JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2019, 1–19
doi: 10.1093/cybsec/tyz001
Research paper

Research paper

Cybersecurity education in a developing nation: the Ecuadorian environment

Frankie E. Catota[1,2,*], M. Granger Morgan[1] and Douglas C. Sicker[1]

[1]Department of Engineering and Public Policy, Carnegie Mellon University, PA, USA, and

[2]Engineering Department, Universidad Internacional SEK, Quito, Ecuador

*Corresponding address: 5000 Forbes Ave., BH 129, Pittsburgh, PA 15213, USA.
Email: frankie@cmu.edu; frankie.ec@outlook.com

Received 3 November 2016; revised 26 September 2018; accepted 20 December 2018

Abstract

The ability to prevent successful cyber attacks against a nation's critical infrastructure depends on the availability of a skilled cyber-literate workforce, and therefore, on an educational system that can build such capabilities. While it is possible to hire foreign nationals or to outsource many operations, this is not a sustainable solution and raises other concerns. The current literature provides strategic guidelines on developing a national cybersecurity workforce; however, there has been relatively little research on identifying the factors that are responsible for impeding the development of cybersecurity education in developing economies. Based on qualitative analysis of data from 28 semi-structured interviews with educational leaders from thirteen Ecuadorian institutions of higher education, this article explores challenges faced by the higher educational system of Ecuador in advancing cybersecurity education. On the basis of the insights gained, opportunities for enhancing the system are then identified and discussed. Today cybersecurity education is mostly elementary in Ecuador. Nationwide, interviewees at only four of the thirteen universities studied expressed some confidence in their institution's ability to provide students with reasonable preparation. The challenges that domestic cybersecurity education faces include: cybersecurity skills, structural capabilities, social integration, economic resources, and governance capacity. To enhance current preparation, there is an urgent need for a national cybersecurity education strategy that bolsters multiple initiatives as well as a multi-stakeholder space in which government, industry, and academia can actively work together to address national cybersecurity educational requirements. Further initiatives should include strengthening educators' training and cybersecurity academic programs, as well as advocating research (and development) capabilities and cybersecurity awareness. Recent revisions in Ecuador's higher education system offer a timely opportunity to advocate for advancing academic cybersecurity competencies.

Key words: cybersecurity education; Ecuador; capacity building; cybersecurity workforce; developing nations

Introduction

Many recent reports of cybersecurity attacks highlight the prevalence of a wide range of malicious activity and point to the growing sophistication of cyber threats. These threats carry many ramifications for governments, organizations, and individuals across the globe. Frameworks designed to address the cybersecurity challenge at a national level focus on the need to build cybersecurity capabilities to achieve greater cyber readiness. In these models, developing a cybersecurity workforce is identified as an essential prerequisite to developing such capabilities. Confronting cyber challenges requires people with skills to detect and respond to cyber threats, and protect critical infrastructure [1]. Accordingly, nations have designed

strategies to develop essential human talent, including cybersecurity education, training, and certifications. These strategies are designed to ameliorate the current shortages of skilled professionals that even countries with advanced preparation in cybersecurity often face.

Building workforce capacity requires the development of strategic and operational structures that are often not available in developing nations. Hence, understanding the constraints faced by those nations is an important first step in identifying courses of action to advance cybersecurity. By conducting a qualitative *thematic analysis* of interviews with leaders in higher education, this study explores challenges faced by the higher educational system of Ecuador in cybersecurity education and subsequently examines opportunities for improvement. We offer answers to the following questions: what are the challenges that universities face in order to provide cybersecurity education in a developing country (specifically, Ecuador)? How can this country enhance cybersecurity education to support national cybersecurity capabilities? While this study was inspired by the barriers to security incident response we found in our previous work on the Ecuadorian financial industry, the results of this investigation should help improve protection of a range or Ecuador's private and public critical cyber infrastructure.

Ecuador follows the Spanish educational model. The higher educational system is composed of public and private[1] institutions, 50% of which are located in two major cities. Over the last decade, the country has been experiencing a transformation of its educational system. The government has implemented a regulatory framework to assess, control, and improve the quality of higher education [2]. In 2012, 14 universities were closed down after a second assessment found that these institutions lacked academic quality [3]. Since 2015, universities have been standardizing and updating their academic programs to comply with government requirements. However, these efforts are focused on improving general education, and are not specifically linked to education in cybersecurity methods and strategies. At the undergraduate level, some aspects of information security are taught in computer science, computer networks, and telecommunication programs. At the graduate level, there have been two specialized master's cybersecurity programs, one of which started in 2005 (MS in *applied information security*) by incorporating teaching done by specialist professors who come from other Latin American countries, such as Chile, and from Spain. This strategy of importing instructional talent continues today.

In the interview we conducted for this study, many Ecuadorian academics described the current state of cybersecurity education in the country as insufficient. While some educational institutions have not even started initiatives in cybersecurity, others struggle, mainly because of a lack of instructors with the necessary skills. Ecuador needs to develop a national cybersecurity education strategy to guide its cyber workforce development in both the short- and longer-term.

The balance of this article consists of eight sections: Section 'Literature review' addresses related work; Section 'Method' describes the research method employed; Section 'Perceptions on cybersecurity' presents respondents' perceptions on cybersecurity; Section 'Current cybersecurity education' explains the current situation in cybersecurity education in Ecuador; Section 'Factors driving cybersecurity education' identifies circumstances driving cybersecurity education in the nation; Section 'Discussion of findings' discusses research findings; Section 'Strategies for advancing cybersecurity education' introduces strategies for improving cybersecurity education; and Section 'Conclusion' offers some concluding observations.

Literature review

Many aspects of cybersecurity education have been addressed as part of national capacity building strategies, workforce development, and education-specific studies. Issues related to both the scarcity of cybersecurity professionals and strategies for improvement have been comprehensively documented in developed economies by the US Department of Homeland Security, the US National Institute of Standards and Technology (NIST), the US National Security Agency, the UK Government Communications Headquarters, the United Nations, the European Union, "think tanks" such as the RAND Corporation, Booz-Allen Hamilton, and the SANS Institute, among others. However, literature that is specifically focused on similar issues in developing nations is modest.

The USA recognizes education as a crucial component of its national cybersecurity readiness and has established legislation[2] and strategies[3] to develop cybersecurity education and a workforce. The National Initiative for Cybersecurity Education (NICE) was created to improve the long-term cybersecurity posture of the USA [4]. NICE addresses awareness, formal education, professional training, and workforce structure. In supporting this initiative, NIST developed the National Cybersecurity Workforce Framework, which provides a common language (lexicon and taxonomy) to be used by academia, industry, and government [5]. This includes seven cybersecurity areas of provision, job functions, and associated skills, which some US universities are using to develop academic programs. These programs are also supported by qualified workforce (i.e., people with significant cybersecurity experience) that US educational institutions can find in the industry. In fact, educational institutions participating in RAND's survey (2014) report not having problems in recruiting professionals from the cybersecurity market despite high industry salaries [6]. Nevertheless, the USA still struggles to effectively develop cybersecurity workforce. A study by the SEI reports concerns regarding appropriateness of cybersecurity practices applied by the workforce in the workplace as well as concerns related to the workforce readiness to effectively protect IT infrastructure [7].

In the UK, enhancing cybersecurity education and skills is one of the four main components of the national program (2011) to secure cyberspace [8]. UK cyber policy has incorporated cybersecurity at all levels of education starting at the age of 11 years. Current strategies include, supporting schools (e.g., "Girls get coding"), providing resources (e.g., The Open University), apprenticeships, support for undergraduate and postgraduate research, cybersecurity career opportunities, and internships. In 2013, a self-assessment (including interviews in academia) to identify challenges in implementation of their program found that present gaps in cyber education should be overcome in less than 20 years [9].

The European Commission Tempus Project (2013) studied approaches to formal and informal education, and public education. Formal education considers several areas of cybersecurity instruction at universities in the USA, Europe, Asia, and Australia, while informal education addresses professional training and domain specific training (e.g., Supervisory Control and Data Acquisition Systems). Public education spans awareness and informative

1 Private universities often receive partial government support.

2 Border Patrol Agent Pay Reform Act of 2013, Federal Cybersecurity Workforce Assessment Act of 2015.

3 Federal Cybersecurity Workforce Strategy (2016).

campaigns. Conclusions indicate that: (i) countries at the forefront in cybersecurity, such as the USA, Canada, the UK, and Australia incorporate cybersecurity education at every stage of academic instruction; (ii) cybersecurity education has strong ties with military and security agencies—predominantly in the USA; and (iii) there is a gap in both domains of education (formal and informal), and some countries have not even started their cyber educational development [10].

In a comparative analysis between Czech Republic and Lithuania—with a focus on cyber legal issues—Harasta (2013) [11] reports a lack of citizens education regarding cyber threats in both countries.

In Finland, Lehto (2015) conducted a survey to assess education and research in cybersecurity at nine universities and research centers and summarizes the approaches and areas of strength in each. Findings show that while cybersecurity education is improving in Finland, the cyber educational system lacks strategic objectives. Universities provide education based on particular initiatives, and efficiency in collaboration as well as a solid structure bolster cybersecurity research. However, institutional initiatives in cybersecurity education do not envision national strategic proficiencies [12].

Among developing nations, the literature addresses some aspects of cybersecurity strategies and capacity building, including cyber education for children, specific areas of teaching, and regional cybersecurity practices. Newmeyer (2015) addresses elements for a national cybersecurity strategy for developing nations, which includes education and cybersecurity awareness [13]. Muller (2015) suggests areas in which developing countries find challenges to build cyber capacity. These include institutional stability, building knowledge, legal framework, and private sector cooperation. When adopting strategies from advanced countries, developing nations should consider their ability (knowledge, capacity) to effect strategies in a timely manner [14]. Cyber education is briefly mentioned as a component of the discussion and as an essential part of securing cyberspace.

Kortjan and Von Solms (2012) identify cybersecurity educational gaps in the South African national cybersecurity strategy based on a high-level comparison with USA and UK initiatives. Suggestions include identifying milestones, allocating resources, and establishing a plan with allocation of responsibilities [15]. Von Solms and Von Solms (2015) propose a cyber safety curriculum for children (based on videos) in order to educate and help them protect their privacy on the Internet (e.g., social networks). Emphasis is placed on the fact that some African governments do not necessarily devote resources to this educational endeavor as in developed economies [16].

In Puerto Rico, Curbelo and Cruz (2014) discuss the appropriateness and conditions under which *ethical hacking* courses should be taught in university undergrad levels. The study advocates incorporating both courses on *ethical hacking* and *ethics* together for undergraduate degrees [17]. Lastly, based on an online survey and Oxford's Cybersecurity Capability Maturity Model, together the Organization of American States (OAS), Inter-American Development Bank,' and Global Cyber Security Capacity Center (2016) report current efforts of 32 Latin American and Caribbean nations in five areas of cybersecurity, one of which is cybersecurity education. Some representative educational initiatives are summarized for each nation. Here, Ecuador reaches mostly the second level (i.e., formative) in the cyber education dimension (although details are missing given the nature of the report) and lack of awareness of society is highlighted as an important challenge [18].

