developed. This study addresses ***determinants*** in ***Yemeni*** higher education system in ***cybersecurity education*** and explores development prospects through a qualitative thematic analysis of interviews with higher education leaders. These inquiries are addressed by this survey. What ***determinants*** do ***Yemeni*** universities face

© 2023 by the authors; *licensee JDET by Bastas, UK. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).*

in providing ***cybersecurity education***? How can supporting ***cybersecurity education*** improve the nation's cybersecurity capabilities?

Yemen's higher education system consists of both state-owned and private institutions. The country's education system has changed over the past decade. In order to assess, control and improve the standards of higher education, the government has created a regulatory framework (Academic Accreditation Council ***Strategy*** [AACS], 2022). The university closed in 2022 after a second evaluation revealed an absence of academic quality. Since 2022, the university has been revising and standardizing its academic he curriculum to comply with legal obligations. However, these initiatives are not directly related to training in cybersecurity methodologies and tactics. Instead, they focus on improving general education. Prior to 2020, information security education was included in the computer science, computer networking, and telecommunications curricula.

In the meetings, which was conducted for this study, several ***Yemeni*** academics assessed the country's current ***cybersecurity education*** system as inadequate. While some institutions are suffering primarily due to a shortage of teachers with the necessary skill, others have yet to start cybersecurity projects. ***Yemen*** needs to develop a national ***cybersecurity education strategy*** to guide cyber ***labor market*** growth in the short and long term. The rest of this article consists of seven sections: Literature review section addresses related work. Research methodology section describes the research method employed. Perceptions on cybersecurity section presents respondents' perceptions on cybersecurity. ***Determinants*** of current ***cybersecurity education*** and training section explains circumstances ***determinants*** of ***cybersecurity education*** in the nation. Discussion section discusses research findings. Approaches to improve ***cybersecurity education*** section introduces strategies for improving ***cybersecurity education***. Conclusions section offers some concluding observations.

LITERATURE REVIEW

Several aspects of ***cybersecurity education*** were addressed as part of the research. In particular, it focuses on education, workforce development, and national capacity building methodologies. US Department of Homeland Security, US National Institute of Standards and Technology (NIST), US National Security Agency, UK Government Communications Headquarters, United Nations, European Union, and SANS Institute, a think tank such as RAND Corporation and Booz-Allen Hamilton, among others thoroughly documents all issues related to cybersecurity expert shortages and remediation strategies. Despite this, the number of research papers specifically addressing similar issues in ***Yemen*** is modest.

The USA sees education as a key component of national cybersecurity readiness, so it has enacted legislation [1] and strategies [2] to improve ***cybersecurity education*** and ***labor market***. National Initiative for Cybersecurity Education (NICE) (NICE, 2010) was established to strengthen the US cybersecurity posture for the long term. NICE (2010) includes workforce structure, formal education, vocational training, and ***awareness*** raising. Created by NIST to support this program, national development framework provides standard vocabularies (terminology and taxonomies) for use by governments, the ***labor market***, and the academic community (Petersen et al., 2020).

The UK national program for safeguarding cyberspace has four main components, one of which is ***cybersecurity education*** and skills development (National Cyber Security Strategy, 2011). Cybersecurity is now part of education in the UK at all levels, starting with her 11-year-old pupils. For example, Open University provides resources. Other current methods include apprenticeships, undergraduate and graduate research funding, cybersecurity employment opportunities, internships, and support for schools (such as Girls Get Coding). According to a 2013 self-assessment (including conferences at academic institutions to identify barriers to program delivery), the current gap in cyber education should be closed within his 20 years (National Audit Office, 2013). Aury and Alfredo (2013) discuss whether and under what circumstances an undergraduate course in ethical hacking should be taught in Puerto Rican universities. Studies recommend combining ethics and ethical hacking courses for a bachelor's degree.

Lehto (2015) conducted a study in Finland, evaluating cybersecurity teaching and research at nine universities and research institutes, highlighting the methods and strengths of each. The results show that while ***cybersecurity education*** is developing in Finland, the system lacks strategic objectives. The university offers project-based education and cybersecurity research is supported by effective participation and solid structures. However, organizational education programs on cybersecurity do not predict national strategic capabilities. Harašta (2013) notes the absence of civic education on cyber risks in both the Czech Republic and Lithuania and compares the two countries with a focus on cyber law issues. European Commission's Tempus Project (TEMPUS, 2013) considered strategies for formal, non-formal and public education. Informal education focuses on professional development and subject-specific training, while formal education addresses a variety of ***cybersecurity education*** topics at institutions in the United States, Europe, Asia, and Australia. (e.g., supervisory control and data collection systems). ***Awareness*** and information campaigns include public education. The conclusions show that the United States, Canada, the United Kingdom, and Australia, which are at the forefront of cybersecurity:

(a) integrating ***cybersecurity education*** into all stages of academic education,

(b) ***cybersecurity education*** has close ties primarily to US political and security agencies, and

(c) gaps in both education sectors (formal and informal) and some countries have not started developing cyber education (TEMPUS, 2013).

[1] Border Patrol Agent Pay Reform Act of 2013, Federal Cybersecurity Workforce Assessment Act of 2015.
[2] Federal Cybersecurity Workforce Strategy (2016).

Table 1. Key elements of cybersecurity education

Education, research, & training	Influence variables: Absence of	Improvement strategies
Perceptions	Professionals	Regulation
Education	Participation	Skill
Curriculum	Resources	Programs
Provision	Awareness	Participation
Qualifications	Interest	Others

Kortjan and Von Solms (2012) found deficiencies in ***cybersecurity education*** in South Africa's national cybersecurity regulation, based on broad comparisons with US and the UK initiatives. Identifying milestones, allocating resources, and creating strategies to share responsibilities are some suggestions. To educate children and protect their online privacy, Von Solms and Von Solms (2015) offer them (social networks, etc.) a cybersecurity curriculum (based on videos). It is emphasized that some African governments are not necessarily investing as much money in this education project as wealthier countries.

The literature discusses multiple aspects of cybersecurity tactics and development, including cybersecurity practices, cyber education for children, and specific subject areas. ***cybersecurity education*** and ***awareness*** are two components of his national cybersecurity ***strategy*** for developing countries covered by Newmeyer (2015). Muller (2015) identifies areas, where poor countries struggle to improve their cyber capabilities. These include cooperation between the public and private sectors, knowledge expansion and institutional stability. Developing countries should consider their ability (knowledge and ability) to implement plans in a timely manner when adopting developed country strategies. The discussion includes a brief mention of cyber education as an important aspect of protecting cyberspace.

Organization of American States (OAS), Inter-American Development Bank, and Global Cybersecurity Capacity Center report on the current efforts of 32 Latin American and Caribbean countries in five cybersecurity areas. ***Cybersecurity education*** on online surveys and Oxford cyber capability maturity model[3]. A selection of notable educational projects is outlined for each country (Inter-American Development Bank, 2016). In summary, most of the linked research focuses more generally on high-income countries and emphasizes different elements of education as components of cybersecurity literacy development. For Finland and the UK, there is a national assessment of university-level ***cybersecurity education*** and research. The development of national cyber capability has been hindered by a number of specific problems, despite recent initiatives to address cybersecurity skills in less developed nations. So, the goal of this study is to better understand the ***determinants Yemen*** has when it comes to ***cybersecurity education*** and approaches to improve ***cybersecurity education***.

RESEARCH METHODOLOGY

In banking and other businesses in Yemen, people with CS background occupy a large part of the operational roles that address cybersecurity ***determinants***. To conduct semi-structured meetings, meeting guidelines were developed based on the main components shown in **Table 1**. A desk study was also conducted to find a suitable development path for Yemen, used in other countries.

Crosstabs have been added to the meeting to explore the following topics:

(a) cybersecurity ***awareness*** and ***awareness***,

(b) determinates of current ***cybersecurity education*** practices,

(c) ***determinants*** to initiation and improvement of ***cybersecurity education*** in institutions, and

(d) strategies that Yemen's education system may adopt.

