Cybersecurity Capabilities in a Critical Infrastructure Sector of a Developing Nation

Submitted in partial fulfillment of the requirements for

the degree of

Doctor of Philosophy

in

Engineering and Public Policy

Frankie Catota Quintana

B.S., Informatics Engineering, Escuela Politécnica Nacional (EPN)
Specialist, ICT Management, EPN and Escuela de Organización Industrial (EOI)
M.S., Information and Communications Technology Management, EPN

Carnegie Mellon University
Pittsburgh, PA

December, 2016

Abstract

When information technology is incorporated into the operations of financial critical infrastructure, it brings with it a range of cyber risks, and mitigating them requires that firms and regulators develop capabilities to foster protection. The sophistication of cyber threats to the financial sector has been growing rapidly. Developed nations have worked hard to improve their knowledge of these threats and establish strategies to respond accordingly. However, in developing nations, both the understanding of the risks posed by cyber threats and the ability to address those risks have been slower to evolve. Developing the needed cybersecurity capabilities in developing countries encounter challenges that need to be identified and addressed.

In order to begin to do that, this thesis reports on three studies conducted in the context of Ecuador. The first study identifies and assesses incident experiences, challenges, barriers, and desired actions reported by financial security managers with the objective of identifying strategies to enhance incident response capabilities. The second study begins with the security incidents reported by the Ecuadorian financial stakeholders during the first study and assesses the potential effectiveness of the government policy that is intended to address IT risk in the financial sector. The third study explores the challenges that universities face in order to provide cybersecurity instruction to protect critical infrastructure and explores potential strategies to advance cybersecurity education at the university level.

In support of this work we collected data from national practitioners involved in responding to security incidents and in developing cybersecurity skills. Sixty-one in-depth, semi-structured interviews across five cities were conducted (95% in person, the rest by telephone) with respondents who had good knowledge in the subjects. Respondents come mainly from: the financial sector (CISOs, risk and IT managers, security chiefs, security officers, authorities); telecommunications sector, especially ISPs (managers, directors, engineers, authorities); and academia (deans, directors, professors). We transcribed all the interviews, coded them and conducted qualitative text analysis.

This research finds that (1) the financial sector is already facing risks driven by outsiders and insiders that lead to fraud and operational errors and failures. The main barriers to improving protection are small team size, network visibility, inadequate internal coordination, technology updating, lack of training, and lack of awareness. The sector has little community support to respond to incidents, and the national legal framework has not supported appropriate prosecution of cyber criminals; (2) the national IT risk management policy has reasonably covered most countermeasures related to reported security incidents. There are however, several areas of gap, one of the most important is network security, which can enable sophisticated malware attacks; (3) today the level of cybersecurity education is mostly elementary in Ecuador. Academic interviewees at only four of the thirteen universities studied expressed confidence that they can provide students with reasonable preparation. Ecuador needs to design a national cybersecurity plan that prioritizes protection for critical infrastructure and should support strategies that allow the country to enhance cybersecurity capabilities. Properly designed these initiatives should allow the nation to develop a core structure to confront current and emergent cyber challenges in the financial sector and other critical national operations, and build the human resources necessary to continue that effort.

To my Mother

Elsa María Quintana

Acknowledgments

I consider myself fortunate for having had the opportunity to work with M. Granger Morgan, and Douglas Sicker. I am deeply thankful for the support, guidance, and advice I received from Granger since I started my journey at EPP. I also express my gratitude to Doug for his support, advice, and encouragement.

I am grateful to Howard Lipson (now deceased) for his efforts to support my work in chapter two and part of chapter three, even as his health continued to deteriorate. I am also thankful to Howard for sharing his unique professional experiences at the early days of CERT/CC.

I would like to thank the members of my dissertation committee Lorrie Cranor for her support and feedback about conducting interviews for Chapter two. I also thank David Thompson from the Software Engineering Institute for providing feedback of my work. I thank Gabrielle Wong-Parodi for her support regarding qualitative analysis in Chapter two.

I thank Pedro Leon for sharing his experiences as a researcher at EPP. I appreciate the kind support of the EPP staff, especially Vicki, Patti, and Adam. I would like to thank the Global Communication Center for providing feedback about the readability of several sections of the main chapters of this thesis.

For their generous contribution, I would like to express my gratitude to the anonymous interviewees from universities, financial sector, telecommunications sector, and others areas of the Ecuadorian society. Finally, I want to thank my family for their constant support, Elsa María, Cristina, Ivonne, and Alex.

This research received economic support from the Department of Engineering and Public Policy at Carnegie Mellon University, as well as from faculty-discretionary funds of M. Granger Morgan and Douglas Sicker. The author also received support from the Fulbright-Senescyt Program.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

While there are obvious benefits from using ICT to support critical infrastructure, most applications also bring inherent risk that cybersecurity threats impose on essential operations of modern societies. ICT implementations can open cyber-doors of these critical operations to knowledgeable adversaries. The financial services, particularly, have recently been undergoing cyber (and cyber-physical) attacks that have grown in sophistication and persistence. The financial services have consistently been one of the most targeted industries globally [1, 2]. It is widely known that (advanced) adversaries have managed to intrude into internal financial networks and subsequently cause massive financial-data breaches and important economic losses.

Addressing the cybersecurity risks posed to infrastructure sector requires (1) understanding the multiple manifestations of the threat (in the form of security incidents) and (2) developing cybersecurity capabilities in order to implement measures to protect and respond to the threat. Worldwide, several well-developed nations have taken advantage of their societal capabilities to advance their ability to confront cyber threats. Although a few developing nations, such as Malaysia, have made an exceptional work [3], many developing countries struggle to prepare to the challenge of cyber threat [4].

Past research regarding security incidents and cybersecurity capabilities have an important concentration in the context of developed economies. Studies on security incidents have typically been reported by Verizon, IBM, Symantec, FBI, CERT/CC, US-CERT, and more. In the realm of cybersecurity capabilities at the national level, they have been addressed by DHS, NIST, NSA, GCHQ, RAND, BAH,[1] SANS, UN, EU, among others.[2] However, there is little related literature that allows us to understand specific issues arising during both the occurrence of cybersecurity incidents and the enhancement of cybersecurity capabilities in developing nations. Most studies in *developing countries* have only started to arise recently [5–9] and to our knowledge no study has been conducted in depth in a particular infrastructure sector of these countries.