In summary, most related research concentrates on aspects of education as a component of cybersecurity capacity building, focusing more comprehensively on high-income countries. An assessment of cybersecurity education and research in universities at the national level is available for Finland and the UK. Despite recent efforts to address cybersecurity capabilities in less equipped economies, little work has been done to uncover particular issues preventing national cyber capacity building. Hence, this study focuses on developing a deeper understanding of the challenges arising in the environment of a specific developing nation in the context of cybersecurity education.

Method

This study focuses on cybersecurity education for information technology (IT) students, including undergraduate and graduate students in programs in computer science (CS) and computer networks (CN). Most operational jobs that address cybersecurity issues in Ecuadorian financial and other industries are filled with individuals from these backgrounds. Based on the key elements depicted in Figure 1, we prepared interview guides to conduct semi-structured interviews. We also conducted desk research to identify strategies for improvement that have been implemented by other countries that might be suitable for Ecuador.

Interviews were supplemented with cross-tabs to explore: (i) perceptions and awareness about cybersecurity in the local ecosystem—the financial sector was selected as a starting point; (ii) current practices in cybersecurity education; (iii) factors that prevent initiating and improving cybersecurity education in institutions; and (iv) potential strategies that the Ecuadorian educational system could pursue.

Data collection

Seventeen universities and polytechnic schools[4] were contacted in the three largest cities, and one medium sized city, in Ecuador. One decline, 16 agreed to participate, and interviews were successfully conducted at 13. In the remaining two, while our requests for participation were initially accepted, subsequent communication attempts were ignored.

This purposeful sample corresponds to 31% of all Ecuadorian universities offering degrees in CS and includes most leading educational institutions in the nation. The sample is composed of three universities of category A (100%), eight in category B (42%), one in category C (7%), and one in category D (17%).[5] Our analysis mainly focuses on categories A and B so as to span a diverse group of universities with higher standards in education. In these institutions, 28 representatives of public (68%) and private (32%) universities were recruited in person (75%), by email (21.4%), and by phone (3.6%) between 16 July and 27 August 2015.

Twenty-eight respondents were interviewed, 27 in person and one over the phone. Respondents (24 males and 4 females) whose ages range between 34 and 65 contributed to the study without compensation. All respondents authorized recording of interviews with

4 In this article, we use the term 'universities' to describe both.

5 The Ecuadorian government assessment (2013) has classified (ranked) universities in categories: A (highest), B, C, and D according to quality standards. Although a new (voluntary) assessment and categorization of (only) thirteen universities occurred in May 2016, we maintained the 2013 categorization because it was used as a criterion to design our study in 2015.

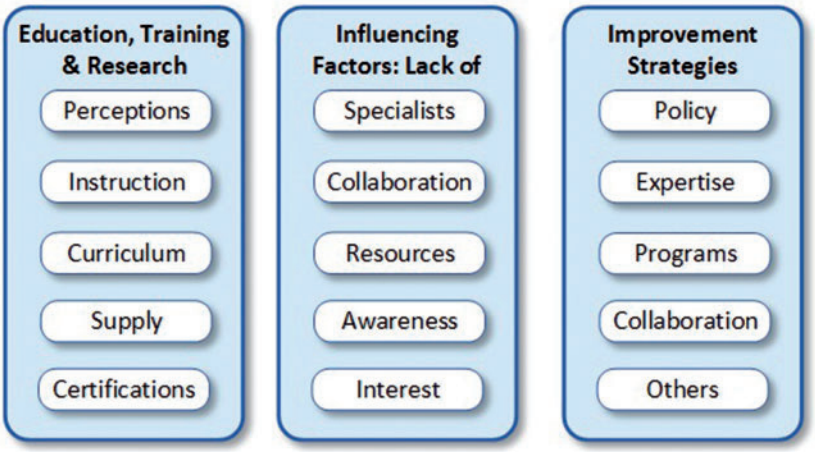

Figure 1: Key elements of cybersecurity education

average duration of 62.8 min (std. dev.: 12.6 min, range: 45–93 min). Table 1 presents respondents' academic background, role, and education.

We transcribed all the interviews. The transcription process used specialized software (F5 Transkript), rules of transcription, timestamps, and technical and domestic terminology. Steps were taken to protect respondents' privacy during recruitment, interview, transcription, and analysis.

Data analysis

We conducted a standard qualitative text analysis of all transcripts using *thematic analysis*. This approach does not focus on reporting statistical significance but rather on an exploratory examination in order to uncover patterns, themes, and categories important to the problem we investigated. The analysis included text coding (annotating), categorization, interpretation, and reporting [19]. Coding was performed in three stages: (i) coding three interviews on paper to develop our first version of the codebook, (ii) performing an inter-coder agreement process on a subset of the interview transcripts, and (iii) coding the complete dataset by using qualitative data analysis software (Maxqda).

The main purpose of conducting an inter-coding agreement analysis (*consensual coding*) was to obtain benefits from the interaction of two coders to identify conflicting annotations and to treat them properly before coding the entire dataset. While consensual coding does not necessarily focus on calculating interrater-reliability coefficients [19], in order to be informative about the process we report those metrics below. The second coder, a Spanish native speaker, had formal education in written text comprehension in his native language and was familiar with the data since he transcribed about 70% of the interviews.

Accordingly, we performed agreement analysis for six interviews in four steps: (i) creating a first draft of the codebook and an index of the codebook (a summary of codes on one page), and training a second coder in both understanding the codebook and coding text; (ii) coding interviews to identify disagreements; (iii) discussion of disagreements; (iv) reviewing and updating the codebook. We followed this procedure iteratively for each interview. For the last interview the metrics were: code coexistence 80%, code frequency 68%, and segment agreement 59.8% at 95% correlation. The following three interrelated sections present the results.

Table1. Interview respondents' profile

Academic background	*N*	Role	*N*
Computer science	10	Director	10
Telecommunications	4	Professor	10
Software engineering	3	Coordinator	5
Information security	3	Dean	2
Business administration	3	Chief	1
Education	2		
Business intelligence	1	Education	*N*
Informatics	1	Master	22
Network connectivity	1	PhD	6

N: Number of respondents.
Total respondents: 28.

Perceptions on cybersecurity

Interviews started with a brief introductory inquiry to learn about the level of the participant's awareness of cyber threats and to obtain their perceptions of current cybersecurity practices in local financial services.

At this time, cybersecurity is seen as an emerging issue and is increasingly becoming relevant in light of well-known worldwide data breaches as well as cyber-attacks on local private and public infrastructure, such as fraud driven by phishing in financial services and hacking of government websites.

Perceptions of cybersecurity in financial services indicate that the sector has been improving security measures lately, but there is a need for further enhancement. Often, respondents intuitively assessed security appropriateness based on perceived effectiveness of authentication methods used in online financial services. Because of improvements implemented by more robust institutions in this area, including multi-factor, biometrics, limited time password, one time password, out of band communication, SMS and e-mail verification,

and selective authentication,[6] respondents assess the security of their bank is now slightly inappropriate (18%), slightly appropriate (36%), appropriate (39%), or absolutely appropriate (7%).

Authentication methods not only work as a countermeasure to prevent malicious actors from breaking into banking systems, but they also signal the security posture of institutions, which can foster or undermine customers' trust. A few interviewees described personal experiences with—publicly known and even privately managed—financial incidents and highlighted uncertainty about the appropriateness of institutions' internal security. While some institutions have improved, they perceive that others still need to do so. For instance, they observe institutions still having virtual keyboards, proved to be ineffective in the presence of screen-loggers [20], for customers to login to online banking websites. Areas of improvement were observed in aspects of usability of authentication methods [Respondent R41],[7] internal security practices [R49], propagating advanced authentication methods among smaller institutions [R58], and willingness to pay for security [R61].

Current perceptions of cybersecurity are important to understand because they can shape awareness and, therefore, the position that university programs, and individual academics, take with respect to cybersecurity instruction.

Current cybersecurity education

Academic instruction

Many computer science students in Ecuador are educated in a combination of software engineering and systems engineering. Some universities have separated those areas into two different programs. In both cases, teaching at most universities has focused on computing applications development and computing networks. In the past, security instruction was hardly been considered. Over the last six years, some universities have been gradually incorporating one or two security courses into their programs, but adding such courses often encounters some difficulties in practice. At the time of interviews, universities were updating or re-designing their academic programs because of government compliance requirements. Participants claimed that security content is being enhanced as part of these updates.

Currently, there are three main approaches for teaching security: (i) including one or two formal courses in the entire curricula; (ii) teaching security topics in other computer or network courses; and (iii) less formal methods, such as seminars and workshops. Among the academic curricula of surveyed academic departments 20% offer two security courses, half offer one course, and 30% offer no courses. Table 2 reports the names of the courses offered by 20 different university academic departments in which respondents work.

Often, security courses are offered during the final semesters of a student's program. In some cases, a security course is an elective, which produces an unwanted effect because students avoid taking it during the last semester (when for example they are concerned with searching for a job). Some students appear to believe this security course may be difficult and could jeopardize the completion of their studies [R34, R38]. For this reason, two additional courses have either been only occasionally offered (*forensics informatics*) or not taught at all (*design of secure applications*). In the second approach, security content is included in other information and communication technology (ICT) courses, such as *operating systems, computer networks, databases,* and *software application programing*. It was often argued that security should be addressed across several academic courses. This inclusion takes place depending on both the instructors' knowledge of the topic and their taking the initiative to address such content in the syllabus. This can change drastically when a skilled professor leaves the university. In both approaches, information security content varies among universities and departments. In approximate order of frequency, the topics respondents mentioned were:

- Generalizations of information security
- Security management
- Security in operating systems
- Network security (e.g., Wi-Fi)
- Perimeter security (e.g., firewalls)
- Attacks on applications (e.g., SQL injection)
- Auditing
- Legal informatics
- Ethical hacking
- Security in databases
- Security awareness
- Cryptography

Because it is based on recall, this list is likely not complete.

To better understand the capabilities of universities, we also presented participants with a list of areas of information security, including: secure coding, network security, IT systems security, security management, and incident response. Most interviewees believe it is more feasible to teach the first three areas, but were much less confident about teaching *incident response*. Occasionally, we observed some overconfidence by respondents when asked about how well their institution is teaching *secure coding*.

The third approach involves the use of informal initiatives to promote information security knowledge. Some universities organize seminars, presentations, and other activities[8] that promote information security awareness among students by bringing in external speakers. Such initiatives are reportedly very well received by students and raise interest in the field. Lastly, some security content is evidently covered in material related to professional certifications.

Table 2. Academic security courses

Course name	*N*
Information security	9
Network security	3
Security	2
Cryptography	1
Data security	1
Informatics auditing	1
Information security management	1
Legal informatics	1
Security technologies	1
Total	20

N: Number of academic departments.

Professional certifications

At the time of the interviews, all universities offered some level of support to students for professional training in Cisco networking

6 Sophistication of the authentication method is used depending on the sensitivity of the transaction being performed by customers.