10 universities and academic entities[4] were contacted in Sana'a city. One decline, nine agreed to participate, and meetings were successfully conducted at seven universities. In the remaining, while our requests for participation were initially accepted, subsequent communication attempts were ignored.

This purposeful sample corresponds to 60% of all ***Yemeni*** universities in Sana'a city offering degrees in cybersecurity and includes most leading educational institutions in the nation. In these institutions, 19 representatives of public (28.6%) and private (71.4%) universities were recruited in person (85.7%) and by phone (14.3%) during period between 2021 and 2023. **Table 2** presents respondents' academic background, role, and education.

The transcripts were thematically analyzed in accordance with conventional qualitative text analysis procedures. This method focuses more on an exploratory study to find patterns, themes, and categories crucial to the topic that was researched than it does on reporting statistical significance.

PERCEPTIONS ON CYBERSECURITY

At the beginning of each meeting, a short opening question was asked to assess how well-informed participants about cyber threats were and to get their views on the state of current cybersecurity practices. Considering well-known global data protection breaches and cyberattacks against local private and public infrastructure, for example, financial services phishing scams and hacking of government websites, cybersecurity is currently, is seen as an emerging problem of increasing relevance.

Respondents often made security decisions based on the effectiveness of their chosen authentication technology.

[3] Similar to capability maturity model integration (CMMI) for software development (see http://cmmiinstitute.com for more).
[4] In this article, 'universities' refer for both.

Table 2. Meeting respondents' profile

Characteristics	Number of respondents
Academic background	
Computer science	8
Telecommunications	2
Software engineering	1
Information security	1
Business administration	1
Education	2
Artificial intelligence	2
Networks	2
Role	
Professor	15
Dean	2
Chief	2
Education	
MSc	6
PhD	13

Respondents rated their agency's security as moderately poor (34%), moderately adequate (42%), adequate (22%), or completely adequate (2%) due to advances their agency has made in this area, including multi-factor, biometrics, temporary passwords, one-time passwords, out-of-band communications, SMS and email verification, and selective authentication[5]. Authentication technology not only acts as a deterrent against hostile actors accessing your network, but it also serves as a signal to your agency's security posture that can increase or decrease customer trust. Some respondents shared personal accounts of public and privately managed situations and highlighted questions about the adequacy of institutional homeland security. If so, I believe there are still some institutions that need improvement. For example, some universities continue to use virtual keyboards, which have proven useless in the presence of paperless recorders (Parekh et al., 2011). Improvements can be made in the following areas: Internal security procedures [respondent R29][6], advanced authentication techniques employed by smaller institutions [R19], and willingness to pay for security [R22]. Understanding current cybersecurity thinking is critical because it can influence ***awareness*** and, consequently, the attitudes of academics and university programs toward ***cybersecurity education***.

DETERMINANTS OF CURRENT CYBERSECURITY EDUCATION AND TRAINING

According to the statistical study on the most important seizure and sending agencies in Sana'a city and the number of accused, seized devices, pure cybercrimes, as well as cybercrimes with traditional crimes, for each of them, the cybercrimes in **Yemen** has begun to increase dangerously (Humied, 2022b), which makes there is an urgent need for cyber security education. ***cybersecurity education*** in specially is also needed for schools' students to control addiction to computer games. This addiction certainly has a negative impact. Teens use their devices to socialize and spend a lot of time on computers. Teens' precious time is consumed by their addiction to devices over time, and playing online games becomes an addiction that cannot be ignored. Young people are severely affected. Teenagers often use the Internet at night, which can exacerbate the situation and even lead to health problems. Users are not always aware that they are under attack, and these threats and attacks can take many forms. Educating and empowering users in the responsible and safe use of online resources and platforms is critical to creating a culture of cybersecurity.

In fact, some ***Yemeni*** institutions offered degrees in computer science within the Department of Mathematics and Statistics in the 1990s. Later, it was further expanded to allow computer science majors to gain disciplinary autonomy within science or engineering departments. Ultimately, with the advent of the 21st century, computer science became a separate discipline, expanding rapidly to include additional disciplines such as information technology, information systems, and software engineering. Computer science, computer engineering, information technology, information systems, and software engineering are just a few of the disciplines that make up independent computing faculties that have grown over time.

On October 14, 2020, a cybersecurity ***awareness*** workshop was implemented at Police College-Ministry of Interior (2020)[7]. During period 7-9 June 2021, Ministry of Communications and Information Technology held the first national conference on cybersecurity in Sana'a (NCC, 2021), and the most important research on cybersecurity was presented[8]. On November 2, 2021, a generalization was issued by Ministry of Higher Education and Scientific Research (2021) regarding adding the topic of cybersecurity to the requirements of universities[9].

Accreditation and Quality Assurance Council (CAQAY) held a workshop from January 31 to February 2, 2018, to develop the first edition of national academic reference standards for computing programs. Some higher education institutions offer a number of computer programs, such as cybersecurity, but are not included in the 2018 edition of national academic reference standards for computing programs because they do not have a national academic reference standard.

As a result, CAQAY (2023) held a workshop to produce 'national academic reference standards (NARS) for computing programs' second edition[10]. Through the process of creating and evaluating academic programs, the aim of the workshop was to improve faculty understanding and adherence to international standards.

[5] Depending on the sensitivity of the consumer transaction, more sophisticated authentication mechanisms are used.
[6] In this article, respondents are identified as Rn; where n=[14-32].
[7] The author who did the training.
[8] The author contributed a paper (see Humied, 2022a for more).
[9] Cybersecurity book (Humied, 2023) is the main reference.
[10] The author is one of the participants in Cyber Security Standards Preparation Committee.

Table 3. Level of influence of variables on cybersecurity education

Factor/Likert scale	1	2	3	4	5	6	7
Government support	0	0	1	1	4	5	8
Full understanding of labor market needs	0	1	1	2	3	4	8
Specialization of educators	1	1	1	2	4	3	7
Awareness	2	3	1	0	5	3	5
Absence of available resources	1	2	3	3	4	2	4

Note. Likert scale: (1) Not at all; (2) Very low; (3) Slightly; (4) Neutral; (5) Moderate; (6) Very; & (7) Extremely

The innovative and efficient technology for computational research provided by NARS should meet the anticipated needs of the organization. Meeting these demands and current and future problems requires a working knowledge of many technologies and problem-solving skills. Thus, NARS's general assertion of computers in this document conveys broad expectations for standards across multiple undergraduate programs (CS, IT, IS, SE, AI, CYS, and DS). These sets define the properties associated with a particular degree. Holders of these degrees should be able to initiate and perform actions related to computer processes, systems, problems, opportunities, history, potential future impact, ethics, etc.

How ***cybersecurity education*** is delivered in Yemen, with factors (such as demand) influencing universities' decisions to include security content in their cybersecurity curricula, and factors influencing universities' capacity to deliver security education. (lack of teaching materials, etc.). Factors grouped in 'other variables' subsection were not summarized in **Table 3**, which she investigated, as they were addressed during the meeting. Each of these variables is described below in order of importance given by the respondents.

Absence of Educator Skill

There are not many educators in ***Yemen*** with formal training in cybersecurity. Representatives of seven universities' departments reported having no security professionals (55%), one (25%), two (10%), and three or more (10%). Nevertheless, some professionals do not necessarily teach cybersecurity because they pursue further education or teach another subject. There are some exceptions, but most Security instructors were trained at a time when local universities did not offer cybersecurity courses.

This shortage impacts cybersecurity skills delivery and security education. This cybersecurity material is often limited and does not combine theory with practice, undermining the quality of cybersecurity courses taught by non-professionals. That universities struggle to fulfill demand for cybersecurity is evident from the fact that:

(a) students' requests for advice for dissertation research exceeded the capacity of the university [R22],

(b) MS security program requested by graduated students; have not been feasible [R20], and

(c) government requests for support in cybersecurity have not been fulfilled by a few universities [R16 & R20].