Developing nations may present to an adversary with an environment that is different from that existing at developed economies, and this difference may enable successful attacks. Many developing nations have modest economic, technologic, and academic resources, which can limit their ability to protect against and respond to cyber-attacks and develop cybersecurity capabilities. A poor security posture of financial

[1] Booz-Allen Hamilton

[2] A literature review section is provided in each major chapter

institutions and governments can in turn provide incentives to attackers and therefore influence a nation's cybersecurity environment.

Establishing effective cybersecurity capabilities in a critical financial infrastructure cannot take place solely within that sector because the financial sector cannot confront cyber, national and transnational threats on its own. Indeed, many cybersecurity threats transcend physical and cyber boundaries. Thus, at a minimum, informed public policy that fosters affordable, cost effective initiatives at the national level is needed. To complete the cycle of risk management, such policy interventions should also be analyzed under the lens of the manifestations of the risk they are intended to mitigate.

This thesis presents a three-fold approach to address cybersecurity issues arising in the financial critical infrastructure in context of a developing nation, Ecuador. The main objectives of this investigation are to: (1) explore the experiences with cybersecurity incidents in the Ecuadorian financial sector and investigate its ability to deal with those incidents; (2) assess the effectiveness of the cyber policy governing the risks that are being imposed by those cybersecurity incidents, and (3) explore the challenges that higher education face to develop the human resources with cybersecurity skills needed to support the critical infrastructure protection.

1.1 Research Questions

This research is focused on exploring the challenges the financial sector faces in order to effectively respond to cybersecurity incidents and examine strategies for improvement. In support of this, the academic environment is also considered. More specifically, we ask:

- What types of security incidents has the financial sector been experiencing? What are the barriers that financial institutions face when handling security incidents? How might potential strategies to raise response capabilities in the sector work?
- What is the potential effectiveness of a national financial regulation designed to mitigate risk imposed by security incidents? Where are the opportunities for improvement that could be undertaken?
- What are the challenges that higher educational institutions confront in order to supply workforce trained in cybersecurity? How might these educational institutions enhance national performance?

1.2 Research Framework

As a basic method for our research, we used a case study design, which focuses on the analysis of a particular group [10]. This research allows us to hear from a segment of the world population that has not been studied with the goals, scope, and methods we have used. **Figure 1** depicts the general conceptual framework that this dissertation follows. On top, our first study not only investigates issues related to cybersecurity incidents in financial services but also provides inputs for the second and third studies. In fact, the second study (on the left) examines the regulatory treatment of reported incidents, while the third study (on the right) addresses one of the barriers cited by participants, which is lack of trained/specialized workforce.

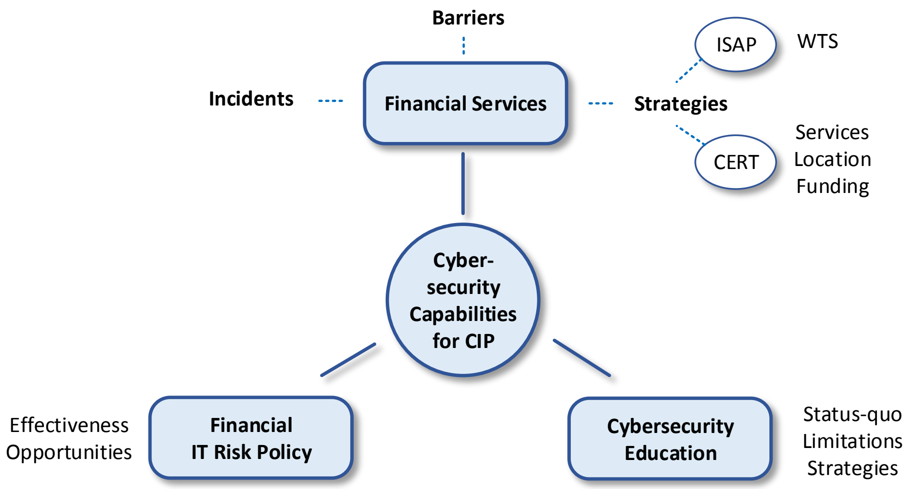


Figure 1: Framework used in this thesis for analyzing cybersecurity capabilities CIP,[3] ISAP,[4] CERT,[5] WTS[6]

The integration of the three studies emphasizes the fact that cybersecurity response capabilities not only depend on the ability of a particular sector to prepare to cyber challenges but also on the ecosystem [11] that may provide the means and incentives to strengthen those capabilities.

1.3 Methods

This research is based on a *qualitative text analysis* of interviews for the first and third studies, whereas the second study uses threat modeling based on attack trees. We conducted detailed semi-structured interviews across five cities in Ecuador with sixty-one respondents who had privileged knowledge of the issues under analysis. Respondents come from: the financial sector (CISOs, risk and IT managers, security chiefs, security officers, authorities); telecommunications sector, especially ISPs (managers, directors, engineers, authorities); academia (deans, directors, professors); and CSIRTs. This analysis focused on a thematic analysis as described by Kuckartz [12]. In addition, the analysis of the third study conducts an attack-tree analysis of security incidents initiated by smart adversaries, as well as a mapping procedure of security controls with regulatory requirements.

1.4 Thesis Contribution

This thesis contributes to existing literature addressing cybersecurity capabilities in developing nations and informs public policy to improve the practice of cybersecurity in Ecuador. The results provide details on security incidents that have been occurring in several financial institutions of different sizes and types in the Ecuadorian financial

[3] CIP: Critical Infrastructure Protection

[4] ISAP: Information Sharing and Analysis Program

[z] CERT: Computer Emergency Response Team

[6] WTS: Willingness to Share

sector. In addition, we report barriers to improve incident response in the financial sector and barriers to developing cybersecurity education at national level in academic institutions. We identify and discuss strategies for improving performance in the financial sector and academic arena. Furthermore, we develop and apply a method to analyze effectiveness of a financial cybersecurity policy, and presents a summary of gaps in the Ecuadorian cyber-policy addressing risk in financial infrastructure. Overall, it is our hope that this work contributes to improving cybersecurity practice in Ecuador's financial sector and enhancing cybersecurity education at national level. Beyond the financial sector, results from this thesis can also inform broader national cybersecurity policy for Ecuador.