7 In this article, respondents are identified as Rn; where $n = [34–61]$.

8 The first national contest in cybersecurity (capture the flag) occurred in December 2015, http://detri.epn.edu.ec

certifications such as Cisco Certified Network Associate. A few of them offer similar support for Microsoft and Oracle products, and fewer still for Linux. Support schemes vary among universities, which include providing content of the material required for certification as part of academic courses, granting credits for achieving professional certifications, and partial economic assistance for course preparation. In most universities, obtaining certification is optional. However, in one it is a requirement for graduation. Such support from universities has been promoted by demand for certified professionals in the labor market, by availability of instructors, and by free access to software. For example, Microsoft provides educational institutions with relevant licenses for free, which encourages teaching the practice of software engineering. As an illustration, here are some excerpts of interviews reflecting what was asserted.

> *In general, certifications are very valued in the local industry* [R50, R55]. *Certifications supplement professional education* [R46].

Conversely, no university in our sample supports training that leads to cybersecurity certifications. Access to security equipment necessary to support such initiatives was reported to be expensive. Others indicated that they have not even considered such an initiative for security.

> Specialized equipment to support training in security certifications is expensive. Microsoft makes license concessions to universities, but such initiatives cannot be found in makers of security technologies [R38]. There has never been a proposal to support security certifications [R41].

When participants were asked about the role of academia regarding professional certifications, most of them stated that it is beneficial because it fosters learning in professors and students. However, others indicated that such support is not consistent with the role of academia, although it may not hurt providing them as supplementary resources.

Research

Although there had been a few research initiatives, we saw very little evidence of academic cybersecurity research. Two universities' representatives reported having performed specific research projects in the past (e.g., authentication in a financial application), and another explained that it is starting research projects at the doctoral level—engineering PhD programs having only been instituted during the last two years in the nation. Beyond that, most initiatives come from students who propose undergraduate thesis projects related to information security.

To better understand potential research abilities and collaborative initiatives with industry, we also presented respondents with a hypothetical scenario: the creation of a Computer Security Incident Response Team (CSIRT)[9] that would use research capabilities in academia to support the financial services. Then, we asked their thoughts about the ability of academia to support such an initiative. Most respondents (58%) believe that right now there is not enough capability to host such a CSIRT, but it was stated that a collaborative initiative with the financial industry would be more viable.

Self-assessment

The majority of interviewees qualified undergraduate cybersecurity education as elementary, basic, limited, generalized, or insufficient. They justified their perceptions by citing lack of security content coverage, lack of security courses, and lack of practice (mostly information security theory is taught). The following are some illustrative comments:

> *Very little [about security] is taught* [R34, R43]. *There is no a security course* [R40, R49, R57]. *A [security] chapter in another course is* taught [R41]. *We have one [security] course* [R43, R47]. *Deficient, much remains to be done* [R57]. *There is no a course but chapters in three other courses* [R45]. *We have just some security chapters* [R58]. *Chapters in different courses are taught but informally* [R48]. *We do not get into details; security knowledge is very little* [R56]. *We have a shortcoming in security* [R38]. *We are starting* [R37, R59, R60]. *Student's security knowledge is not solid* [R55]. *Quality is the problem* [R61]. *I do not have a professor who can teach a course of this type* [R47]. *We are not specialized in information security* [R44]. *We teach theory but not practice [Many respondents].*

On the other hand, cybersecurity education was considered appropriate by four respondents because they have incorporated at least one security course, compared themselves to other institutions, or considered that what they offer is enough according to the goals and scope of the academic program.

> *Now, it is better; we have had two [security] courses since 2009* [R42]. *In this program [computer networks], since the beginning we have taught network security* [R50]. *We had a good security course and now we have another one* [R54]. *We are reinforcing theory of security although not its applications* [R58].

We observed that appropriateness of current security education was occasionally assessed in different ways. While a university offering two security courses considers that to be appropriate and sufficient, another institution considers offering just two security courses is not sufficient. Also, while one academic department indicates security teaching is improving, another department at the same university thinks this is not the case, which indicates that some departments (Computer Science, Computer Networks, and Electronics Engineering) at the same universities have different levels of expectation and preparation in security. In addition, conflicting opinions about appropriateness between two respondents of the same academic department occurred in one public university, which signals that appropriateness of security teaching needs to be defined and discussed at a department level. In summary, 86% of respondents indicated some level of weaknesses in academic security instruction. Table 3 depicts self-assessment of *appropriateness* by respondents in Likert scale. Appropriateness was defined as the perceived level of cybersecurity knowledge with which an undergraduate student leaves the university.

Ongoing changes

As noted, when we conducted the interviews all universities had been working to update academic programs because of a government mandate. The new Ecuadorian Educative Accreditation Policy for higher education (EAP-2015) requires universities to harmonize academic programs according to specific guidelines across the country. To comply with this rule, departments of computer science and

9 The terms CSIRT and CERT (Computer Emergency Response Team) are used as synonymous in this article.

Table 3. Appropriateness of security education

Likert scale	*N*
1 Absolutely inappropriate	0
2 Inappropriate	2
3 Slightly inappropriate	7
4 Neutral	6
5 Slightly appropriate	9
6 Appropriate	4
7 Absolutely appropriate	0

N: Number of respondents.

electronics and telecommunications across the nation created working networks (e.g., REDSIC,[10] RECIETA[11]). Those departments were working together to adopt a subset of common guidelines on their curricula. To take advantage of these changes, some respondents claimed they plan to include security courses in their new curricula. Another initiative, considered by a few universities, is to include security content in multi-purpose courses of specialization called *itinerary,*[12] which is offered in the last semester of undergraduate programs. However, it is unclear how some respondents plan to effectively operationalize these initiatives without cybersecurity specialists. In fact, improving the level of quality in cybersecurity instruction depends on a number of factors, which are discussed next.

Factors driving cybersecurity education

How cybersecurity education in Ecuador is conducted depends on the factors affecting universities' decisions to incorporate security content in CS curricula (e.g., demand) and on factors influencing universities' abilities to implement security instruction (e.g., lack of resources). Factors described in further sub-sections were hypothesized during our research design, so we asked explicit questions about them, whereas factors grouped in sub-section 'Other factors' were raised during the interviews, so they are not summarized in Table 4. All these factors are addressed next in order of their relevance, as highlighted by the interviewees.

Lack of security specialists

There are few educators with formal education in cybersecurity in Ecuador. Representatives of 20 universities' departments reported having no security specialists (45%), one (35%), two (10%), and three or more (10%). In the last case, however, some specialists are not necessarily teaching security because they are pursuing higher degrees or teaching something else. Many professors teaching security were educated during a time when local universities did not provide cybersecurity education, although a few exceptions are those educated overseas.

As a result of this shortage, security instruction and supply of cybersecurity skills suffer. Cybersecurity courses cannot be incorporated into the curricula when desired, and the quality of security courses is compromised when taught by non-experts since security content is often constrained in scope and lacks integration of theory with practice. That universities struggle to fulfill demand for cybersecurity is evident from the fact that: (i) students' requests for advice on undergrad thesis research have exceeded the capacity of universities, given the limited number of qualified advisors [R61]; (ii) MS security programs demanded by graduated students have not been feasible [R40]; and (iii) government requests for support in cybersecurity have not been fulfilled by a few universities [R55, R59]. The following interview excerpts illustrate these issues:

> We do not really have [security] specialists [R40]. Graduates ask for a master's program in security, but we do not have faculty to supply it [R41]. We can find people with experience in security but not educated in security [R49]. We do not have someone holding a master's in security but people familiar with the field [R58].

Several strategies have been adopted to overcome this professional shortage. At the undergraduate level, at least three universities have been using professionals who hold security certifications from industry as instructors for security courses, especially in the field of security management and auditing. For seminars and talks, two universities draw on specialists with practical experience who come from the government and two from an academic CERT. At the graduate level, master's cybersecurity programs have been using visiting professors from Spain, Mexico, Chile, and Argentina. Interviewees observed that the industry has followed a similar approach by importing specialists to solve specific needs. Nationally, the government has implemented the *Prometeo Program,* which temporarily brings scientists, including Ecuadorians living overseas (i.e., return policy), from around the world to improve general research in the higher education system. Yet, no university in our sample reported using this program in the field of cybersecurity.

Lack of interaction with industry

The level of interaction between academia and industry can be described in three groups. First, most participants (61%) believe communication between academia and the industry hardly occurs. Among interviews, the term "divorce" was metaphorically used ten times to describe such absence of relationship:

> There is a divorce between the business sector and universities [Seven respondents]. It would be great that after a few years the industry were integrated with academia [R42].

Additionally, 32% of participants noted some interaction with industry, especially regarding aspects of software engineering and computer networks. However, this interaction is limited and only one has received security requests from industry.

> Historically, there has been very little communication. Now, this communication is occurring, but still there is lack of feedback [R55]. We have agreements with industry for CS internships, but we have not worked on security projects yet. More support from the industry is needed [R58].

Two respondents mentioned having made agreements with private and public sector groups. They also have received requests for support in security. In our sample, interaction between academia and industry works better in the two less populated cities because it is more likely that people involved in both sectors know each other [R56, R60], whereas in the two largest cities interfacing appears to be more difficult.

10 *Red de Sistemas Computacionales*.

11 *Red Nacional de Carreras de Ingeniería en Electrónica, Telecomunicaciones y Afines*.

12 A last-semester course with flexibility to be adapted to specific needs of the curricula.

> We have research projects with about five organizations, public and private. But, since we do not have a security research team, we have not started many initiatives in the field of security [R60]. We have annual meetings with professionals from the local industry, and we do receive security requests from them [R56].

As a result of this lack of communication, opportunities for academia-industrial partnerships and understanding of cybersecurity demand have not developed. This barrier prevents collaboration concerning technical support and research funding. In this context, interviewees, some of whom were educated overseas, observed that the industry is not as involved locally with academia as it is in other nations.

> There is lack of support from the industry [R37, R54]. The industry has not been willing to fund initiatives; there is no commitment [R30]. The university has no agreements with the private business sector as those occurring in other countries [R57].

Also, universities have experienced difficulties learning what the industry needs in terms of cybersecurity skills. Because of the policy EAP-2015, universities have been taking steps to improve communication with industry, in particular, to learn about demand from areas of ICT to establish (or confirm) academic programs and design new curricula. However, respondents reported difficulties obtaining successful survey responses from industry independently, so they are now working in academic networks to improve results.

Insufficient understanding of cybersecurity demand

Comprehensive knowledge about labor market demand for cybersecurity is not available, and there are different perceptions in universities across the country. First, many assert that the private industry does not ask universities for security workforce (82%). Most universities do not see private firms approaching them to ask for support in security. They perceive that corporations prefer to look for specialists overseas, and, in particular, the financial sector does not ask universities for skilled workforce (92%). Second, and more broadly, there has been an eventual demand for security provision from industry, justice administration, or the government (23%). Third, demand for security training more often comes from students and alumni. Among them, very-well known attacks in the country (finance and government) raise interest. The first-born cybersecurity MS program, in fact, reports overflow of admission requests.