The following meeting excerpts illustrate these issues: We do not really have experts in security [R20]. Graduates are demanding a cybersecurity master's program, but there is a shortage of faculty to provide it [R21]. You can find people with security experience but no security training [R29]. There are experts in this field, but none with a master's degree in security [R19].

There are many approaches to addressing this shortage of skilled workers. At least three universities have hired cybersecurity-qualified professionals from the ***labor market*** to teach bachelor-level cybersecurity courses, specifically in the areas of cybersecurity management and testing. Two universities use state-owned experts with practical experience in their seminars and lectures.

Full Understanding of Labor Market Needs

Universities across the country have many perspectives. First, many argue that the private ***labor market*** needs university security specialists (82%). The majority of universities report encountering private companies seeking security assistance. Nevertheless, certain companies prefer to hire professionals from abroad, especially the financial sector, which does not seek skilled workers from universities (92%). Second, and more broadly, they eventually needed protection from the government, the court system or the ***labor market*** (23%). Finally, students and alumni are more likely to request safety training. Among these, widely publicized attacks on the country's finances and governance are intriguing. Identify some requirements for establishing security [R25]. According to the ***labor market***, cybersecurity engineers are not needed [R26]. To deal with their problems, they sometimes import experts from other countries [R26 & R22]. We know the commercial sector needs security experts, but the administrator responsible for security may not have the authority to request them [R18]. ***Labor market*** believes science has no value, so it stays away from it and instead seeks experts elsewhere [R19]. Security training is required for students, but there are no security jobs in the ***labor market*** [R18]. The need for security in the local market is partially met by local experts and consultancies, many of which have foreign roots [R26, R31, & R22]. According to those surveyed (42%), the need for security in the commercial sector is currently very high. Some argue that society as a whole need to take more security measures. With the introduction of a master's degree in security, more talent will be needed before the market saturates. An investment in security professionals is easily defended [R14]. There are many unresolved opportunities in this area as I believe the business community is aware of the security risks [R28]. Nonetheless, additional cybersecurity training is required [R15]. Take care! [R18].

The government and financial services sectors are the most obvious and promising sources of cybersecurity needs. Indeed, some participants recognized the dominant position of the financial sector in the country.

The demand for on-premises cybersecurity must be viewed from two perspectives. First, the market is pushing educational institutions to hire graduates with security skills integrated into CS and CN courses so they can perform core tasks while implementing security principles. For example, the banking industry is looking for system engineers who understand secure implementation of IT infrastructure and software engineers who are familiar with secure coding (Catota et al., 2019). Second, a job like security engineer requires a specialized level of security expertise. The majority of

respondents believe that specialization at the MS postgraduate level is more practical than at the undergraduate level, but they need reliable needs information before starting this MS process. For us, demand is the most important factor [R18].

However, some universities believe they are constrained by a lack of authoritative information about their security needs and the lack of demand created by the corporate sector's security posture. As mentioned earlier, recent university efforts to learn more about ***labor market*** needs included research on CIT-related issues, but security was not a major concern. Public and private sector employers' perceptions of cybersecurity also differ. While some organizations have learned the importance of cybersecurity skills, others are unsure of the type of development required, especially if they have had previous negative security experiences. As long as the need for commercial security is clear, it's not difficult to promote a cybersecurity academic program. Employers and educators need to work together to identify the employee skills they need in the workplace. If not, cybersecurity will continue to be a low priority for some institutions [R18 & R22].

Absence of Available Resources

Several university departments have various resources to help improve ***cybersecurity education***. In this case, the responder falls into three categories. The first group (21%) strongly agree that the resource is adequate. Two participants feel constrained by today's government regulations that regulate tuition fees and influence college financial decisions. Some argue that ***cybersecurity education*** competes or will compete with other CS courses for resources such as time and infrastructure. Our IT infrastructure is inadequate [R27]. Getting a security lab is not as important as a general purpose computer lab [R30]. A second group (66%) faces certain resource limitations, impacting their ability to teach security literacy from mild to moderate. Infrastructure, equipment systems and licenses require investment, but sometimes we prefer not investing in those things [R25]. There are some significant issues that we are working to resolve. Acquisition of resources takes time but is prioritized [R23]. Her third group of respondents (13%) believes they do not face significant financial barriers to providing ***cybersecurity education***. Resource availability is not an issue [R22]. Due to poor management, the sector lacks infrastructure. Nevertheless, it is about mentality, not lack of resources [R19]. Economic constraints hinder the development of cybersecurity knowledge, primarily by making it impossible to set up cybersecurity laboratories and hire qualified trainers. Most universities do not have well-equipped labs to teach cybersecurity techniques. Additionally, 46% of his respondents specifically cited the lack of security labs as the biggest barrier to ***cybersecurity education***. Only 11 know that cybersecurity labs exist but have some perceived deficiencies such as lack of expertise and ignorance of technology [R18]. Respondents acknowledge the existence of open source technologies to meet their specific needs but indicate that the specialized equipment required for security training is prohibitively expensive. There are some subjects that cannot be taught because there is no laboratory. This [security] facet has a very low resource allocation [R22]. There is no security lab here [R15 & R17]. A new laboratory should be established [R18]. There are no special laboratories here [R15]. Due to recent increases in import tariffs, and siege and wartime conditions, security equipment is now significantly more expensive [R30]. There are no labs here. You can buy items, but you cannot buy tools. Laboratory exercises are rewarding [R20]. Unfortunately, when we tried to put specialists on, we often had no way to pay for them [R16]. Even if some professionals were willing to work for us, we may not be able to pay for them as much as the ***labor market*** [R14]. I cannot pay the specialist I want $20 [R20] an hour.

Formerly, we had to hire specialists from the private sector, who almost always demanded money. Nowadays, it is much simpler to hire specialists from the public sector [R21]. As a result, ***cybersecurity education*** in ICT programs and future research areas will be affected, especially at institutions that recognize the need for improvement. In addition, economic factors may prevent us from taking the initiative. However, economic factors are usually not the primary ***determinants***, especially when considering the development of an academic security program when market needs are paramount.

Government Support

Here, various national policy issues were discussed that may affect ***cybersecurity education*** and discuss respondents' views on government actions as a means of promoting ***cybersecurity education***. Most respondents agree that some public policies encourage general research and improve general education. However, they pointed out the following unintended consequences for ***cybersecurity education***.

Overregulation

Some respondents believe that universities are now under too much scrutiny and have lost the ability to independently make certain important decisions. Indeed, the development of new undergraduate programs requires government approval, which can be more difficult to achieve, especially if they are not integrated into government structures [R29]. Our autonomy is declining these days [R24]. There is more control now; in the past it was easier to implement changes [R29].

Barrier to hiring professionals

Over the last few years, university professors have been required to have at least an MSs degree in the discipline they teach and their number in the program must not be less than two. Although this regulation is widely seen as having a significant beneficial impact on quality, several universities have noted that certain ***labor market*** experts who were assisting them before the regulation was put in place are no longer allowed to do so. In addition, a rule requiring university professors to obtain PhDs could impact ***cybersecurity education***, given the country's shortage of individuals with degrees and skill in cybersecurity, both in academia and in ***labor market***.

Student dropout rate

In order to unify higher education, a separate collection of courses for students has been defined according to current regulations. As a result, there are barriers for students seeking admission to cybersecurity programs to focus on higher mathematics such as algebra and calculus. Several students

dropped out of her program in cybersecurity in her first year because of knowledge gaps in these areas [R26 & R27]. This issue may affect the number of graduates receiving cybersecurity training.