1.5 Conceptual Definitions

Throughout the thesis, the terms *security incidents* and *cybersecurity incidents* are used as synonyms; the definition of security incident has been taken from NIST. These two terms are different from *event* in the sense that an event is an occurrence that does not necessarily cause a negative outcome. Similarly, the terms CERT and CISRT, which refer to a computer incident response team, are used as synonyms. Although critical infrastructure is often defined depending on the nations' posture, these definitions often have a common goal. In this thesis, we adopt the US DHS definition: critical infrastructure is a "nation's infrastructure [that] provides the essential services that underpin [a] society and serve as a backbone of [a] nation's economy, security and health."[7] Regarding incidents, we define a three-level terminology to analyze incidents and present results in Chapter three.

1.6 Thesis Organization

The entire structure of the thesis is organized in five chapters, three of which report research conducted in three interrelated papers. The next chapters report the research as follows:

Chapter 2 addresses the three main elements of the first study. The chapter reports security incidents occurring in the Ecuadorian financial sector and the associated concerns that arise among stakeholders. Next, the study uncovers internal and external barriers that financial stakeholders confront in preparing for and responding to security incidents. Then, we present a brief assessment of two potential strategies to develop cybersecurity capabilities widely used in developed countries and beyond, a computer emergency response team (CERT or CSIRT) and an information sharing and analysis program (ISAP). We report on financial practitioners' preferences regarding type of CSIRT-services required and CISRT organization, as well as willingness to share information.

Chapter 3 reports the second study, which collects, categorizes, and analyzes the security incidents narrated in Chapter 2, and conducts a gap analysis on the Ecuadorian national policy addressing IT risks in the financial sector. The categorization and analysis

[7] https://www.dhs.gov/what-critical-infrastructure

uses attack-trees, especially regarding security incidents initiated by smart adversaries. Here, we define the term *incident profile* to characterize types of incidents. Then, the study identifies countermeasures from security standards and best practices—from ISO, PCI, and CSI—to mitigate the risk. Lastly, the chapter presents a gap analysis for every incident profile and subsequently provides a summary of results.

Chapter 4 expands the research to the academic arena, which should be directly involved in building cybersecurity capabilities to support the financial sector (and more). This chapter reports on the perceptions of senior academics regarding the cybersecurity practice of the local financial industry. Then, the focus is on the current practices on cybersecurity education and the factors driving this education in Ecuador. Lastly, based on both the previous analysis and literature review, we present policy options to improve cybersecurity education that we believe are more suitable for Ecuador. These policy options are organized in six dimensions: capacity governance, academic programs (instruction), training, certification, research and development (R&D), and awareness.

Chapter 5 concludes the thesis by mainly summarizing findings, indicating contributions, communicating implications for policy and practice, and highlighting policy recommendations to advance cybersecurity capabilities in a developing nation, Ecuador.

Chapter 2

Cybersecurity Incident Response Capabilities in a Developing Nation: the Ecuadorian Financial Sector

Abstract

Cyber-threats have been targeting the financial services worldwide over the last few years, so a diverse level of actions to respond has arisen across nations. In developed countries, both the ramifications of these cyber-threats and strategies to mitigate the associated risk have been reasonably well documented. However, there is little related literature that allows us to understand specific issues arising in developing nations. Because many of these nations have modest cyber capabilities, their ability to respond to cyber-attacks can be likewise limited, yet the need to respond to these attacks is crucial for protecting the critical financial infrastructure in these countries.

This study explores the posture and the ability of the Ecuadorian financial industry to deal with cybersecurity incidents and examines two potential strategies often applied in the developed world—*CSIRTs* and *information sharing*—to mitigate cyber-risks. Thirty-three semi-structured interviews with multiple stakeholders (financial security managers & security officers, authorities, and managers at Internet service providers) were conducted using both structured and open-ended questions, and two cyber-attacks scenarios. Based upon a qualitative text analysis, this work uncovers experiences with security incidents, barriers to responding to threats, and stakeholders' desired responses.

Findings indicate that the financial sector already confronts: (1) cybersecurity risks, driven by both outsiders and insiders, that eventually lead to fraud and operational failures; and (2) constraints imposed by a lack of awareness by computer systems' users, scarcity of financial and technical resources, and challenges imposed by the ecosystem, such as little community support and weaknesses in the legal framework. In the pursuing of improvement, stakeholders' postures suggest that there is an opportunity to establish better incident response strategies for the Ecuadorian financial services but with some limitations. To decrease uncertainty about threats, stakeholders are likely to share technical information as opposed to quantitative information about security incidents.

2.1 Introduction

Several nations recognize the financial sector as an essential component of their critical infrastructures and economies [13]. Nevertheless, the sector has been repeatedly targeted by cyber attacks. In the USA, well-known reports financial or payment services about data breaches include firms like JP Morgan, Card Services, Target, TJX, and more. A report by Verizon [1] shows that relevant threats on the financial sector include web attacks, cyber espionage, card skimming, and attacks on point of sale (POS) terminals. The persistence and sophistication of cyber-attacks has given raise to multiple strategic initiatives for cybersecurity critical infrastructure protection (CCIP), such as the NIST cybersecurity framework, information sharing programs, and others. Worldwide, most advanced nations have adopted similar approaches. However, ability to understand cyber-threats and most strategies to advance cybersecurity capabilities make an assumption of societal development in several dimensions, including legal, technological, economic, and skilled workforce. Unfortunately, developing nations often lack some of these competencies that restrain their range of actions to detect cyber threats and respond accordingly.