> We do not see many requirements to implement security [R45]. They [industry] do not ask for security engineers [R46]. They [industry] import specialists from other countries to solve their problems [R46, R61]. We know the business sector needs security professionals, but they [managers responsible for security] probably do not have the ability to ask for these professionals [R38]. The industry does not approach academia because they think it is not worth, so they prefer to search specialists outside [R39]. There is demand [for security instruction] from students, but there are no security industry positions [R38].

In the local market, demand for security is supplied, to some extent, by available specialists and consultancy firms, many of which are originally from outside the country [R46, R51, R61]. Respondents (42%) felt that today demand for security in the business sector is very low, so they fear that creating security programs for specialists may saturate the labor market rapidly. Others added that more security provisions are needed at the societal level.

> We feel the need, but there is little demand. It is less than demand for software engineers. If we launch a security master's program, the market will reach saturation. It is difficult to justify investment in a security professional [R53]. I do not think the business sector is aware of security risk, so there are no many available positions in that area [R48]. We need more security knowledge [R54]. We need security please! [R57].

Most visible and potential sources of cybersecurity demand are in the financial services and government. In the financial sector, the IT risk regulatory framework (2012, 2014) has been already shifting demand of security services. Regulatory requirements have become stronger in the sector in response to security incidents like fraud. In fact, some participants recognized the leading role of the financial sector in the nation. In addition, from our study on security incidents in the Ecuadorian financial services [21], we found that the financial and telecommunication sectors needed skilled professionals in a few areas, including secure coding, network security, and incident response. In the government, demand should be driven by the introduction of the Ecuadorian executive order 166 (2013) that makes implementation of ISO 27001 mandatory for public institutions.

Local demand for cybersecurity should be understood in two ways. First, institutions in the market need graduates with security knowledge incorporated into CS and CN training, which will allow them to perform their primary jobs while applying security principles. For instance, in the financial sector software engineers familiar with secure coding and systems engineers knowing secure implementation of IT infrastructure are desired [21]. Second, security knowledge at the specialization level is wanted for positions such as security engineer. Most respondents believe specialization is more feasible at the MS graduate level as opposed to undergraduate level, but accurate knowledge about demand is necessary before this MS process can begin.

> *Demand is the most important factor for us* [R38].

In brief, universities feel they are limited by both a lack of accurate knowledge about security demand and little demand driven by the business sector's security posture. As has been noted, recent universities' efforts to learn about industry requirements include surveys on areas related to CIT, but the focus has not been on security. Also, employers in the private and public sectors have different cybersecurity situational awareness. While some employers are discovering that they need individuals with cybersecurity skills, especially because they have already had harmful security experiences, others do not know what they need in terms of cybersecurity workforce. As long as the market demand for security is not clear, it will be difficult to advocate for cybersecurity academic programs, even if resources become available. Hence, it is essential that employers and educators collaborate to identify the workforce competencies needed in the workplace. Otherwise, in several educational institutions cybersecurity will continue to have low priority [R57, R61].

Lack of resources

Scarcity of resources varies among university departments and harms cybersecurity education when universities want to enhance such instruction. Here, three groups of respondents were identified. The first group (21%) feels strongly about inadequacy of resources. Two participants feel limited by current government regulation that control tuition rates, which impact universities' financial decisions. Others indicate that security instruction has or will have to compete with other CS courses for time and infrastructure.

> We cannot increase tuition. We do not have enough IT infrastructure [R47]. Acquiring labs dedicated to general purpose computing has higher priority than a security lab [R50].

The second group (66%) experiences some degree of resource limitation, which has a slight to moderate influence on their ability to teach security.

> We would need to invest in infrastructure, equipment systems, and licensing, but sometimes we prefer not investing in those things [R45]. We do have little problems with resources, but we are solving them. It takes time to get resources, but we get them according to priorities [R43].

In the third group (13%), respondents believe they do not have important economic constraints that prevent them from providing security education.

> We do have budget for research. Having resources is not a problem [R42]. Here, there is lack of infrastructure because of deficient managerial issues; lack of resources is not the problem but the mindset [R39].

Economic constraints impact the advancement of security knowledge mainly because they preclude the establishment of security labs and hiring specialists to teach security. Most universities do not have a well-equipped laboratory to teach cybersecurity practice. In fact, 46% of respondents explicitly mentioned lacking a security lab as an important barrier to teach cybersecurity. Only 11% recognized having security labs, although some admitted insufficiencies, such as little sophistication or lack of knowledge about the equipment [R38]. Interviewees argued that specialized equipment suitable to teach security is very expensive, but they also recognized availability of open source tools to solve particular needs.

> There are many things we cannot teach because there are no labs. Allocation of resources for this aspect [security] is very low [R61]. We do not have security labs [R35, R37]. We need to implement new labs [R38]. We do not have specialized labs [R54]. Security equipment is even more expensive now because of the recent increase on import taxes [R50]. We do not have labs. We could buy something but not equipment. It is difficult to conduct lab practices [R59].

Moreover, given economic limitations, ability to temporarily incorporate specialists to teach security content is even harder. Universities cannot match business sector salaries. On a few occasions, however, a few universities have obtained specialized support—especially for seminars or talks—because some specialists had motivations other than income (e.g., affinity for teaching, established relationships), although this is not the rule. Another source of speakers for talks, reported by two universities, is specialists with practical experience coming from the government at no cost.

> Many times, when we have tried to bring professionals there has not been a way to cover the payments, unfortunately [R55]. Although there are a few specialists willing to come and collaborate, many times we cannot pay a specialist as the industry does [R53]. I cannot pay a professional asking $50 per hour [R40]. We used to obtain specialists from the private sector (which always asked for a payment), but now it is much easier to get speakers from the public sector [R41].

Consequently, security teaching in ICT programs and potential areas of research are impacted, particularly in those universities responsive to the need for improvement. In other cases, economic factors prevent them from taking the initiative. Nevertheless, the economic factors are not always the biggest barrier, especially when considering establishing an academic security program where market demand takes precedence.

Government intervention

Here we address some issues driven by current national policies that can potentially impact cybersecurity education, and subsequently we describe respondents' feelings regarding government intervention as an instrument to advance cybersecurity education.

First, interviewees feel that some government policies are improving general education and fostering general research. Nevertheless, they pointed out the following unintended consequences for cybersecurity education.

Over-regulation. A few respondents feel that universities are over regulated now, and that they have lost their autonomy to make some important decisions. In fact, creation of new undergrad programs requires government authorization, and it could be more difficult to implement, especially when they are not included in the government framework. At the master's level, participants observe that creating a security specialization is more feasible although it will take time to obtain approval [R49].

> Lately, we have lost some autonomy [R44]. There is more control now; in the past it was easier to implement changes [R49].

While it is recognized that total educational autonomy has not worked in the past in Ecuadorian higher education (see [3]), it certainly appears to us that university regulation has gone too far, has become too bureaucratic. This loss of flexibility will make implementing a security program at the undergrad level difficult. A better balance is needed between university autonomy and regulation.

Barrier to hiring specialists. Over the last few years, university professors have been required to have at least an MS degree in the discipline they teach. Although this policy is generally seen as very positive for improving quality, a couple of universities reported that some industry professionals familiar with security who had been supporting them before the policy was in place are no longer able to do that. In addition, a proposed policy mandating that professors teaching at universities must hold a PhD degree can potentially affect security teaching since specialists with such degrees and expertise in security are very rare in the country, in both academia and industry. [13]

Student dropout rate. Current policy to harmonize high school education has defined a unique set of courses for students. Hence, students planning to pursue CS programs face barriers to concentrate their education in higher mathematics, including algebra and calculus. As a result, many students have left CS programs after their first year because of deficiencies in such areas of knowledge [R46, R47]. This issue may potentially impact the number of graduates pursuing security learning.

Constraints on updating dying programs. Current regulations require programmed elimination of *non-standard academic programs*, which are types of programs not included in the new government framework for higher education. Therefore, modification of current curricula for such programs is not allowed, which prevents incorporation of additional security courses [R50].

Second, there is controversy as to whether or not the government should actively intervene to advance security teaching in universities. Supporters (43%) indicated that (i) universities need clear guidelines

13 In our sample of 61 participants, during interviews in both the financial sector and academia, we only found one PhD in the area of information security.

from the government to establish priorities and (ii) enforcement benefits the effective achievement of goals.

> Cybersecurity is a pending task from the government [R43]. Security is vaguely defined in the 'good-living' national plan [R59]. The government should help know about security industry needs [R44]. There have not been clear government policies about cybersecurity [R39]. There should be a policy from the government with mandatory topics [R37]. We need a governance security policy [R60].

Conversely, others (43%) believe that the government does not need to be so prescriptive because (i) there is already too much oversight by government agencies, and (ii) universities should communicate with the industry to learn about security demand and act accordingly.

> Government should not intervene [R41]. There is excess of intervention [R54]. Although some regulation is good, over regulation is bad [R53]. More important than government intervention is improving interaction between industry and academia. The government may not need specifics about the industry needs [R48].

Beyond the industry, the fact that the government has widely been advocating the use of ICT in public services signals an implicit message to universities about the need for developing security capabilities to protect citizens' information [R60]. Overall, government intervention is not only seen as a set of policies guiding cybersecurity but also as vital support to operate education and training in cybersecurity.

Lack of awareness

Despite the interviewees' general argument that institutional awareness exists, a few argued that there is insufficient awareness of the specific needs for cybersecurity education. Before government intervention, two universities reported having academic programs dating from 10 years ago, when cybersecurity was not a prominent issue. Nevertheless, they emphasized that this fact has recently been changing. Networking among university groups can be helpful to raise awareness among participants.

> Nobody here foresaw security [R59]. There is no awareness about what universities should have in terms of security [R45]. We have not discussed this [security] aspect [R52]. We see [security issues] in the news, but the administrative function is slow to react [R53]. More than anything else, the problem is lack of awareness and initiatives, including—us—professors. The steering committee should be 'the engine' showing concern and say: let us implement a curriculum containing security topics [R57]. We had not given importance to security, but now in our new curriculum design, it is very relevant [R60].

Beyond academic educational practices, interviewees offered two other sets of comments on security awareness. Suboptimal security practices in the university infrastructure were mentioned twice to highlight lack of awareness. An interviewee reported cyber attacks on the academic system that processes students' grades, and another one explained attacks to informational faculty websites. Another interviewee admitted that (unspecified) security incidents have occurred at the university and have been managed with discretion. Interviewees also commented on a lack of awareness at the societal level. Although several initiatives have been undertaken in the financial industry and government, there is a perception that the general population lacks knowledge about cyber threats and their implications. Raising awareness was cited as a means to follow a preventive approach to cyber insecurity.

> We can have robust technical security, but a security breach can occur because of users' miss behaviors. We need educational talks for all, starting at schools [R42]. We should establish awareness and not to wait for incidents to happen to start taking actions [R45]. Here I have to work very hard on employees' awareness, especially when teaching them about not sharing passwords, phishing, and web browsing [R57].