Constraints on updating programs

CAQAY (2023) governance framework does not include non-routine academic programs mandated by current law [R30]. There is also debate about whether governments should take proactive steps to improve security teaching in universities. Proponents said the government needs to prioritize universities and set clear rules to ensure these are implemented. Governments still have work to do when it comes to cybersecurity [R23]. Understanding the requirements of the security ***labor market*** requires government involvement [R24]. Government cybersecurity policies are not explicit [R19]. There must be state regulations containing binding topics [R17]. Requires governance security rules [R21]. In contrast, others (43%) believe that there is already too much regulation by government agencies, so the government does not need to provide much direction, and universities need to talk to the ***labor market*** to understand the need for security. State involvement is inappropriate [R21]. Excessive intervention is a problem [R15]. Some regulation is beneficial, but too much regulation is harmful [R14]. Improving interaction between ***Labor market*** and academia are more important than government involvement. Governments may not request details of ***labor market*** requirements [R28]. Outside the ***labor market***, the government's widespread encouragement for the use of ICT in the public sector is sending an implicit message to universities that they need to develop security features to protect citizens' personal data [R21]. Government involvement is generally seen as an integral part of ***cybersecurity education*** and training, as well as the set of cybersecurity regulations.

Awareness

Respondents agreed that organizational knowledge exists, but some argued that there was insufficient ***awareness*** of specific needs in ***cybersecurity education***. Two universities report he offered an academic program a decade ago when cybersecurity was not a major concern. Nevertheless, they emphasized that this fact has recently developed. A network across the university system helps raise ***awareness*** among the people. No security was expected here [R20]. No one knows the security requirements that should apply to institutions [R25]. We have not discussed this [security] aspect [R32]. We see [security issues, for more] in the news, but the administrative function is slow to react [R14]. More than anything else, the problem is ***awareness*** and initiatives, including professors. CAQAY (2023) should act as an 'engine' by raising concerns and requesting the inclusion of security-related topics in the curriculum [R18]. Security, which previously received little attention, is now essential in the design of new curricula [R21]. Respondent provided his two additional sets on security ***awareness*** in addition to academic teaching practices. To raise ***awareness***, inadequate security procedures in the university's infrastructure were discussed twice by him. Social ***awareness*** was discussed by the respondents. Despite numerous government and financial sector initiatives, the general perception is that the general public is unaware of cyber threats and their impact. It has been suggested that one of his ways of combating cyber vulnerabilities is to raise ***awareness***.

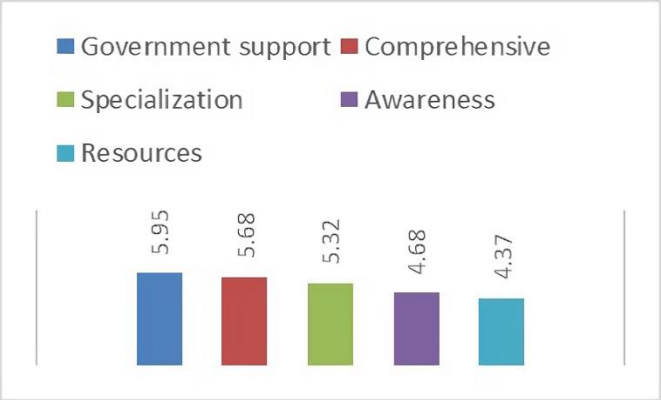

Figure 1. Weighted average computed as number of respondents by Likert scale in **Table 3** (Source: Author)

Despite strong technological protections, careless human behavior can still lead to security breaches. Educational dialogue is needed for everyone, and these should start in schools [R22]. Rather than waiting for incidents to arise before acting, we need to raise ***awareness*** [R25]. Here you should be very diligent in improving your employee's knowledge, especially in teaching her about web surfing, phishing and prohibiting password sharing [R18].

Table 3 shows the distribution of ***cybersecurity education*** factor effectiveness predicted by the study design to complement what was previously discussed. The extent to which a factor (a positive situation) contributed to the advancement of ***cybersecurity education*** should be considered when determining the impact of that factor. Responses were given on a Likert scale ranging from (1) not at all influential to (7) extremely influential. For instance, 1 respondent reported the factor ''Absence of available resources'' as not influential at all. This means that respondent believe that ''Absence of available resources'' has not been a contributory factor to support ***cybersecurity education*** at their universities. Conversely, 8 respondents reported ''government support'' as extremely influential. **Figure 1** shows a weighted average computed as the number of respondents by the Likert scale in **Table 3**.

Belonging

Occasionally, a tendency to naively accept cyber threats was noted. This is consistent with Catota et al.'s (2019) and Target's (2010) findings on risk attitudes in poor countries. Several discussions indicate that ***labor market*** actors become aware of threats and take action to mitigate them only after experiencing a security incident and its consequences (financial or otherwise). Therefore, situational ***awareness*** comes at a price. This way of dealing with cyber risk is detrimental to cyber security preparedness: one of her participants also cited a lack of belonging as a barrier to cyber security progress. Because of our peculiarities, we needed government incentives to initiate research [R24]. Due to our idiosyncrasies, promoting safety is a challenge [R26]. I think our peculiarities set us apart from other civilizations. We do not really feel belonging [R19].

University regulations

Restrictions at some universities hinder cybersecurity efforts and educational progress. There is another professor who has had formal security training, but an academic leader from two institutions (one public, one private) is a security he teaches the topic but has no formal security training. It states that a scholar who has not received it cannot be replaced. In addition, organizational regulations stipulate that the university retains ownership of intellectual property arising from student research initiatives (such as dissertations). The local ***labor market*** [R18] has found this restriction insufficient as it limits participation and innovation. Finally, political and personal interests were cited as challenges to advancing scientific goals. Despite current efforts, the university paradigm is still based on the political interests of people and organizations [R19].

Absence of foreign language skills

This issue, once raised, prevents academics with insufficient English education from accessing the latest information in cybersecurity and other fields. The English spoken here is rudimentary, and although the professor has been teaching mor than five years, the current subjects [in computer science-related fields] are available in English [R17].

Training

In addition to educating students and parents on how to use the Internet at home, rather than promoting a restrictive approach to cybersecurity, teachers should be properly qualified and up-to-date to promote critical knowledge. Lack of knowledge, resources, and funding are some of the serious problems schools face when implementing ***cybersecurity education*** (Salamzada et al., 2015). When it comes to online, teachers are underprepared and under skilled. Schools and government agencies may not have the necessary resources and infrastructure to provide ***cybersecurity education***. Rapid technological progress creates new hazards that require novel solutions. Instructors may struggle to develop an understanding of cutting-edge technology and ensure student safety (Miles, 2011). Teachers face significant challenges due to lack of access to educational resources and the need to be aware of technological advances. Cybersecurity symposiums should be used to encourage early training and experience among students at educational institutions. The future source of national cyber defenses is expected to be cybersecurity-exposed and trained individuals.

DISCUSSION

It has been said that no country is fully equipped to deal with cybersecurity threats (Hathaway et al., 2015). Research shows that cyber literacy is building slowly in Yemen. This is in contrast to certain developed countries with high levels of national cybersecurity performance, which have already launched stronger workforce and education initiatives to support this readiness. In this study, has described the current state of ***cybersecurity education*** in ***Yemen*** and the unique factors that have contributed to the current situation.

Semi-structured meetings were used with 19 key respondents (professors and executives) from seven institutions (Including most major universities) to gather information relevant to our research.

This is a carefully selected sample of people whose first-hand experience has helped us understand the problem. From this data, common themes relevant to addressing research concerns were extracted, and categories were derived by associating these themes (Creswell & Creswell, 2017). During the meeting, several themes prevailed among the participants as common issues. The importance of these issues in research depends on the sources and methodologies used for the analysis. In presenting ideas in essays, I frequently included quotes related to what the respondent said. All of our results were obtained from a combined examination of the respondents' responses and, of course, represent their opinion. The fact that many of these ideas are fairly consistent across respondents and suggests that they are grounded in underlying realities.