Understanding the type of incidents a critical sector faces and the barriers that prevent stakeholders from appropriately responding is essential to improve incident response capabilities. This paper explores the challenges that practitioners in the Ecuadorian financial services experience when dealing with cybersecurity incidents and examines two potential strategies frequently applied in the developed world and other countries—a CSIRT and an information sharing program. We expect that the results of this study inform courses of action to enhance cybersecurity in this critical infrastructure sector. This paper is organized as follows: *section 2* addresses related work; *section 3* explains the research method; *section 4* describes stakeholders' experiences with security incidents; *section 5* identifies the barriers that stakeholders face; *section 6* examines two strategies; and *section 7* concludes.

2.2 Literature Review

By considering the field of research and the context, relevant literature can be classified into two major dimensions: (1) cybersecurity incidents in the financial sector, and (2) cybersecurity research in the critical infrastructure of developing nations.

First, surveys have traditionally been conducted as a means to learn about security incidents affecting several industries. Organizations, such as AT&T, CSI, FBI, IBM, SANS, Verizon, and security firms typically publish reports informing about trends on cyber-crime incidents, threats, practitioner response strategies, and security investment decisions. These studies provide a global perspective that allows us to position risks by industry. The financial services often ranks as one of the most targeted sectors. There are several recent research initiatives in the financial domain. The New York State Department of Financial Services (2014) reported results from a cybersecurity survey data [14]. Here, 154 institutions report on their approaches to cybersecurity (compliance, information sharing, and preparedness to breaches), criteria for investments (economic condition, business directives, compliance, and reputation), governance, and plans. This report provides statistics on incidents, including malware (22%), phishing (21%), and pharming (7%), but it does not provide details on how they occurred. At CERT/CC Randazzo et al. (2004, 2005) [15, 16] and Cummins et al. (2012) [17] focus on assessing one type of risk, insider threat, in financial services. CERT/CC analyzed 67 malicious insider cases and 17 non-malicious to identify patterns in people's behavior and techniques. Findings include insiders' approaches (not sophisticated, slow tactics), insiders' targets (e.g., PII), and detection methods (audits, co-workers report) [17]. Lastly, several publications such as the CFA[8] Institute's in the UK provide recommendations to protect financial transactions.

Second, in the context of cybersecurity in developing countries, prior literature addresses cybersecurity issues in a number of African nations, but in the Americas literature is modest. In the global sphere, an ITU report (2007) provides an explanatory guide for cybersecurity geared toward developing countries [5]. The report includes forms of cybercrime, cyber-attacks, standard security technologies (e.g. PKI, IPSec), and legal elements (e.g., intellectual property). Incident response is not addressed but mentioned in the appendix.

In Africa, a study by Cole et al. (2008) addresses national cybersecurity practices from a continent perspective [18]. Cybersecurity posture in African nations (grouped in regions) was assessed based on a number of criteria, including cyber-crime legislation, CSIRTs, higher education programs, end user education, national PKI, law enforcement, and policies for security measures. Very few African nations were addressing cybersecurity and, among them, the main focus was mostly legislation of cybercrime. In addition, most investments were done in the private business. The report emphasizes the need for improving cybersecurity in Africa. In his CMU PhD thesis, Target (2010) conducts a comparative analysis between two African nations (Rwanda and Tunisia) to investigate the posture of governments regarding cybersecurity threats from a general perspective [6]. The author calls for customized strategies because strategies and policies designed for cyber-defense of developed countries can be irrelevant for developing nations. Another finding is that governments in those developing nations have higher risk tolerance to cyber-threats than in developed countries. Additionally, in Nigeria, Osho and Onoja (2015) conduct a comparative analysis between the Nigerian National Cyber Security Policy and strategies of other similar and different nations [19]. They found gaps in addressing cybersecurity elements specific to the county's environment.

In the Americas, Newmeyer (2014) conducts a qualitative study to assess the national cybersecurity readiness of Jamaica [8]. This investigator recommends adoption of international best practices. In terms of incident response, CERT/CC very briefly narrates two case studies. A Colombia case study describes steps taken to create a national CSIRT and summarizes lessons learned. This study highlights the vision of the government to support the creation of the team and coordination with academia [20]. Similarly, Tunisia is presented as an example of a successful national CSIRT that overcomes resources constraints by using open source tools [21]. In the Latin American context, a report from OAS-Symantec (2014) identifies trends, best practice guidelines for firms, and national efforts toward improving cybersecurity in every country [22]. Here, national cybersecurity posture is described in terms of availability of the following initiatives: a national CSIRT, national cybersecurity governance functions, awareness

[8] Chartered Financial Analyst

campaigns, a cybersecurity policy, a program for CIP, and international collaboration capabilities. Because this OAS report was designed to overview several nations, it does not address in deep issues in any particular country.

In summary, cybersecurity research in financial services is concentrated on environments of developed economies. In developing nations, most studies have focused on assessing nations' cybersecurity posture, national strategies, national best practices, and high-level description of incidents. Nevertheless, an effective approach to develop cybersecurity capabilities in a developing nation's critical sector requires a deeper understanding of security challenges the sector faces and elements that prevent enhancing effective response.

2.3 Method

This case study focuses on the analysis of the Ecuadorian financial services. Semi-structured interviews were conducted in order to allow sufficient flexibility to capture meaningful data while having enough structure to facilitate posterior comparative analysis [24, 25]. The goal was to explore the financial stakeholder's experiences with security incidents, to investigate the internal and external limitations they face when handling those incidents, and then to inform strategies for improvement. Based on these objectives, **Figure 2** displays a conceptual framework, which led in turn to our interview guide topics and subsequently to the interview questions.[9] We supplemented semi-structured and open-ended questions with cyber-attack scenarios and printed cross-tabs to elicit responses (e.g., frequency of incidents, level of concern, preferences of security services, and willingness to share information). Interviews were conducted in two stages: (1) spontaneous approach—respondents were asked to express what was already in their minds; and (2) guided approach—respondents were presented a list of choices.