Other factors

Idiosyncrasy. A tendency to simply accept cyber risk was occasionally mentioned. This is consistent with Target's (2010) findings regarding attitude toward risk in developing countries [22]. Throughout multiple interviews it was heard that industry stakeholders learn and take actions to manage risks after they experience security incidents and consequences (of economic or another type), so situational awareness comes with a cost. This approach to cyber risk negatively impacts cybersecurity readiness from the proactive standpoint. One participant also suggested that a lack of a sense of community as a barrier to advance cybersecurity.

> Because of our idiosyncrasy, we had needed an incentive from the government to start doing research [R44]. It is difficult to advocate for security because our idiosyncrasy; people are going to say: yes, yes! I know security is important, but now I want to release my product to the market [R46]. I believe our idiosyncrasy is different from other cultures. We do not have much sense of community [R39].

Internal university policies. Some university policies prevent improvements in cybersecurity teaching and collaboration. In two institutions (one public and one private), academic leaders indicated that they have no ability to replace professors who lack formal security education yet currently teach security topics, even though there is another professor who does have formal security education. In addition, internal policies require that the university retains intellectual property on the outcome of research projects conducted by students (e.g., thesis). This rule has been found unacceptable by local industry [R38] and prevents innovation and collaboration. Lastly, particular and political interests were raised once as barriers to enhancing academic goals.

> Despite current efforts, the university model responds to political interests of groups and individuals [R39].

Lack of foreign language proficiency. This issue—mentioned once—prevents accessibility to current knowledge in cybersecurity and beyond, especially in faculty who have not received appropriate training in English.

> Here, I have professors who have been teaching for 15 years, and our level of English is very basic; however, up to date topics [in areas related to CS] are available in English [R37].

To supplement what has been discussed above, Table 4 presents a distribution of the level of influence of factors preventing cybersecurity teaching that we had hypothesized in our study design. The level of influence of a factor should be understood as the degree or extent to which that factor has contributed to (a negative situation) preventing cybersecurity education. Responses were given on a Likert scale ranging from (1) *not at all influential* to (7) *extremely influential*. For instance, 12 respondents reported the factor

Table 4. Level of influence of factors on preventing cybersecurity education

Factor | Likert scale	1	2	3	4	5	6	7	Score[a]
Lack of specialization of professors	0	1	3	0	4	10	10	5.8
Lack of feedback from industry	1	1	0	3	6	9	8	5.5
Low availability of professors	3	4	2	2	6	4	7	4.6
Lack of resources	0	2	6	6	8	3	3	4.5
Lack of awareness of universities	4	3	1	6	3	8	3	4.3
Lack of government intervention	5	1	2	6	6	3	5	4.3
Lack of students' interest in security	12	6	4	2	4	0	0	2.3

Likert scale: (1) not at all, (2) very low, (3) slightly, (4) neutral, (5) moderate, (6) very, and (7) extremely
[a]Weighted average computed as the number of respondents by the Likert scale respectively.
Total number of respondents = 28.

"student's interest in cybersecurity" as *not influential at all*. This means that respondents believe that "students' interest" has not been a contributory factor to preventing cybersecurity education at their universities. Conversely, 10 respondents reported "lack of specialization of professors" as *extremely influential*.

Discussion of findings

It has recently been suggested that no country is fully prepared to meet the cybersecurity challenge [23]. While some developed nations with a higher level of national cybersecurity performance have already started stronger workforce and educational programs to foster such preparation, studies suggest that many less developed nations have moved slowly to develop cyber capacity [10, 18]. In this study, we have reported on the current cybersecurity educational status of Ecuador and the specific factors contributing to current conditions. Data relevant to our analysis were collected through semi-structured interviews with 28 key respondents (professors and leaders) from13 universities (including most leading universities) across four cities in Ecuador. This is a purposeful sample comprised by individuals with first hand knowledge that helped us understand the problem [24]. From these data, we have identified common themes relevant to answering our research questions, and subsequently established relationships among these themes to obtain categories. These themes emerged among participants during the interviews as common issues. The value of such themes for our investigation relies on the source and the rigorous qualitative analysis we followed (e.g., sampling included site, interview role, and institution triangulation, and coding included *intercoder agreement*). When presenting the themes through the article, we have often provided citations making references to what was said by interviewees. Our conclusions are all based on the analysis of the aggregation of interviewees' responses, which of course reflect interviewees' perceptions. That many of those perceptions reflect a significant similarity across interviewees and regions suggest that they reflect some underlying realities.

Cybersecurity education is mostly at an elementary level in Ecuador. Nationally, at only four out of thirteen universities respondents feel some confidence about having made reasonable preparations, no undergraduate academic cybersecurity programs exist, and there are just a few graduate initiatives. The challenges that cybersecurity education currently faces mainly involve structural capabilities (e.g., skills), community integration, uncertainty of demand, lack of awareness, economic resources, and governance.

In undergraduate programs, most security content is integrated across several courses in CS and CN, but such integration is informal since, very often, academic instruction depends on instructors' decisions, knowledge and security skills. Lack of coordination among faculty can foster redundancies and/or gaps in security content. Although some security courses do exist, in many cases they were reported to be incomplete in scope or depth, especially because of lack of expertise or resources such as labs. Relevant security content for protecting critical infrastructure is being omitted. In fact, pertinent content such as *incident response* was virtually absent. Initiatives faced by universities do not include a common national vision, which is consistent with Lehto's (2015) findings in Finland [12]. Therefore, quality, completeness, and relevance of security content are compromised. At the graduate level, although there we found two active MS cybersecurity technical programs (and another one with focus on cyber defense has been announced), even these appear to be insufficient.

The results of the interviews suggest that there is a shared perception that university priorities, lack of specialists, lack of institutional flexibility, and lack of understanding of demand prevent academics from advancing cybersecurity education. Educating in cybersecurity is not only a matter of having capabilities but also requires decisions to assign higher priority to such endeavors. In addition, introducing security content in curricula competes for resources and time allocation with other academic content inherent to CS or CN programs, which also discourages augmenting cybersecurity knowledge. In the research arena, recent efforts to advance cybersecurity initiatives include a recently created PhD program in CS with information security as one of its research specializations, just a few undergraduate projects, and several undergraduate and graduate theses.

The lack of cybersecurity specialists at universities is one of the biggest issues limiting the ability of institutions to provide cybersecurity instruction. Overcoming this barrier is complicated by strict policies that prevent universities from incorporating industry professionals without graduate degrees, high security professional rates, and the national shortage of skilled cybersecurity professionals.

We fund that the lack of communication and collaboration with local industry limits improvement and adaptation of academic programs and the initiation of research projects that could properly respond to societal needs. Although government intervention has helped take the first steps to address this issue, there is a virtual wall between universities and the business sector that impedes collaboration. This issue is more serious in larger cities than medium-size or small cities.

When working on the research designing for this paper, we of course began with a number of hypotheses about what we would find. We expected to find a lack of cybersecurity workforce at universities as it also occurs in the local industry, but the extent to which lack of interaction between universities and industry has been

happening across several educational institutions was a finding we did not expected. Also, while economic and human resources to strengthen cybersecurity education are prevalent factors in developing cybersecurity workforce, we found that having such resources does not guarantee success. Some of the barriers that undermine resources availability are inadequate university policies (e.g., inability of universities to assign educated professors to teach cybersecurity courses even when having them), particular interest of groups and individuals, and inadequate administration of economic resources.

While lacking educators trained in cybersecurity was a barrier we expected, we also found that a few universities have initiatives that try to compensate such limitation. Unfortunately, the courses being taught are somewhat limited (e.g., only one university reported teaching a course on cryptography). Furthermore, we expected some reluctance from interviewees to recognize weaknesses in their ability to provide cybersecurity education to students, but we found that most interviewees did not have problems recognizing and sharing issues unknown for the investigators, which we sincerely appreciate.

Moreover, understanding of cybersecurity demand has been mostly based on academics' perceptions, including observations (the media), experiences (security incidents), feedback from students and alumni, and eventual consultancy (security or educational) projects in the private sector, especially academics who are more specialized in the cybersecurity field. Regarding current perceptions that suggest low demand, we observe two plausible reasons: (i) some universities do not experience direct demand because industry often needs to solve specialized problems in a timely manner, so they look for support somewhere else (there is evidence of this in the financial sector); and (ii) the security posture of some industry sectors does not seem strong. Recently, surveys in areas of CS and CN were reported, where some cybersecurity needs arose. Isolated university efforts on surveys are not as effective as those conducted by university networks. Lastly, other barriers, less often reported, are the language barrier that impedes access to up-to-date knowledge in cybersecurity, university policies that prevent collaboration, and administrative weaknesses.

Although there are no universal, accepted standards against which Ecuadorian cybersecurity education can be judged, there exist global references proposed by developed nations that can provide insights. According to the NSA and the DHS in the USA, academic excellence in Information Assurance[14] can be achieved through: (1) partnerships with educational institutions, (2) treating IA as a multidisciplinary science, (3) encouraging the practice of IA, (4) research in IA, (5) an IA curriculum that influences outside the university, (6) faculty involved in IA practice, research, and contribution to the literature (7) availability of state-of-the-art IA resources, (8) an academic program with IA concentrations, (9) a center for IA research from which IA curriculum is emerging, and (10) IA faculty devoted full time to IA [25]. In Ecuador, areas (4, 6, 8), and (10) are partially covered by only the most mature universities in our sample, and need to be dramatically improved. The development of the rest of areas should be envisioned in Ecuadorian universities that want to excel in cybersecurity education, but these areas need to be prioritized with the feedback from the local industry.

Beyond the actions performed by universities, national cyber security capabilities can be judged by using the Oxford Cyber Capability Maturity Model.[15] This model has five dimensions, one of which is cybersecurity education. Maturity is expressed in terms of five levels: start-up, formative, established, strategic, and dynamic. According to a high-level investigation performed by OAS in Latin America, cybersecurity education in Ecuador would reach the *formative level* because of limitations found in educational opportunities and technological development [18]; nevertheless, details that lead to such conclusion are missing.

Our study has not incorporated many views from universities with weaker academic standards (our purposeful sample includes only 7% of category C and 17% of D), we believe that sampling about 30% of the population with in-depth interviews, a mixture of participant's roles, and geographic triangulation provides enough diversity to capture a wide range of data for our analysis. Inclusion of additional institutions of those types (C & D) might reveal other barriers, especially associated with lack of infrastructure and academic resources. Nevertheless, it is safe to think that barriers, such as lack of specialists, collaboration, and understanding of demand, occur among those universities as well.

In this work we have mostly concentrated on CS/CN programs because most cybersecurity positions in Ecuadorian industry are filled with individuals coming from IT backgrounds. Evidence of this fact was obtained in the financial sector in our previous study [21], where we found that about 55% of interviewees (cybersecurity workforce in several roles, technical and managerial) working at financial institutions came from CS/CN programs. However, there are also others academic disciplines that contribute to that workforce—although in far smaller numbers. These include people moving over domestically or internationally from backgrounds in business and telecommunications.