In Yemen, most cybersecurity courses are taught at undergraduate. Today, absence of educator skill, full understanding of ***labor market*** needs, absence of available resources, government support, constraints on updating programs, and ***awareness*** are the main ***determinants*** that ***cybersecurity education*** needs to adhere to it. Lack of collaboration among professors can lead to gaps in security knowledge and redundant information. Even when some safety courses are available, they often lack depth or breadth, especially if they lack the necessary skills and resources such as labs. In fact, most of the critical information, such as how to respond to incidents, was missing. Similar to his Lehto (2015) results in Finland, the initiatives encountered by universities do not include a single national vision. As a result, the quality, completeness, and relevance of security content are compromised. There is an active cybersecurity program at postgraduate level, but it appears to be inadequate.

The results of the discussion suggest that there is a widespread view that academics cannot advance ***cybersecurity education*** because of university priorities, lack of experts, lack of organizational flexibility, and lack of recognition of needs. ***cybersecurity education*** requires not only capabilities, but also the determination to assign higher priority to such efforts. One of the major problems hampering the ability of universities to provide ***cybersecurity education*** is their lack of cybersecurity professionals. Adhering to this ***determinant*** due to stringent regulations prohibiting universities from hiring professionals without a college degree, high costs for security professionals, and a nationwide shortage of qualified cybersecurity professionals It is difficult.

Even if government actions have helped take the first steps towards solving this problem, effective barriers exist between the university and corporate sectors, preventing participation. Therefore, semi-structured meetings had started semi-structured meetings for this article using a set of predictions about the outcome. The lack of progress in college was expected, as this also applies to the local ***labor market***. Having the financial and human resources to improve ***cybersecurity education*** in emerging markets is a common factor, but having such resources have found does not guarantee success. Inadequate higher education policies (e.g., inability of

universities to hire trained professors to deliver cybersecurity courses), specific interests of groups and individuals, and inadequate management of business resources. are some of the barriers that affect the availability of resource.

the lack of cybersecurity-trained professors had been expected to be an obstacle, but some universities learned that offer programs try to fill this gap. Unfortunately, it does not offer as many courses as it should (for example, only one university was reported to offer a course on cryptography). Respondents were expected to be reluctant to acknowledge gaps in their ability to teach cybersecurity to students, yet most respondents identified and reported issues that were unclear. I'm very grateful to know that there were no issues.

Furthermore, the majority of academics' understanding of cybersecurity demands comes from observations (from the media), personal experience (from his security incidents), feedback from students and alumni, potential projects (from security or education), etc. based on the theory of private sector projects, especially projects by academics with a strong focus on cybersecurity. Regarding current perceptions that suggest low demand, two plausible reasons were observed:

(a) ***labor market*** often has to seek help from other sources in order to respond quickly to specific challenges, so some institutions do not see an immediate need (proven in the financial sector) and

(b) security appears to be unstable in certain ***labor market*** sectors.

Other less-mentioned ***determinants*** are belonging, university regulations, language barriers that make it difficult to obtain the latest cybersecurity know-how, and training.

Although there are no universal, accepted standards against which ***Yemeni cybersecurity education*** can be judged, there exist global references proposed by developed nations that can provide insights. According to the USA NSA and DHS, academic excellence in information assurance (IA)[11] can be achieved by:

(a) forming partnerships with educational institutions,

(b) view IA as an interdisciplinary science,

(c) promoting the practice of IA,

(d) promotion of IA research,

(e) developing an IA curriculum that has impact outside of academia,

(f) faculty engaged in IA practice, research, and literature contribution,

(g) access to state-of-the-art IA resources,

(h) an academic program with an IA focus,

(i) IA Research Center, where IA curriculum is developed, and

(j) IA teachers who devote all their time to IA (Schweitzer et al., 2006).

Oxford cyber capabilities maturity model can be used to assess national cybersecurity capabilities beyond what institutions do. ***cybersecurity education*** is one of the five dimensions of the model. The description uses five maturity levels: startup, formative, established, strategic, and dynamic.

Multiple sectors of society can benefit from ***cybersecurity education***. Both the ***labor market*** and universities serve as important centers of readiness, especially for training, but how effective this is will depend on the cyber skills they currently possess and the incentives to improve them. Financial institutions and major ISPs have been training their technical staff in these areas for some time, as their management believes most universities do not teach certain cybersecurity skills effectively. In the financial services major incentives to provide cybersecurity are domestic regulations and ***labor market*** self-regulation (Catota et al., 2019). Although there are no cybersecurity regulations in the telecommunications industry at the time of writing, some ISPs are trying to enter the security services market. In the regulation, cyber skills development is often influenced by many incentives, including ***awareness*** of the risk imposed by cyber threats to national security, domestic political strategies, and geopolitical interests. These factors do not appear to push ***Yemen*** to build a significant cybersecurity capacity, at least not capabilities that have benefited areas outside of the regulation. Thus, despite the fact that the best educated universities have developed specific strategies (MS programs, research initiatives, professional security courses, etc.) to address cybersecurity aspects, great efforts should be made to strengthen ***cybersecurity education***.

A literature review indicates that there are several advantages if universities are able to successfully implement ***cybersecurity education***. It is therefore important that universities develop as information centers and educate the public on cybersecurity issues. Academics and university administrators can work together to plan programs and events related to cybersecurity. Additionally, ***Yemeni*** government provides financial support to universities to help them cover the costs associated with conducting such community activities. Also, ***cybersecurity education*** can help change people's perspectives. Those who lack cybersecurity ***awareness*** do so because they do not recognize the importance and consequences of cybersecurity. These initiatives should consider the diverse developments in ***cybersecurity education***.

APPROACHES TO IMPROVE CYBERSECURITY EDUCATION

Successful ***cybersecurity education*** cannot be achieved as an isolated effort pursued only by universities. Instead, it requires a steady effort. A review of the relevant literature reveals that the national initiative to promote ***cybersecurity education*** (and employee skills) includes six dimensions of her: capacity governance, academic programs, training, qualification, research and development (R&D), and cybersecurity ***awareness***. In what follows. The following paragraphs propose regulatory options formulated for these dimensions.

[11] Although these are similar terms, information assurance and cybersecurity are often not equivalent.

Capacity Governance and Multipurpose Strategies

First, national programs will be talk about that address governance and other activities that can affect various aspects of ***cybersecurity education***.

National cyber strategies and regulation

National cybersecurity strategies, national ***cybersecurity education*** initiatives (such as the U.S. NICE, 2010 framework), and industry-specific cybersecurity capability maturity models (CMMs) all advocate cyber education and human resource governance to improve cyber education and human resource governance. It's a tool being developed by a nation moving towards better preparedness. (e.g., cybersecurity capability maturity model for the U.S. power subsector). According to the NICE (2010) framework cybersecurity work vocabulary definitions, the seven categories of cybersecurity workforce roles are: securely provision, operate and maintain, protect and defend, investigate, collect and operate, analyze, and oversight and development (Petersen et al., 2020). While it is well known that there are not enough skilled professionals in the world to support these categories of HR functions, oversight and development expertise is lacking in cybersecurity policy and legal frameworks. On January 4, 2023, National Cyber Security Strategy (2023)[12] has been approved by Council of Ministers. Also, presently, the draft law on combating information technology crimes 2023 is being discussed[13].

To start improving ***cybersecurity education***, ***Yemen*** must implementation of the national ***strategy*** for cybersecurity to provide governance guidelines and promote instruments that can develop cyber capabilities across academia, government, and ***labor market***. This ***strategy*** should identify and prioritize key national infrastructure sectors requiring urgent attention. It also requires identifying and prioritizing the cybersecurity knowledge and skills that need to be developed for the general public, professionals, and students in schools, universities, and other organizations. ***Yemen*** must allocate resources to train computer systems and network security teachers, set up cyber labs, and initiate cyber research and development activities to meet the country's most pressing needs. R&D grants, educational grants, and private funding for education are examples of possible tactics. Additionally, it is important to encourage equipment donations from both the public and private sectors.