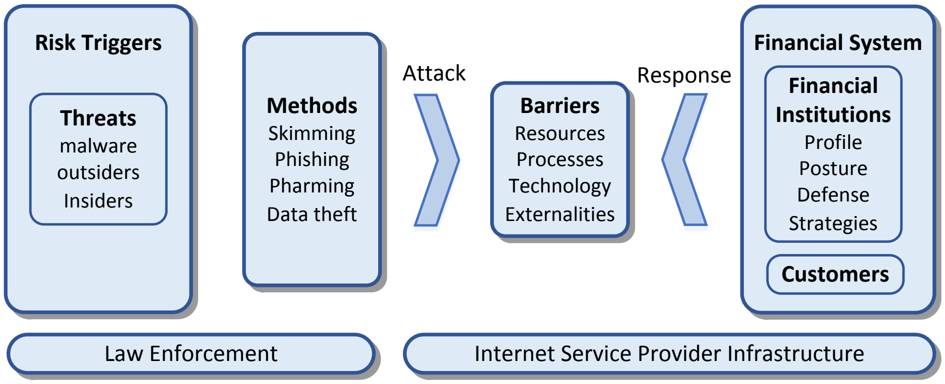


Figure 2: Conceptual framework

2.3.1 Data Collection

Respondents in this study were representatives from financial institutions, Internet service providers (ISPs), CSIRTs, and authorities with responsibilities in cybersecurity.

[9] Details on the interview guide topics are provided in Appendix D and questions in Appendix H.

Thirty-three respondents were recruited by phone, e-mail, and in person. In financial institutions, we visited their offices and asked for functionaries responsible for information security management. Twenty-four financial institutions were contacted, 17 agreed to participate, and 13 actually participated. In these institutions, 18 respondents were CISOs, risk managers, security chiefs, security officers, risk officers, a compliance manager, and an IT manager. In addition, we interviewed authorities who control, regulate, assist, and investigate managerial and technical aspects of security incidents, including managers, supervisors, and a police officer. Finally, executives and technical managers at ISPs and experts from CSIRTs were also interviewed.

Purposeful sampling was used to obtain information-rich cases that allow in depth analysis [25]. In order to collect a diverse range of experiences and verify these experiences across respondents [26], we used person, organization, and site triangulation to avoid effects of issues particular to specific groups or locations [27]. Hence, our criteria include: (1) the size of financial institutions measured by their number of customers, including large (national coverage), medium, and small size institutions; (2) the type of financial institutions, such as bank, mortgage institution, credit card institution, and cooperative; (3) the geographic location of the headquarters of participants' institutions; and (4) the institution's sector of operations—public and private. Regarding ISPs, three are very large with national coverage and one is small with local coverage. While the sample is diverse, we make no claim that it is statistically representative.

Respondents (29 males and 4 females) were told that we, at Carnegie Mellon University, were conducting a study to improve incident response capabilities in the financial sector. Respondents (age range 30-65) offered their time without compensation. Interviews were conducted from 21 July to 12 September 2014, and most of which (31) were conducted in person, one by phone, and one over the Internet. Recordings were allowed for all but two of the interviews. The two exceptions involved authorities. In those cases notes were taken. The average time of all interviews is 87 min (std. dev.: 20.7 min, range: 63–138 min, total: 47.9 hours). When potential participants declined to participate, we pursued replacements in other institutions of similar size. Some explanations given by decliners are presented below.

> *We do not talk about these issues [security incidents] outside of the organization.*
> *Apologies, we do not consider appropriate our participation now.*
> *We have no time.*
> *Thank you, we have already participated in a study.*

Transcriptions of audio recordings were conducted by two native Spanish speakers, one of whom was the main researcher (interviewer), in a secure and private setting.[10] To ensure accuracy of the data we: (1) used specialized software to assist with transcriptions; (2) incorporated rules of transcriptions; and (3) conducted periodic revisions between the two transcribers. Privacy and accuracy considerations increased the cost and time of transcriptions substantially. We also made efforts to keep respondents' participation confidential before, during, and after the recruitment, interview, transcriptions, and analysis.

[10] I acknowledge Graciela Khan for her contribution in transcribing 67% of the interviews.

2.3.2 Data Analysis

Using the country's local language, we conducted a qualitative content analysis (category-based analysis) focusing on a thematic analysis as described by Kuckartz (2014) to identify themes related to our research questions [12]. Interview files were organized into four groups: financial stakeholders, authorities, ISPs, and CSIRTs. The dataset was indexed in two stages. First, five interviews were coded on paper to develop the draft of a codebook, which was refined through discussions with another researcher. Then, the analysis was assisted by qualitative data analysis (QDA) software to annotate the entire dataset. Frequency of incidents, level of concern, and preferences for information sharing and CSIRT services were coded directly in cross-tabs during the interview. The results of the study are presented in the three following sections.

2.4 Experiences, Attitudes, and Approaches

Respondents defined *information security* and *security incident*, and they elaborated the distinction between an *incident* and an *event*. These clarifications were essential to ensure a common language during the elicitation of frequency of incidents and concern of stakeholders. In their definitions, respondents often incorporated C.I.A.[11] and terms they later used to narrate their experiences during the interview (e.g., fraud).

Respondents' conceptualizations of incidents were diverse and driven by corporate policies and security managers' perceptions. The most elaborated definitions considered numerical thresholds set for monetary losses, and a categorical subjective assessment for negative effect on reputation. Differences of conceptualizations were found when drawing the line between an incident and an event. Some stakeholders thought that an incident implies an economic or reputational impact, whereas others believed that the intention of an attack that demands their attention (effort and time) is sufficient to qualify a particular occurrence as an incident. We processed this distinction, and adopted NIST's incident definition[12] when eliciting types of incidents [28].

2.4.1 Incident Experiences

Interviewees narrated security incidents they have been experiencing over the past four years. They also narrated consequences (unavailability and fraud). Hence, the collected data are composed of past and *current* occurrences. In particular cases, such as card skimming, respondents made clear that frequency of occurrence at the time of the interview was changing[13] because the financial sector was implementing EMV.[14] **Figure 3** reveals two key findings: (1) information that respondents spontaneously reported was limited when asked about incidents, but respondents were willing to report additional information when specifically asked about particular types of incidents by using guided elicitation; and (2) there are five major incident types (and the outcome unavailability) that respondents often report, which were confirmed by authorities.