We note further that cybersecurity education can take place in several areas of society. Both industry and the military can be important centers of preparation, especially training, but how successful that is depends on their current cyber capabilities and incentives to improve them. From some time now, financial institutions and large Internet Service Providers have been training their technical personnel in areas of cybersecurity since their managers feel specialized cybersecurity skills have been inadequately provided by most universities [21]. In the financial services major incentives to provide cybersecurity are domestic regulations and industry self-regulation (e.g., PCI/DSS). In the telecommunications sector, while cybersecurity regulations are not in place at the time of writing, some large ISPs are seeking to enter the security services market. In the military, the acquisition of cyber capabilities often depends on several incentives, including awareness of the risk imposed by cyber threats to national security, domestic political strategies, and geopolitical interests. It seems these factors have not yet pushed Ecuador to develop noticeable cybersecurity capabilities, at least not capabilities that have benefited areas outside of the military. Interestingly, our interviewees reported requests for support from the military [R55], so it appears that the military is seeking support for their cybersecurity efforts.

Accordingly, although universities with the most advanced preparation have developed particular strategies to address aspects of cybersecurity (e.g., MS programs, research initiatives, and specialized security courses), substantial efforts to strengthen cybersecurity education need to be pursued nationwide. These efforts need to take into account multiple areas in which cybersecurity education evolves.

14 Information Assurance is often not treated as equivalent to cybersecurity although they are related terms.

15 Similar to the Capability Maturity Model Integration (CMMI) for software development (see http://cmmiinstitute.com).

Strategies for advancing cybersecurity education

The successful improvement of cybersecurity education cannot be achieved as an isolated effort pursued only by universities. Rather a community-based effort will be required. Examination of relevant literature shows that national initiatives to advance cybersecurity education (and workforce capabilities) involve six dimensions: capacity governance, academic programs, training, certification, research and development (R&D), and cybersecurity awareness. In what follows, we introduce policy options framed in terms of these dimensions.

Capacity governance and multipurpose strategies

We begin by addressing national initiatives focused on governance and other initiatives that can impact several dimensions of cybersecurity education.

National cyber policy and strategies. Nations following a path towards improved cyber readiness develop at least one of these instruments to exercise governance in cyber education and workforce development: national cybersecurity strategies, national cybersecurity education initiatives (e.g., the US NICE framework), cybersecurity capability maturity models (e.g., the UK Cybersecurity Capability Maturity Model), and sector specific CMMs (e.g., the US Electricity Subsector Cybersecurity Capability Maturity Model).

The NICE framework has defined a lexicon for cybersecurity work, according to which cybersecurity-workforce functions span seven categories: securely provision, operate and maintain, protect and defend, investigate, collect and operate, analyze, and oversight and development [5]. While it is a well-known fact that worldwide there is lack of sufficient qualified professionals to support these categories of workforce functions, in the context of developing countries, skills related to *oversight and development*[16] are especially critical because these nations often lack policies and legal frameworks addressing cybersecurity issues, or such governance instruments have weaknesses (see [21] as an example). Consequently, Ecuador also needs to carefully consider such type of skilled workers to provide strategic planning and support governance initiatives nationwide, such as cybersecurity policies, standards, and cybercriminal law, for both the short and the long run.

To start improving cybersecurity education, Ecuador must develop a national cybersecurity strategy to provide governance guidelines and promote instruments that can develop cyber capabilities across academia, government, and industry. This strategy should prioritize areas of national critical infrastructure that require urgent attention, and, subsequently, identify cybersecurity knowledge and skills that schools, universities, and other entities need to develop for students, professionals, and the public.

To address the nation's most pressing requirements, Ecuador must allocate resources to educate instructors in computer systems and network security, implement cyber labs, and establish cyber research and development initiatives. Potential strategies to do this include education R&D grants, educational scholarships, and private funding. The Ecuadorian government is already offering international study funding in *applied information security*, so informative campaigns could be conducted to motivate students to pursue degrees in the field. Furthermore, equipment donations from public and private sectors should be encouraged [26]. Once the barrier to *lack of collaboration* between academia and industry is addressed, partnerships to self-fund research projects should be pursued.

Policies are needed that bolster a better preparation in math and hard sciences, and engage students with CS and cybersecurity content at early ages. Approaches followed by the USA, the UK, Israel, and others, could be used to build the foundation for better student performance in the long run, and would help decrease the current high student dropout rates in the first years in CS programs.

Secondary education students should learn about what CS and cybersecurity careers entail so as to attract them to the field. Informative campaigns and talks with CS and cybersecurity professionals should be encouraged [12]. Currently, because most students do not have early contact with CS courses in high school, nor an opportunity to hear informative talks or see demonstrations, they have misperceptions about CS programs [R43]. They think CS is just about learning software programs, so some students are discouraged from pursuing a CS career [R43].

Also, participation by women in cybersecurity education needs to be encouraged, both to expand the pool of potential experts, and to increase diversity. In two studies we have conducted, in financial cybersecurity and this research, the gender proportion of participants were 4: 29 and 4: 24 (female: male), respectively.

Private and public support. Incentives to promote participation of both the private and public sectors in advancing cybersecurity capacity building are needed. Presently, there is a substantial opportunity to improve industry support to the academic environment.

In Ecuador, most successful universities at developing ties with the industry are in small cities. Universities in major cities need to develop similar closeness by finding incentives that promote the initiation of mutual relationships with business sectors. Some mechanisms used by the first group of universities are: (i) establishing relationships with the industry through their alumni of whom universities keep employment tracking; (ii) finding pragmatic problems in the industry that universities can help solve and proposing projects that mutually benefit both parties (consultancy services). Additional initiatives to strengthen ties with the industry are:

- Engaging with university contractors with the potential to initiate technical ties. For instance, universities are customers of Internet Service Providers which potentially could provide technical feedback in cybersecurity matters in the telecommunications area.
- Bringing cybersecurity experts from mature academic centers, organizing conferences, and inviting people from the industry to approach them.
- Promoting courses that industry needs, initiating relationships, and following up on them.
- Starting university coalitions to approach industrial actors in a collaborative way.

Once such approaches are in place universities should pursue industry commitment for:

- Informing the most imperative industrial cybersecurity challenges and needs, as well as providing qualified answers to surveys. Acquisition of this relevant information by using both techniques would have an important impact on improving understanding about the demand for cybersecurity. This would also

16 "Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work" NICE.

allow universities to align curriculum with industry requirements.
- Funding cybersecurity research projects and other educational initiatives, such as cybersecurity labs.
- Supporting training of students through internships and apprenticeships (see sub-section 'Cybersecurity training').

Among initiatives to advance cybersecurity education, educators should act to assign a higher priority to developing collaborations with potential employers (private and public). As stated above, there are several potential benefits, one of which can be a better understanding of employee needs and another is financial support, a type of resource that is needed by a large portion of universities participating in our study.

Another important actor that needs to be involved in building relationships between academia and the industry is the government. At the national level, a multi-stakeholder space in which government, industry, and academia actively convene to address national cybersecurity educational requirements and strategies is urgently needed. Ultimately, private and public support to advancing cybersecurity education can be exhibited in many ways and so they are addressed across several dimensions of improvement in this article.

Institutional policies. Universities need to review and in some cases relax current policies (restrictive copy-right rules, limits on the allocation of specialist professors, elective status of security courses, and allocation of university funds) that prevent innovation and collaboration with external entities, preclude improvements in cybersecurity instruction, discourage students from taking security courses, and prevent investment in cybersecurity research. In addition, initiatives to foster inter-university collaboration are needed. Distributed cybersecurity expertise across university departments could consolidate efforts to strengthen cybersecurity knowledge at the institutional level. Today, at least one university is engaging in such a strategy, which allows students across different programs to get access to integrated cybersecurity courses with common content.

Academic networks. Beyond university level initiatives, networks have the potential to promote national and international collaboration. Countrywide, newly created Ecuadorian academic networks could be extended to actively address cybersecurity initiatives. In this domain, Chile has created a network of researchers and academics residing overseas and locally in order to foster collaboration to build capacity in several areas, including policy on science and technology, research centers, and scientific competencies [27].

CERT support. The term CERT comes from the first Computer Emergency Response Team (CERT/CC) established at Carnegie Mellon University (CMU) in 1988 for handling computer security incidents.[17] Worldwide, teams handling these types of incidents use either the term CERT, licensed by CMU, or generally CSIRT (Computer Security Incident Response Team). CERTs have been demonstrated to be suitable mechanisms to advance national cybersecurity in different economic contexts and in several *dimensions*.[18] In the USA, the NSF-funded *Information Assurance (IA) Capacity Building Program* at CMU, CERT/CC has supported multiple educational initiatives, such as training of university faculty in information assurance, developing survivability, and IA curriculum, as well as educational materials, establishing *regional academic clusters* (i.e., group of academic institutions in a US region) to foster collaboration, and promoting projects that assist colleges and universities [28].

For several years now, CERTs have moved beyond being an exclusive cyber resource that is only used by developed nations. CERTs now play an essential role in promoting cybersecurity knowledge and awareness in developing countries, such as Oman, Cameroon, Rwanda, India, and others [29]. Particularly, the national CERT in Oman, a country with a roughly similar GDP and size as Ecuador, supports cybersecurity training in several domains, including awareness and security certifications. Comparatively, Oman is a country with a roughly similar size and GDP as Ecuador—although Oman's per capita GDP is around 2.5 times Ecuador's according to the World Bank's data (2017).[19] Its national CERT has helped Oman become a leader in cybersecurity readiness in the Arab Region and third worldwide according to the ITU's cybersecurity global index [30]. This reveals that a developing nation can perform at a high level in recognizing cyber needs and building cyber capacity. A capable and well-operated CERT can be a key, multidimensional instrument to achieve such goals.

In Ecuador, potential CERT support to cyber education requires stronger capabilities. Although the nation now has an internationally recognized response team (EcuCERT), a CERT with regulatory power, its coverage is limited to only the telecommunications sector and certain areas in the public sector [21]. This CERT and the existing academic CERT (CEDIA[20]) could be strengthened to support cybersecurity education initiatives. Also, assistance from foreign centers with established relationships, such as CERTs from Uruguay and Brazil, could be pursued. Here, one very important initiative should be to train the educators in order to ameliorate lack of specialists at universities. In the mid-term, Ecuador should consider the creation of a national CERT to provide nationwide support.

Language competences. Both the novelty of cybersecurity as a field and the status of English as a *lingua franca*[21] for science and technology represent a challenge in academia, especially because it constrains knowledge transfer for non-native English speaking academics [31]. Although many local academics have English competencies, language skill remains a barrier for some educators. To foster accessibility in the short term, although insufficient and costly, forms of translation of very relevant scientific material into the local language can be explored, an approach that was followed by the Japanese to substantially improve their knowledge in the social sciences [32]. However, in the mid-term and long run, there is no substitute for implementing policies that foster English language skills.