Policies are need policies to improve math and science preparation and introduce computer science and cybersecurity to students from an early age. Techniques used in the United States, United Kingdom, Israel, and other countries can be used to lay the groundwork for long-term improvements in student performance, helping to overcome the current high early dropout rates in CS programs. Students need to understand what it takes for a career in computer science and cybersecurity. Educational initiatives and discussions with CS and cybersecurity professionals should be encouraged (Lehto, 2015). Most students today have a misconception about computer science programs because they either were not exposed to computer science courses early in high school or never had the opportunity to attend lectures or watch demos [R23]. Some students discourage careers in computer science because they think that learning software is all he does [R23].

Public and private support

Incentives should be put in place to encourage the development of cybersecurity capabilities in both the public and commercial sectors. There is now a significant opportunity to increase ***labor market*** support for the educational environment. Universities in the first group use different strategies such as

(a) establish links with the ***labor market*** through alumni and track the employment status of graduates by the university,

(b) identify real ***labor market*** problems that universities can solve, and

(c) propose projects that are mutually beneficial (consulting services).

Other efforts to improve ***labor market*** connectivity include:

1. Interacting with university contractors who can help establish technical connections. For example, an ISP serving a university may be able to provide technical advice on cybersecurity issues for telecommunications sector.
2. Encourage people in ***labor market*** to reach out, hold conferences, and involve cybersecurity experts from established academic institutions.
3. Facilitate programs needed by ***labor market*** and establish and maintain links.
4. Build university alliances to collaborate on approaches to practitioners. After implementing such strategies, universities should address the following in ***labor market***:
5. Educate and provide relevant research answers on key real-world cybersecurity needs and issues. Collecting this relevant data in both ways greatly improves our understanding of cybersecurity needs. Universities can use this to align their curriculum with that of job market.
6. Support research activities in the field of cybersecurity and other educational programs such as cybersecurity labs.
7. Promoting student training through apprenticeships and internships. According to educators (private and public), building partnerships with prospective employers should be a high priority in advancing ***cybersecurity education***. As mentioned earlier, there are some potential advantages. Two of these are the financial support needed by the significant number of universities participating in our research, and increased ***awareness*** of staffing needs.

Government is an important additional actor that needs to be involved in developing the relationship between academia and ***labor market***. There is an urgent need for a multi-

[12] The author is one of the members participating in the preparation.
[13] The author also is one of the members participating in the preparation.

stakeholder arena with active engagement of governments, the ***labor market*** and academia to respond to national ***cybersecurity education*** needs and initiatives. Ultimately, public and private support for expanding ***cybersecurity education*** can be seen in many different ways.

Institutional policies

Universities must comply with current regulations that restrict collaboration with outside parties and impede progress (strict copyright laws, limits on the number of professional professors employed, selective status in security courses, and allocation of university funding). Initiatives to promote engagement among universities are also needed. By distributing cybersecurity know-how across university departments, you can focus your efforts on improving your organization's understanding of cybersecurity. One such technique is now being used by at least one university to give students from various major's access to integrated cybersecurity courses in a common curriculum.

CERT support

The term CERT comes from the first computer emergency response team (CERT/CC) formed at Carnegie Mellon University (CMU) in 1988 to address computer security issues. The teams that deal with such situations use the common names CSIRT or CERT and are licensed worldwide by computer security incident response team. CERT has proven to be an effective tool to promote national cybersecurity in a variety of economic environments and orientations CERT/CC, CMU's IA capacity development program funded by NSF, sponsors a number of educational initiatives across the country, including faculty training in IA, survivability and IA curriculum development, and educational resources. Regional academic clusters (i.e., groups of academic institutions in the US region) to facilitate participation and promotion of projects that support universities (Sledge, 2005).

CERT has evolved in recent years from cyber resources used primarily by developing countries. In emerging markets such as Oman, and India, CERTs are becoming increasingly important to spread cybersecurity expertise and ***awareness*** (ITU, 2007). In particular, Oman's national CERT promotes ***cybersecurity education*** in a number of areas, including ***awareness*** and safety practices. According to ITU global cybersecurity rankings (ITU, 2014), the national CERT helps Oman to rank first in the Arab Region and third globally in cybersecurity readiness. This shows that developing countries like ***Yemen*** are aware of their cyber needs and can develop advanced cyber skills. A strong and efficient CERT could be an important multifaceted tool to achieve these goals.

Academic networks

Beyond institutional level activities, the network has the capacity to foster national and international engagement. Yemen's academic network could be expanded nationwide to actively address cybersecurity measures [R32].

Academic Programs

Academic security resources should be incorporated into the educational system at different levels in different disciplines, such as practical systems, electronics, telecommunications, criminal justice, and business. In fact, respondents believe that business positions (such as MBAs) should include training to help assess cyber risk, and that law enforcement agencies should also include training to assist with investigations [R15].

Clearly, the current lack of expertise makes such projects difficult to implement, but the situation should improve in the end. With its enhanced ability to explicitly train educators, the current master's program is beneficial to faculty teaching security-related topics at universities. Trainers with cybersecurity expertise can be found nationally and internationally to run this project. Potential sources of experts are, as follows:

(a) Temporary importation of foreign experts. Moreover, given the global shortage of cybersecurity professionals, importing talent in the long term can be difficult.

(b) Security trained professionals abroad.

This includes professionals already residing in the country and professionals who have returned home on government scholarship programs (Raytheon, 2015). A comprehensive ***strategy*** should draw on expertise from several sectors of society (Dark, 2014). When importing an academic curriculum, care must be taken to adapt the design to the native environment. Association for Computing Machinery (ACM) was mentioned by some meeting attendees as one of the sources of cybersecurity program information. However, ACM curriculum has not always been widely adopted, even in American institutions, due to the lack of cybersecurity perspectives from the ***labor market*** and government. Initiate this effort in **Yemen** to identify subject areas that may be incorporated into cybersecurity expertise and appropriate curricula, as current local methods lack such information. It is clear that how content is delivered, is as important as what it is taught (Schneider, 2013). Effective learning strategies should be found and incorporated into the cybersecurity curriculum implementation. For example, real-world case studies and hands-on simulations should be included in academic teaching [38]. Additionally, adversarial thinking can be added to the basic concepts that enable understanding of system vulnerabilities (Klimburg, 2012). This makes it ready to deal with new threats as opposed to detected types of attacks (Schneider, 2013). So, while building skills may take time, it is imperative to take immediate action and start or at least explore more complex projects.

Cybersecurity Training

Developing a more robust academic program will rely heavily on faculty members who receive specialized training in the field of cybersecurity with no prior experience. Her CERT support for educator training can be very important in this situation. Improving proper training of students in the practical aspects of cybersecurity also requires the involvement of extra-institutional labs and experiences. Other measures that should be taken are, as follows:

(a) Provide incentives to the local ***labor market*** to promote educational programs such as providing paid internships and trainers.

(b) Facilitate long-term professional exchanges between government agencies and academic institutions to foster growth.

(c) Support from overseas partners (organizations or commercial companies) such as OAS in Uruguay, IBM in Costa Rica, Microsoft in India and OIC-CERT (in Malaysia).

(d) Training sharing, a ***strategy*** currently followed by at least one **Yemeni** university when training teachers [R31].

(e) Establishment of training courses.

(f) Practice safety competitions, safety workshops and virtual training environments [R14, R21, & R22].

(g) Develop and promote apprenticeship programs that provide students with hands-on experience in cybersecurity.

(h) Focus on thorough, hands-on safety training.

The importance of apprenticeship programs to improve practical technical training in cybersecurity has been recognized in several countries. The government funds cybersecurity training programs to support key industries in the UK (Department for Digital, Culture, Media & Sport, 2017). A US community agency has started offering a cyber apprenticeship program (Tidewater Community College, 2017). In addition, training is needed to keep law enforcement and the state of the art in the ***labor market*** up to date. Due to concerns about the quality of business education, controls to ensure acceptable quality standards should be considered [R19].