[11] Confidentiality, integrity, and availability

[12] "Security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." [28]

[13] Some institutions experience increase in number of incidents while others experience decrease.

[14] Europa MasterCard and Visa

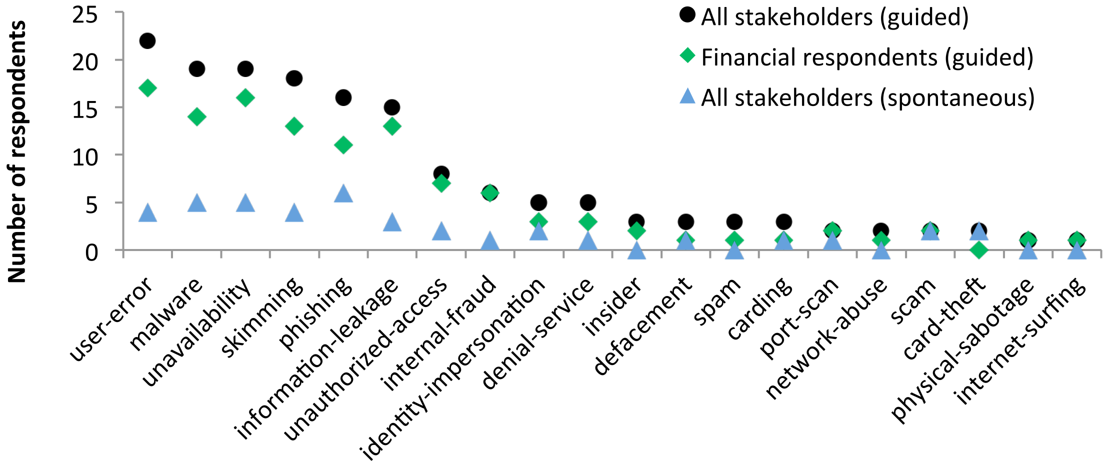


Figure 3: Type of incidents cited by respondents[15]

Frequency of incidents. Given the anticipated wide range of type of incidents, we elicited their frequency on a Likert scale from 1 to 7 according to personal perceptions of financial stakeholders. **Table 1** shows the top ten[16] manifestations of incidents. In the first row, five stakeholders state that they occasionally see incidents related to users' errors[17] (e.g., password sharing).

Table 1: Frequency of incidents reported by financial stakeholders[18]

N	Incident \ Likert Scale	1	2	3	4	5	6	7	Score*
1	User error	0	1	5	7	4	3	1	90
2	Phishing	8	2	3	3	5	3	0	76
3	Skimming	3	5	4	3	3	0	3	73
4	Malware	5	7	4	3	1	2	0	60
5	Unavailability	1	7	8	1	3	0	0	58
6	Information leakage	1	6	0	6	2	0	0	47
7	Unauthorized access	0	4	0	4	0	0	0	24
8	Internal fraud	0	1	4	1	0	0	0	18
9	Carding	0	1	0	1	0	1	0	12
10	Insider	3	1	2	0	0	0	0	11

Scale: (**1**) never, (**2**) rarely, (**3**) occasionally, (**4**) sometimes, (**5**) frequently, (**6**) usually, (**7**) every time
* Weighted sum computed as the of number of respondents by the Likert scale respectively

While some incidents are ubiquitous across institutions (e.g., user error), others are specific to certain kinds of organizations. For example, when targeting their victims, phishing attackers consider: (1) institution's size measured in number of customers and geographical coverage, (2) business model characterized by type of financial business, e-commerce capabilities, and (3) customer market segmentation. **Figure 4** shows that both large and small organizations deal with skimming, whereas phishing appears to be

[15] Types of incidents are not necessarily exclusive
[16] A complete list can be found in Appendix F
[17] Failure to observe corporate internal security policies
[18] This table includes financial institutions and financial authorities reports.

comparatively more serious in large institutions; authorities confirm that the five local major banks often face phishing.

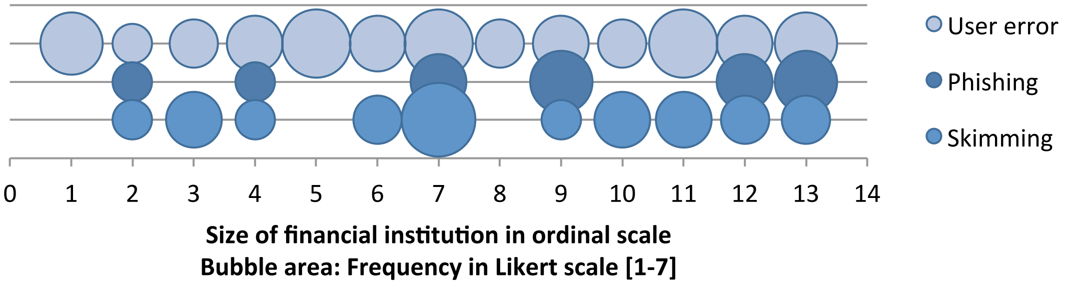


Figure 4: Frequency of incidents by size[19] of institution[20]

Level of concern. Degree of concern about incidents was elicited by using a Likert scale from 1 to 5 to capture financial stakeholders' perception of the associated risk. Concern was also revealed in their descriptions of incidents.