Academic programs

Relevant content must be strengthened in both approaches for formal education in undergrad programs: (i) cybersecurity content integrated across core courses of CS and CN; and (ii) security topics addressed in cybersecurity courses. Here, in order to produce security specialization, a suitable option would be incorporating security content in *itineraries* as suggested by interview respondents. This initiative could provide professionals with solid knowledge in CS or CN and security skills as an additional proficiency, which is likely to be very valuable for the local industry since it often hires professionals to assign them multi-functional tasks, especially in medium size and small companies.

17 One of the authors, Douglas Sicker, collaborates regularly with the CMU CERT and through his leadership of CyLab oversees security research across all of CMU.

18 See Appendix 1.

19 https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

20 *Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado*.

21 http://globalcenters.columbia.edu/content/english-global-dominance-and-other-languages-higher-education-and-research

With appropriate support, designing and creating an undergraduate program in cybersecurity can be considered in at least one university with greater strength in the field, especially if it builds on expertise across university departments. Yet, before proceeding, careful analysis and understanding of demand in the Ecuadorian and broader Latin American labor markets are needed.

At the graduate level, the current capabilities of MS programs should be strengthened and new programs should be started in several cities where such programs are not available. In fact, when respondents were asked about initiatives for improvement, 42% of them believed that one early step to improve general security education should be starting MS programs in cybersecurity. Universities enjoy greater empowerment to make decisions at the graduate level than at the undergraduate level, including hiring specialists, because such programs are often self-funded. Exceptions are universities that cannot create graduate programs because of their lower categorization level.

> Making changes in masters programs is easier and dynamic, whereas in undergraduate level it is more complex [R49]. There should be more master programs in information security [R41].

Beyond CS and CN programs, the educational system needs to start incorporating academic security content in several levels and areas of education, including industrial systems, electronics, telecommunications, criminal justice, and business. In fact, respondents believe that business careers (e.g., MBAs) need to include instruction that helps inform cyber risk decisions, and similar feelings exist for areas of law enforcement to support investigations [R54].

While it is clear that the current lack of specialists is a barrier to undertaking such initiatives, over time it should be possible to improve the situation. Faculty members teaching areas of security at universities would benefit from current masters programs with augmented capabilities to specifically train educators. To operationalize this initiative, trainers with expertise in cybersecurity could be located within and outside the nation. Potential sources of experts are: (i) professionals who have received security education overseas, including those who are already established in the country and those who are returning home as part of government scholarship programs; and (ii) temporary imports of international subject-matter experts, a strategy now being followed by local security MS programs and also the government when promoting research in other areas of science. Of course, the current global shortage of cybersecurity professionals [33] could make it difficult to import professionals for the long term. One important advantage of these initiatives is that the curricula of national master level programs could be designed in a way that better fulfills the current needs of the Ecuadorian society. Another means are international online master degree programs providing standard education in cybersecurity.

Cross-border education[22] is recognized as an important instrument to achieve higher maturity levels of tertiary domestic education [34], and can be advantageous in the domain of cybersecurity as well. When importing academic curricula, care should be taken to adjust designs to the domestic context. Some interview respondents reported that they started following the Association for Computing Machinery (ACM) as their reference to incorporate cybersecurity content into CS curricula (note that they are not referencing The Joint Task Force on Cybersecurity Education). However, reluctance to completely adopt ACM curriculum has been reported in the past even in US universities because it lacked cybersecurity views from industry and government [35]. A comprehensive approach requires incorporating expertise from several sectors of society [36]. In Ecuador, this is an essential initiative towards identifying cybersecurity skills and areas of knowledge that could feed suitable curricula, so this initiative needs to be started because current local approaches lack such feedback.

Clearly, not only what content is taught, but also how it is delivered, is important [35]. The implementation of cybersecurity curricula needs to identify and incorporate effective approaches for learning. For instance, academic instruction should consider real-world case studies and hands-on simulations [26]. In addition, the core principles that allow comprehension of systems vulnerabilities [37] could be supplemented with adversarial thinking to bolster preparation to deal with emergent threats, as opposed to only known types of attacks [35]. Overall, while developing capabilities can take time, it is crucial that feasible steps be taken now, and more complex initiatives started or at least analyzed.

Cybersecurity training

Specialty training for faculty members who do not have a background in specific areas of cybersecurity will be a key part of developing stronger academic curricula. A CERT's support for training educators can play an essential role here. Likewise, appropriate training for students in practical areas of cybersecurity needs to be strengthened with implementation of labs and experiences acquired outside the university. Additional courses of action that should be considered are:

- Providing incentives to local industry to support educational initiatives, such as paid internships and trainers provision
- Promoting temporal professional exchange between academia and government agencies to promote development
- Obtaining support from international partners (organizations or private business), such as OAS (in Uruguay), IBM (in Costa Rica), and Microsoft (in India)
- Sharing the training, an approach already followed by at least one Ecuadorian university, which trains outside educators who replicate the acquired knowledge in house when returning [R51]
- Establishing training programs and training facilities such as forensic centers
- Implementing virtual training environments [R34]
- Extending security workshops [R41, R42]
- Expanding security competitions
- Envisioning and supporting apprenticeship programs to provide cybersecurity work experience to students
- Emphasizing into practical and intense hands-on security training.

Several countries have identified the value of apprenticeship programs in improving practical–technical training around cybersecurity. In the UK, cybersecurity apprenticeship programs support national critical sectors and receive funding from the government [38]. In the USA, cyber apprenticeships programs have started to emerge in community colleges [39] and other similar programs are supported by industrial partnerships [40].

Lastly, training is also needed to advance the state of the practice in industry, and law enforcement. Because of concerns about the

22 "Students, educators, programs, and academic materials cross national boundaries," OECD and World Bank, 2006.

quality of commercial training [R39], controls that guarantee appropriate levels of excellence should be considered.

Cybersecurity certifications

Although promoting professional certifications may not be the main function of universities [R39], some believe students should be encouraged by educators to pursue security certifications [26] as a means to improve knowledge. Some developing nations improving cybersecurity performance consider international accreditation support (e.g., Oman) and certification programs (e.g., Rwanda) with CERT and government support. In order to increase accessibility, pursuing professional security associations with affiliation for students at low cost should be promoted [26].

Research and development

Developing serious research on cybersecurity in Ecuadorian universities presents a great challenge because quality research must build upon existing capabilities and structure, including experienced investigators, funding, research centers, and feasible projects. Efforts need to be devoted for building the foundation that a national program of cybersecurity R&D requires. Nevertheless, current initiatives of universities exploring information security research could be supported and expanded, and if they were, this might further encourage faculty interest in the development of education. An integrated national effort should identify potential areas of research in the public and private sectors to foster critical cybersecurity for infrastructure protection.

Cybersecurity awareness and public education

The need to addressing social awareness at the national level was raised by interviewees and has certainly been highlighted by OAS *et al*. [18]. In the academic context, at least one university is already engaged in initiatives (online education) to educate its internal audience [R50], which would be worth imitating in other institutions.

Worldwide, strategic initiatives include national awareness programs (Rwanda), cyber hygiene campaigns, and national cybersecurity awareness week (South Africa). To be effective, such initiatives need to identify the audience, topics, and means to deliver awareness and education. Some suggest that audience must include children, adults, and the elderly [41]; and also consider several areas of society: business, decision makers, and justice. Topics should address current cyber threats facing the domestic environment but should not ignore global trends. They should include basic information about the methods or techniques of attack (e.g., malware infection, social engineering), consequences (e.g., fraud and personal privacy invasion), and strategies for protection (e.g., patches & passwords good practices). Depending on the audience, strategies to deliver education already being used in developing countries include school curricula, radio (in Cameroon), TV, and web resources. As with formal education, the methods used to deliver awareness material are important to achieve the goals. Some candidate vehicles include: videos, cartoons (in Brazil), and analogies taking advantage of existing mental models on the physical world to improve understanding of cybersecurity [42].

Kortjan and Von Solms present a framework that provides strategic insights to address cybersecurity awareness and education for South Africa [43]. While such insights are very valuable and many may be applicable to a developing context, applying them in a developing country must take into account the availability of national capabilities.

Of course, awareness alone will not solve the problem of insecurity because: (i) ICT users will fail to accomplish what is expected from them in their roles anyway [44]; and (ii) attackers can adapt to defenses, especially if a victim is specifically targeted by an advanced adversary. Nevertheless, effective awareness and education can be essential against a subset of attacks (e.g., malware infection, social engineering) and also informative to improve personal information protection.

Finally, improving formal and informal cybersecurity education requires planning for both the short and long term, so to supplement what has been discussed above, in Appendix 1 we summarize relevant practices of other countries highlighted by the literature.

Conclusion

The Ecuadorian educational system has struggled to respond to the cybersecurity challenge. Publicity about cybersecurity attacks to domestic critical infrastructure (e.g., the financial services) has not been enough to foster a comprehensive national academic approach to cybersecurity education, but isolated efforts have begun at a few universities. The novelty of cybersecurity as an emerging issue imposes a challenge on the educational system because it requires new abilities from educators and traditional capabilities from society. Advancing cybersecurity education, in fact, builds on standard capabilities that are expected to already be in place, including academic programs with strong links with societal needs, academic infrastructure, and a solid research structure. Because Ecuador is still in the early stages of developing such structures, addressing cybersecurity is especially challenging. Universities are constrained in their ability to establish academic instruction (i.e., courses, training) because the lack of faculty formally educated in cybersecurity as well as technical resources. Integration between academia and the business sector is a serious issue, especially in major cities, that prevents taking steps (e.g., understanding demand) to promote development.

Although developing cybersecurity workforce is a challenge for many nations, there are remarkable differences when comparing Ecuador to developed countries, where advanced academic systems had been established. Those countries also have actors that support local cybersecurity initiatives, such as security firms, technology makers, and military agencies that are actively involved in cyber operations. Despite limitations, however, good performance in cybersecurity can also be achieved by less equipped nations. Oman and Malaysia are good examples from which developing nations can learn relevant lessons.

While a substantial amount of literature provides strategic guidelines to address cybersecurity education, there has been little research on identifying the actual factors that impede cybersecurity education, especially in the context of a developing economy. This article begins to fill this gap by collecting the views of educators in several geographic areas across a developing country—Ecuador. The article provides answers for: what are the challenges that universities face in order to provide cybersecurity education in a developing country? How can this country enhance cybersecurity education to support national cybersecurity capabilities? In answering these questions, this study explains why the lack of cybersecurity professionals has been observed in the local labor market as cited by stakeholders in the financial industry [21], and identifies where opportunities for improvement appear to be. In that regard, this study presents evidence about factors driving cybersecurity education in a developing nation.

Our objective in this study has been to inform public policy so as to improve critical infrastructure protection in the nation. All countries, but especially developing countries, face many demands and serious resources constraints. While the risks posed by accidental and pernicious cyber events can never be fully quantified, developments around the world make it clear that they are growing. In order to make informed decisions about how much of their scarce public and private resources to devote to cyber protection and security, countries need experts who both understand potential vulnerabilities and can develop cost-effective strategies for risk mitigation. Understanding such issues in detail is a first step to developing beneficial courses of action. In support of this endeavor, we have presented a range of policy options framed into six domains that the country should consider as part of an improvement plan. High priority should be given to: defining and communicating a national cybersecurity strategy that establishes pragmatic objectives and provide directions; developing means of collaboration that integrate industry and academia; and designing suitable curricula while preparing cybersecurity educators.