Cybersecurity Qualifications

While obtaining professional qualifications may not be a primary mission of academic institutions [R19], some believe that teachers should encourage safety qualifications to enhance the knowledge of their students [38]. Several developing countries looking to improve their cybersecurity performance are considering CERT and government support for international certifications (such as Oman) and certification programs (such as Rwanda). Promotion of professional security associations by low-cost student associations should be encouraged to expand accessibility (Wright, 2015).

Research and Development

Deploying full-scale cybersecurity research in ***Yemeni*** institutions presents major ***determinants***, as good research must build upon existing capabilities and structure, such as experience, funding, research centers, and practical projects. It is R&D creates a cybersecurity program. Faculty involvement in further development of education could already be increased if existing university projects on information security research are supported and expanded. A coordinated national effort should identify potential public and private sector research areas to advance cybersecurity critical to infrastructure protection.

Many studies concerned with the field of research have been published in ***Yemen*** (Akkar & Alamery, 2022; Al Khateeb et al., 2021). Higher authority for science, technology, and innovation was also established in 2020, as the authority works to create a stimulating and supportive environment for excellence, creativity, innovation and scientific research in the field of science, technology and innovation and contributes to strengthening the relationship between scientific institutions and research bodies on the one hand and economic units in the public, mixed and private sectors (Higher Authority for Science, Technology, & Innovation, 2021).

Cybersecurity Awareness and Public Education

Respondents stressed the need to address social ***awareness*** at the national level, OAS definitely underscored this (Inter-American Development Bank, 2016). We encourage other academic institutions to follow at least one of her colleges in their efforts to educate their internal audience (online education) [R30].

Cyber hygiene campaign, national cybersecurity ***awareness*** week and national awareness program (Rwanda) are examples of strategic actions around the world (South Africa). For such a program to be successful, it must specify its target audience, themes, and methods of raising ***awareness*** and education. In addition to considering other aspects of society such as business, decision-makers, and justice, some say the target audience should consist of young people, adults, and the elderly (Bishop & Taylor, 2009). When addressing national cyber risks, the issue must also consider global trends. They should include basic details about attack techniques (such as malware infections and social engineering), their impact (such as fraud and privacy violations), and defensive tactics (such as patches and password best practices). School curricula, radio (Cameroon), television and Internet resources are just a few of the methods of delivery already being used in developing countries, depending on the target audience. The techniques used to disseminate ***awareness***–raising information, like formal education, are essential to achieving the goals. Videos, cartoons (Brazil), and analogies that use existing mental models of the physical world to increase cybersecurity knowledge are some possible delivery methods (Furman et al., 2012).

For example, video cartoons have been recognized as a resource for teachers to use when discussing cybersecurity concepts with elementary school students to better understand. Also, ***cybersecurity education*** using the stories of Upin and Ipin (Pitchan at al., 2017). Cybersecurity topics should be included in information and communication technology courses taught in primary schools. Additionally, other courses can be used to teach cybersecurity. For example, a student might be assigned an essay on cybersecurity within her topic Bahasa Melayu. You can also host a cybersecurity ***awareness*** week and promote cybersecurity in classrooms and speech contests. Additionally, security ***awareness*** efforts are one tactic that can support ***cybersecurity education*** in schools. When creating information security ***awareness*** initiatives, IT professionals have generally ignored the concept of cybersecurity ***awareness*** developed in years of social psychology research (Kabay, 1994).

For example, GenCyber is an NSA and NSF funded summer camp for elementary school teachers and children in the United States. All schools should create a curriculum like this. Because it can improve students' understanding and level of preparedness for cybersecurity issues. School leaders can also

establish student councils and groups focused on cybersecurity, which can give children and the entire school community valuable attention. Teachers can help kids who want to learn more about cybersecurity.

The paradigm presented by Kortjan and Von Solms (2014) provides strategic insights for addressing cybersecurity ***awareness*** and education in South Africa. Many of these ideas are applicable to developing environments and are of great value but implementing them in ***Yemen*** requires consideration of the skills of national capabilities. Needless to say, raising ***awareness*** alone will not solve the problem of anxiety. Here's why:

(a) ICT users inevitably fall short to accomplish what is expected from them in their roles anyway (Cranor, 2008) and

(b) attackers may evolve to evade defenses, especially if the victim is targeted by a sophisticated adversary.

However, effective ***awareness*** and education can help prevent some attacks (such as malware infections and social engineering) and provide insight into improving the security of personal data. Last but not least, improving formal and informal ***cybersecurity education*** requires short-term and long-term planning.

CONCLUSIONS

Cybersecurity threats have been difficult for Yemen's educational system to deal with ***awareness*** of cybersecurity attacks against domestic critical infrastructure has not been sufficient to develop a comprehensive national academic approach to ***cybersecurity education***. It poses ***determinants*** to the education system as it requires both new teaching methods and established social norms.

Indeed, improving ***cybersecurity education*** depends on the basic skills that are expected to already exist, such as academic initiatives with strong links to societal needs, academic infrastructure, and robust research frameworks. The development of such structures is still in its infancy in Yemen, making cybersecurity a particularly difficult issue. Universities' capacity to deliver academic courses is limited due to the lack of staff with formal training in both technical subjects and cybersecurity. There are serious problems in the integration of academia with ***labor market***, which hinder the means of promoting development (such as understanding demand). Many countries are struggling to move forward, but ***Yemen*** is distinctly different from developing countries with well-established good academic institutions. Oman and Malaysia serve as good models from which emerging markets can draw useful lessons. Few studies have identified the exact factors that hinder ***cybersecurity education***. There is a large body of literature that provides strategic guidance on how to address the problem, especially in the context of developing countries.

The article is beginning to fill that gap by bringing together the views of educators from several universities. The article answers questions: What are the ***determinants*** academic institutions face in providing ***cybersecurity education*** in Yemen? How can supporting ***cybersecurity education*** improve national cybersecurity capabilities? This study addresses these questions by outlining the reasons for the shortage of cybersecurity professionals in the local ***labor market***. This study provides information on factors affecting ***cybersecurity education*** in Yemen. The purpose of our study was to provide information for public regulation in order to enhance national protection of critical infrastructure. All countries, especially Yemen, suffer from high demand and scarcity of resources. It is impossible to adequately quantify the dangers posed by unintended harmful cyber incidents, but global developments show that they are on the rise. We need experts who can identify and develop cost-effective and efficient risk mitigation strategies. This allows us to make informed decisions about the amount of limited public and private resources to allocate to cyber protection and security.

A detailed understanding of such strategies is a necessary first step in formulating a prudent course of action. To support these efforts, a range of regulatory options have provided grouped into six dimensions for countries to consider as part of their development ***strategy***. Research is needed to determine which tactics are best in general, and to establish systems that balance financial incentives to universities with the public interest. Overcoming the difficulty of developing cyber skills takes time. Fortunately, Yemen's higher education system is undergoing major changes, offering an excellent opportunity to start expanding ***cybersecurity education***.

Funding: No external funding is received for this article.

Ethics declaration: Author declared that the study did not require ethics committee approval. Informed consents were obtained from the participants.

Declaration of interest: The author declares that there are no competing interests.

Availability of data and materials: All data generated or analyzed during this study are available for sharing when appropriate request is directed to author.

REFERENCES

AACS. (2022). *Academic accreditation council strategy*. https://www.caqa-yemen.org/

Akkar, H., & Alamery, A. (2022). Requirements for the development of scientific research in Yemeni universities from expert persons. *Journal of Educational and Psychological Sciences, 6*(21), 1-22.

Al Khateeb, K., Al Awadhi, A., & Al-Hakiem, S. (2021). Half a century of Sana'a University scientific publication collection: A descriptive analytic study (1970-2020). *Yemeni Journal of Scientific Research, 5*, 1.