Table 2: Level of concern reported by financial stakeholders[21]

N	Incident \ Likert Scale	1	2	3	4	5	Score*
1	User error	0	2	7	9	2	71
2	Information leakage	0	2	2	6	7	69
3	Malware	0	8	4	9	1	69
4	Phishing	0	8	5	7	2	69
5	Skimming	0	4	6	7	2	64
6	Unavailability	1	5	4	5	4	63
7	Unauthorized access	0	0	1	3	3	30
8	Internal fraud	0	1	3	0	2	21
9	Insider	0	4	0	1	1	17
10	Identity impersonation	0	2	0	1	1	13

Scale: (**1**) not at all, (**2**) slightly, (**3**) somewhat, (**4**) moderately, (**5**) extremely
* Weighted sum computed as the number of respondents by the Likert scale

Table 2 shows that financial respondents are very concerned about incidents with high frequency of mentioning, including user error, malware, phishing, and skimming. However, respondents are also very concerned about information leakage, which is an incident less often reported. Concern rises because respondents feel they lack adequate tools to effectively detect and prevent information leakage. Although a number of them have implemented elementary access control schemes (e.g., blocking USB ports), they admitted uncertainty about detection of data leakage, especially due to lack of visibility in distributed environments. The Likert scale failed to capture this issue. In addition to frequency, level of concern is often associated with respondents' perception of the quality of their security controls. To allow comparison, **Figure 5** integrates normalized scores of both frequency and concern for the eight top security incidents.

[19] Ordinal scale is used to protect respondents' privacy.
[20] Business models of institutions 10 and 11 do not use online banking services.
[21] Including financial authorities

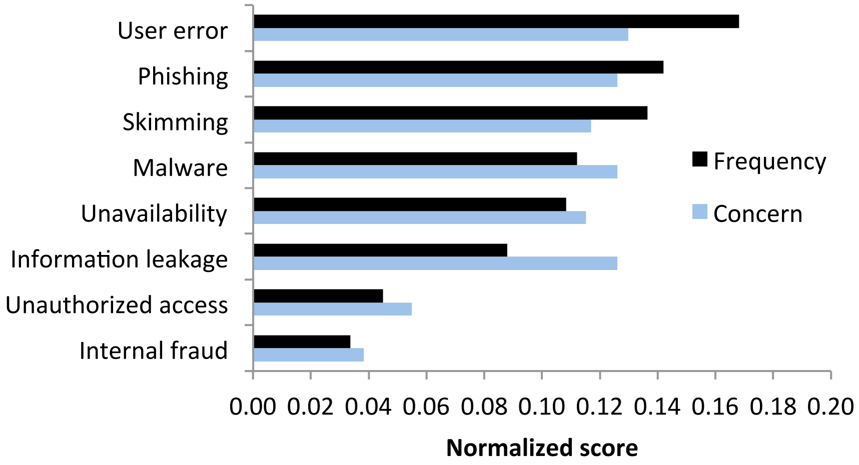


Figure 5: Frequency of incidents and level of concern

Threat Characterization. Financial institutions face threats posed by actions and inactions of insiders, outsiders, and even natural hazards. These threats can be classified in internal and external.

Internal Threats—The human component of an organization is perceived to be as important as the external threat because of inactions as well as intentional and unintentional actions that could lead to fraud or failures in C.I.A. As seen, *user error* is the most cited source of security incidents and the factor from which most concern arises among financial stakeholders.

External Threats—Attackers conduct research, obtain partners, develop tools, and perform individual and group focused attacks. First, they obtain information about their victims by stealing finance portable computers, breaking into customer's personal e-mails, and analyzing e-banking systems and ATM machines. Second, attackers find partners to facilitate the break-in and materialize a financial gain. Third, attackers design electromechanical, electronic, cyber tools, and social engineering methods to break into banks' defenses and to take advantage of customers' unawareness. Lastly, professional criminals conduct attacks, including skimmers with a high level of sophistication, including Bluetooth capabilities,[22] scams which impersonate customers to intimidate institutions employees, and malware to stealthily alter customers' computer operations (e.g., pharming).

Another factor that arose during the interview was an incident triggered by nature; specifically a flooding incident involving a data-center was described to point out that institutions have opportunities to improve their physical infrastructure to address natural disasters. Thus, institutions not only face cyber risks but also physical risks. **Table 3** characterizes the risk and associated level of concern. The most targeted elements of the financial infrastructure are ATMs and Internet banking.

[22] We had visual access to a video and pictures.

Table 3: Summary of risks

Type of risk	Triggers (threat)	Manifestation of the trigger	Freq. Score	Level of Concern*				
				1	**2**	**3**	**4**	**5**
Cyber-physical	collaborator / customer	user error	90		▮▮	▮▮▮▮▮▮▮	▮▮▮▮▮▮▮▮▮	▮▮
Cyber	outsider	phishing	76		▮▮▮▮▮▮▮▮	▮▮▮▮▮	▮▮▮▮▮▮▮	▮▮
Cyber-physical	outsider	skimming	73		▮▮▮▮	▮▮▮▮▮▮	▮▮▮▮▮▮▮	▮▮
Cyber	malware	unavailability / fraud	60		▮▮▮▮▮▮▮▮	▮▮▮▮	▮▮▮▮▮▮▮▮▮	▮
Cyber-physical	outsider/insider	information leakage	47		▮▮	▮▮	▮▮▮▮▮▮	▮▮▮▮▮▮▮
Cyber-physical	outsider/insider	unauthorized access	24			▮	▮▮▮	▮▮▮
Physical	nature	flooding	2					▮

Scale: (**1**) Not at all, (**2**) Slightly, (**3**) Somewhat, (**4**) Moderately, (**5**) Extremely concerned
* Elicitation of level of concern in Likert scale

2.4.2 Attitudes

Confidence. In our sample, some senior stakeholders felt confident enough to talk about their experiences and practices. They even showed examples of innovative techniques to enhance protection of customer's computers to prevent fraud driven by phishing.

Secrecy. High level of concern for confidentiality was observed when: (1) recruiting—it was challenging to obtain respondents (e.g., *"we do not talk about these issues outside of the organization"*) as noted earlier, and (2) interviewing—a respondent recognized secrecy as an institutional posture. Illustrative comments are incorporated here:

> *They [thieves] robbed here [this institution] by using a method, but I am not allowed to communicate and alert another institution* [Respondent R27].

Authorities also have noticed that some institutions act with reserve when dealing with consequences of phishing attacks to protect their reputation.

Perception of risk. We observed over-confidence by a small number of respondents in security controls (e.g., anti malware and perimeter protection) and low concern when dealing with malware in standard users' computers. However, magnitude of concern about malware rises when considering ATMs as a target.