Beyond the Ecuadorian environment, research is needed to assess which strategies are most suitable for developing nations, and to find mechanisms that align universities' economic incentives with the public good. Developing cyber competencies is a challenge that will take time to address. Fortunately, Ecuador has been experiencing major changes in its higher education system that can offer a timely opportunity to start advancing cybersecurity education.

Funding

This work was supported by the Department of Engineering and Public Policy at Carnegie Mellon University, as well as from faculty-discretionary funds of M.G.M. and D.C.S. F.E.C. also received support from the Fulbright-Senescyt Program.

Acknowledgments

We thank the anonymous respondents from Ecuadorian universities for their participation in this study. We also thank Gabriel Valenzuela for his contribution as a second coder during the inter-coding agreement analysis, consensual coding.

References

1. Paulsen C, McDuffie E, Newhouse W, *et al*. NICE: creating a cybersecurity workforce and aware public. *IEEE Secur Priv* 2012;**10**:76–79.
2. CEAACES. *Ecuador: The Assessment Model of the Mandate 14*. (Spanish). Quito, Ecuador, *Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior*, 2013.
3. CEAACES. 'Suspended due to lack of quality.' *The Closure of Forteen Universities in Ecuador*. (Spanish). Quito, Ecuador, *Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior*, 2013.
4. NICE. *National initiative for cybersecurity education (NICE). Relationship to President's Education Agenda*, 2010.
5. National Institute of Science and Technology. The National Cybersecurity Workforce Framework, 2013. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework (4 February 2019, date last accessed).
6. Libicki MC, Senty D, Pollak J. *Hackers Wanted: An Examination of the Cybersecurity Labor Market, Rand Corporation*, 2014. http://www.rand.org/pubs/research_reports/RR430.html (4 February 2019, date last accessed).
7. Baker M. *Striving for Effective Cyber Workforce Development*. Carnegie Mellon University, Pittsburgh, PA, USA: Software Engineering Institute, 2016.
8. UK Cabinet Office. *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World*, 2011. https://www.gov.uk/government/publications/cyber-security-strategy (4 February 2019, date last accessed).
9. General Auditor. The UK Cyber Security Strategy: Landscape Review, 2013. https://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/ (4 February 2019, date last accessed).
10. European Commission Tempus Project. *Report on EU Practice for Cyber Security Education*, TEMPUS (Trans-European Mobility Programme for University Studies) program, European Union, 2013.
11. Harašta J. Cyber security in young democracies. *Jurisprudencija* 2013;**20**: 1457–1472.
12. Lehto M. Cyber Security Competencies: Cyber Security Education and Research in Finnish Universities. In: *ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare & Security: ECCWS 2015*, pp. 179–88. Hatfield, UK: University of Hertfordshire, Academic Conferences and Publishing International Limited, 2015.
13. Newmeyer K. Elements of national cybersecurity strategy for developing nations. *Natl Cybersecurity Inst J* 2015;**1**:9–19.
14. Muller L. Cyber security capacity building in developing countries: challenges and opportunities. *Nor Inst Int Aff* 2015;**21**:1–4.
15. Kortjan N, Solms RV. Cyber security education in developing countries: a South African perspective. *South Afr Comput J* 2012;**52**:29–41.
16. Von Solms R, Von Solms S. Cyber safety education in developing countries. *Syst. Cybern. Informatics* 2015;**13**:14–19.
17. Curbelo A, Cruz A. Faculty attitudes toward teaching ethical hacking to computer and information systems undergraduates students. In: Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technolgy, Cancun, Mexico, August 2013, p. 1–8. http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP086.pdf (4 February 2019, date last accessed).
18. Organization of American States, Inter-American Development Bank. Cybersecurity. Are we Ready in Latin America and the Caribbean?, 2016.
19. Kuckartz U. *Qualitative Text Analysis. A Guide to Methods, Practice and Using Software*. London: Sage, 2014.
20. Parekh A, Pawar A, Munot P, *et al*. Secure authentication using anti-screenshot virtual keyboard. *Int J Comp Sci Issues* 2011;**8**:534–37.
21. Catota FE. Cybersecurity Capabilities in a Critical Infrastructure Sector of a Developing Nation. PhD Thesis. Carnegie Mellon University Department of Engineering and Public Policy, 2016.
22. Target AC. Cybersecurity Challenges in Developing Nations. PhD Thesis. Carnegie Mellon University Department of Engineering and Public Policy 2010.
23. Hathaway M, Demchak C, Kerben J, *et al*. Cyber Readiness Index 2.0, Potomac Institute for Policy Studies, 2015.
24. Creswell J. *Research Design: Qualitative, quantitative and Mixed Methods Approaches*. Los Angeles: Sage, 2014.
25. Schweitzer D, Humphries J, Baird L. Meeting the criteria for a Center of Academic Excellence (CAE) in information assurance education. *J Comput Small Coll* 2006;**22**:151–160.
26. Wright MA. Improving cybersecurity workforce capacity and capability. *Inf. Sys. Sec. Assoc. J* 2015; **13**:14–20.
27. Pollack M. Chile Transition to a Knowledge Based Economy Role of Chilean Professionals Abroad. 2004.
28. Sledge C. Building Information Assurance Educational Capacity: Pilot Efforts to Date. Carnegie Mellon University, Software Engineering Institute, 2005.
29. International Telecommunication Union. ITU Cybersecurity Work Programme to Assist Developing Countries, 2007. Geneva, Switzerland: International Telecommunication Union.
30. International Telecommunication Union, ABI Research. Global Cybersecurity Index, 2014. New York, USA: ABI Research.
31. Montgomery S. English and science: realities and issues for translation in the age of an expanding lingua franca. *J Spec Transl* 2009; **11**:6–16.

32. Kuhn M, Weidemann D, (eds). *Internationalization of the Social Sciences Asia—Latin America—Middle East – Africa – Eurasia*. New Brunswick, NJ, USA: Transaction Publishers, 2015.
33. Raytheon, National Cyber Security Alliance. Securing Our Future: Closing the Cybersecurity Talent Gap, 2015. Sterling, VA, USA: Raytheon Company.
34. Vincent-Lancrin S, Hopper R, Geloso M. Cross Border Higher Education for Development. OECD and World Bank, 2006. http://www.oecd.org/dataoecd/51/42/37477437.pdf (4 February 2019, date last accessed).
35. Schneider FB. Cybersecurity education in universities. *IEEE Secur Priv* 2013;**11**:3–4.
36. Dark M. Advancing cybersecurity education. *IEEE Secur Priv* 2014;**12**: 79–83.
37. Klimburg A (ed.). National cyber security framework manual. (2012). NATO Cooperative Cyber Defense Center of Excellence, 2012. Tallinn, Estonia: NATO CCD COE Publications
38. Department for Digital Culture, Media & Sport. Cyber security CNI apprenticeships, 2017; https://www.gov.uk/guidance/cyber-security-cni-apprenticeships (4 February 2019, date last accessed).
39. Tidewater Community College. TCC to offer first cybersecurity apprentice education in Virginia, 2016. https://www.tcc.edu/tcc-news/cybersecurity-apprenticeship (4 February 2019, date last accessed).
40. The Techpartnership. Who we are, 2017. https://www.thetechpartnership.com/about/the-partnership (4 February 2019, date last accessed).
41. Bishop M, Taylor C. A critical analysis of the centers of academic excellence program. In: *13th Colloquium for Information Systems Security Education,* Fairbanks, AK, USA: University of Alaska, June 2009.
42. Furman S, Theofanos M, Choong Y, *et al*. Basing cybersecurity training on user perceptions. *IEEE Secur Priv* 2012;**10**:40–49.
43. Kortjan N, Von Solms R. A conceptual framework for cyber-security awareness and education in SA. *South Afr Comput J* 2014;**54**:29–41.
44. Cranor LF. A Framework for Reasoning about the Human in the Loop. In: *Proceedings of the 1st Conference on Usability, Psychology, and Security, (UPSEC '08)*, pp. 1–15. Berkeley, CA, USA: USENIX Association, 2008.
45. International Telecommunication Union, ABI Research. *Global Cybersecurity Index & Cyberwellness Profiles*, Geneva, Switzerland: ABI Research, 2015.
46. Business Software Alliance. EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace, Washington, DC, USA: BSA Business Software Alliance, 2015.
47. Feakin T, Woodall J, Nevill L. Cyber Maturity in the Asia-Pacific Region, Canberra, Australia: Australian Strategic Policy Institute, 2015.

Appendix 1: Strategies for Capacity Building.

This appendix summarizes strategies for capacity building highlighted by the literature from 12 countries, 8 of which are developing (Oman, Rwanda, Cameron, Colombia, Uruguay, Chile, Malaysia, India), and 4 developed (USA, UK, South Korea, Finland). They meet at least one of these criteria: (1) relative high ranking in cybersecurity preparation according to ITU [30, 45] and others indices/models [18, 23, 46, 47]; (2) good general education; and (3) geographic similarities with Ecuador.

Dimension	Planning	Promoting	Implementing	Evaluating
Governance	• Plan capacity building • Educational strategy for cybersecurity • Plans for cybersecurity education • Nationwide information security education • Accreditation programs • National accreditation body (standardization) • National cybersecurity workforce framework	• Government bolsters cybersecurity educational initiatives • Promoting cybersecurity courses in higher education • Non-government entities and public-private partnerships • Promoting development of security professionals • Agreements between academia and the military	• Funding • Establishing a network for security education	• National cyber security measures • National information security index • Maturity models
Academic	• Academic programs • Introducing security curriculum in schools and universities	• Promoting cybersecurity graduate programs	• Master's degree and doctoral theses • Online courses • R&D programs for cybersecurity • Academic centers of excellence in cybersecurity research	
Research	• CERT • Research councils	• Agreements between academia and industry	• CERT • R&D programs for cybersecurity	
Training	• Professional programs	• Promoting specialized training in cybersecurity	• Training specialists with international support • Training law enforcement agencies • Training centers on specialized security topics • Computer forensic labs and training facilities • Training in cybercrime investigation • Virtual training environment • Private companies providing security courses • Federal cybersecurity training events • Training provided by defense agencies • Private sector offers training • CERT trains trainers • Cybersecurity education supported by laboratories • Conferences on security topics • Industry talks, workshops or seminars	
Awareness	• Educational programs • National cybersecurity awareness program/ campaigns	• Promoting public education in cybersecurity	• Awareness through radio program • International collaboration (e.g., Microsoft) to design awareness initiatives • Awareness portals • CERT supports awareness and security culture	
Certification	• Government-run IA certification scheme • Certification program	• Promoting certification	• Government supports certification • Certification through internationally recognized government agency • International accreditation support	