Aury, M. C., & Alfredo, C. (2013, August). *Faculty attitudes toward teaching ethical hacking to computer and information systems undergraduates students* [Paper presentation]. Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2013): Innovation in Engineering, Technology and Education for Competitiveness and Prosperity, August 14 - 16, 2013 Cancun, Mexico. https://bit.ly/40gqjoq

Bishop, M., & Taylor, C. (2009). *A critical analysis of the centers of academic excellence program*. https://escholarship.org/uc/item/33k0z5tm

CAQAY. (2023). National academic reference standards (NARS) for computing programs. *Council for Accreditation and Quality Assurance*. http://www.hti.edu.eg/images/webPages/file/NARS%20computer%20science.pdf

Catota, F., Morgan, M., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity, 5*, 1-19. https://doi.org/10.1093/cybsec/tyz001

Cranor, L. F. (2008). A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security* (pp. 1-15). USENIX Association.

Creswell, J., & Creswell, J. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE.

Curbelo, A. M., & Cruz, A. (2013). Faculty attitudes toward teaching ethical hacking to computer and information systems undergraduates students. In *Proceedings of the 11th LACCEI Latin American and Caribbean Conference for Engineering and Technology* (pp. 1-8).

Dark, M. (2014). Advancing cybersecurity education. *IEEE Security & Privacy Magazine, 12*(6), 79-83. https://doi.org/10.1109/MSP.2014.108

Department for Digital, Culture, Media & Sport. (2017). *Cyber security CNI apprenticeships*. https://www.gov.uk/guidance/cyber-security-cni-apprenticeships

Furman, S., Theofanos, M. F., Choong, Y.-Y., & Stanton, B. (2012). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy, 10*(2), 40-49. https://doi.org/10.1109/MSP.2011.180

Harašta, J. (2013). Cyber security in young democracies. *Jurisprudencija* [*Jurisprudence*], *20*(4), 1457-1472. https://doi.org/10.13165/JUR-13-20-4-10

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). Cyber readiness index 2.0. *Potomac Institute for Policy Studies*. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Higher Authority for Science, Technology, & Innovation. (2021). https://www.oecd.org/sti/641/

Humied, I. A. (2022a). *Common risks and challenges in cybercrime*. http://matjournals.co.in/index.php/JCSPIC/article/view/1174

Humied, I. A. (2022b). *Cybersecurity as an emerging challenge to Yemen security*. http://matjournals.co.in/index.php/JCSCS/article/view/1139

Humied, I. A. (2023). *Cybersecurity* (Kindle Edn.). Amazon. https://a.co/d/44cfZbK

Inter-American Development Bank. (2016). *Cybersecurity: Are we ready in Latin America and the Caribbean?* https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean

ITU. (2007). Cybersecurity work program to assist developing countries. *International Telecommunication Union*. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

ITU. (2014). *Global cybersecurity index*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf

Kabay, M. (1994). Psychological factors in the implementation of information security policy. *Control and Security Newsletter, 11*(10), 1-10. https://doi.org/10.1080/07366989409451659

Klimburg, A. (2012). *NATO national cyber security framework manual*. NATO CCD COE Publications.

Kortjan, N., & Von Solms, R. (2012). Cyber security education in developing countries: A South African perspective. In K. Jonas, K., I. A. Rai, & M. Tchuente (Eds.), *e-Infrastructure and e-services for developing countries* (pp. 289-297). Springer. https://doi.org/10.1007/978-3-642-41178-6_30

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal, 54*, 29-41. https://doi.org/10.18489/sacj.v52i0.201

Lehto, M. (2015). Cyber security competencies: Cyber security education and research in Finnish universities. In *Proceedings of the 14th European Conference on Cyber Warfare & Security* (pp. 179-188).

Lokman, H. F. B., Nasri, N. M., & Khalid, F. (2019). The effectiveness of using Twitter application in teaching pedagogy: A meta-synthesis study. *International Journal of Academic Research in Progressive Education and Development, 8*(2), 205-212. https://doi.org/10.6007/IJARPED/v8-i2/5696

Miles, D. (2011). Youth protection: Digital citizenship-principles and new recourses. *IEEE Xplore*. http://ieeexplore.ieee.org/document/5978778/

Ministry of Higher Education and Scientific Research. (2021). The generalization. *Yemen Network for Education News*. https://www.ymnedunews.net/

Muller, L. P. (2015). Cyber security capacity development in developing countries: Challenges and opportunities. *Norwegian Institute of International Affairs*. https://cybilportal.org/wp-content/uploads/2020/06/NUPI Report03-15-Muller.pdf

National Audit Office. (2013). *The UK cyber security strategy: Landscape review*. National Audit Office.

National Cyber Security Strategy. (2011). *Protecting and promoting the UK in a digital world*. https://www.gov.uk/government/news/protecting-and-promoting-the-uk-in-a-digital-world--3

National Cyber Security Strategy. (2023). https://tinyurl.com/sdc85sfa

NCC. (2021). The first national conference on cybersecurity. (2021, June 7-9). *Ministry of Communications and Information Technology, Sana'a, Yemen*. https://www.sabafon.com.ye/en/sponsored-by-the-ministry-of-communications-the-conclusion-of-cyber-security-first-national-conference-in-sanaa/

Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing countries. *National Cybersecurity Institute Journal, 2015*, 9-19.

NICE. (2010). Relationship to President's education agenda. *National Initiative for Cybersecurity Education*. https://www.whitehouse.gov/priorities/

Parekh, A., Pawar, A. M., Munot, P., & Mantri, P. (2011). Secure authentication using anti-screenshot virtual keyboard. *International Journal of Computer Science Issues, 8*(5), 534-537.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy, 10*(3), 76-79. https://doi.org/10.1109/MSP.2012.73

Petersen, R., Santos D., Smith M., Wetzel K., & Witte G. (2020). *Workforce framework for cybersecurity (NICE framework)*. https://doi.org/10.6028/NIST.SP.800-181r1

Pitchan M., Omar S., Bolong J., & Ghazali A. (2017). Analisis keselamatan siber dari perspektif persekitaran social: Kajian terhadap pengguna internet di Lembah Klang [Analysis of cyber security from the perspective of the social environment: A study of internet users in the Klang Valley]. *Journal of Social Science and Humanities, 12*, 16-29.

Police College-Ministry of Interior. (2020). A cybersecurity awareness workshop. *Althawrah*. https://althawrah.ye/archives/641310

Raytheon. (2015). Securing our future: Closing the cybersecurity talent gap (October 2015). *Raytheon Company*. https://library.cyentia.com/report/report_002051.html

Salamzada, K., Shukur, Z., & Abu Bakar, M. (2015). A framework for cybersecurity strategy for developing countries: Case study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia, 4*(1), 1-10. https://doi.org/10.17576/apjitm-2015-0401-01

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy; 11*, 3-4. https://doi.org/10.1109/MSP.2013.84

Schweitzer, D., Humphries, J. W., & Baird, L. C. (2006). Meeting the criteria for a Center of Academic Excellence (CAE) in information assurance education. *Journal of Computing Sciences in Colleges, 22*(1), 151-160.

Sledge, C. A. (2005). Building information assurance educational capacity: Pilot efforts to date. *Carnegie Mellon University, Software Engineering Institute*. https://doi.org/10.21236/ADA452451

Target, A. C. (2010). *Cybersecurity challenges in developing nations* [Doctoral dissertation, Carnegie Mellon University].

TEMPUS. (2013). *Report on EU practice for cyber security education*. https://ecesm.net/sites/default/files/Dev%201.2.-v1.4-FINAL.pdf

Tidewater Community College. (2017). *TCC to offer first cybersecurity apprentice education in Virginia*. https://news.tcc.edu/cybersecurity-apprenticeship/

Von Solms, R., & Von Solms, S. (2015). Cyber safety education in developing countries. *Systemics, Cybernetics and Informatics, 13*(2), 14-19.

Wright, M. (2015). Improving cybersecurity workforce capacity and capability. *ISSA Journal*, 14-20.