Enthusiasm. We found a few financial stakeholders enthusiastic about learning and exploring new ways to better respond to information security risks. They also asked whether this study will pursue the creation of a local financial CSIRT and requested access to the present report.

2.4.3 Current Approaches

Learning by experimentation. Security incidents not only produce negative outcomes but also catalyze *positive* effects. Most executive managers at institutions become aware of incidents when they suffer negative consequences, so incident occurrence is a powerful instrument of situational awareness, especially when fraud is involved. The same reasoning applies to financial customers.

> *Awareness arises with education, communication and unfortunately with incidents* [R3].

Ad-hoc and formal collaboration. Stakeholders have developed small circles of trust, in which members collaborate in informal ways. For example, they may share phishing links when they receive them in their inboxes or specific information about fraud. Furthermore, there is at least one official forum in which institutions formally share information regarding frauds in ATMs—although respondents believe this collaborative initiative can substantially be improved [R20, R27].

Investment and Innovation. Large institutions with substantial budget set the upper bound on the state of the security practice in the nation (e.g., e-banking security), while smaller institutions follow their lead or at least model their strategies accordingly [R3, R20, R28].

> *Larger banks help set security standards* [R26].

Very small institutions seem to confine their efforts to fulfilling regulatory requirements because of budget constraints. In such cases, regulatory requirements play the primary role in fostering investment and managing operational risks.

2.5 Barriers to Incident Response

We first classify barriers by considering organizational boundaries (internal and external) and subsequently by areas in which those barriers were found.

2.5.1 Internal and External

Barriers were mentioned directly and indirectly during the interviews **Figure 6** and **Figure 7** consolidate explicit responses for questions addressing (1) barriers and (2) the biggest barrier. For instance, lack of *awareness* was cited as an internal barrier by five participants, three of whom believed it was the biggest barrier.

Internally, *team size* is the most frequently cited barrier and *lack of awareness* is the biggest barrier. Most of the biggest barriers are internal.

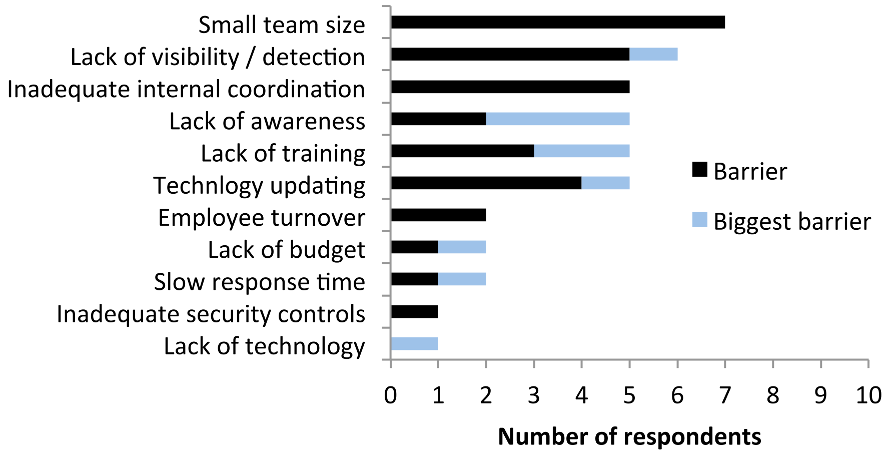


Figure 6: Internal barriers to incident response

Externally, the most mentioned barrier is the *weakness of the legal framework*, and *lack of support from ISPs* was emphasized as the biggest barrier by two respondents.

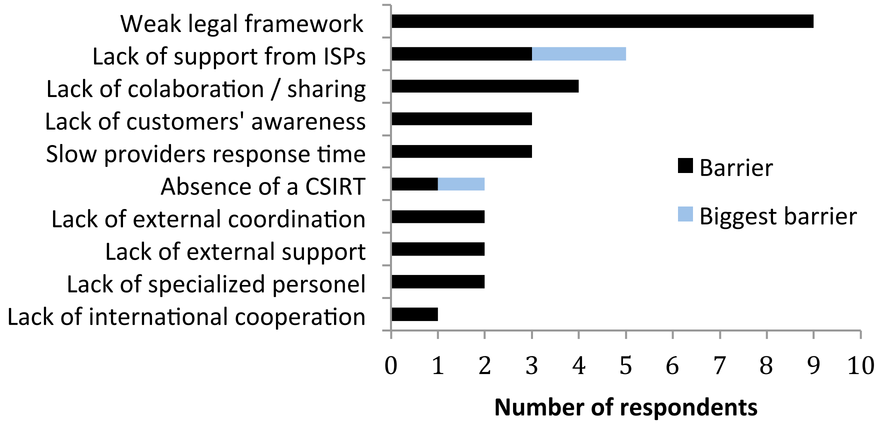


Figure 7: External barriers to incident response

Another way to understand these barriers is to categorize them by risk class: people, processes, technology, and exterior elements of the financial ecosystem.

2.5.2 People

Lack of awareness. The role played by humans in addressing security is a major challenge faced by stakeholders. To address this issue, it has been argued that systems with automatic and intuitive capabilities are needed to prevent human errors [29] and advocated that security awareness can be a major instrument [31, 32]. In this context, financial institutions face at least four of the five *dimensions of awareness*[23] as cited by Siponen [32].

Organizational unawareness—A few executive managers still need to be educated about observing security practices and convinced about investing in security.

> *How can I tell the executive manager that he should not connect his iPad into the corporate network?* [R3]

Some managers assess the probability of an incident occurrence by using a frequentist approach, so it is most likely that they invest in security after an important incident happens. In what follows, we present an illustrative narrative:

Senior executive	*E: Why did this event [incident] happen?*
Security staff	*S: Do you recall that potential issue we talked about some time ago?*
	E: I see. What do you need to take care of it?
	S: As discussed then, I need these resources...
	E: Approved. Do it right now! [R20]

Institutional education—Collaborators experience difficulty in fulfilling security policies and frequently value convenience over security. For example, users share their passwords to avoid organizational procedures or to timely achieve a particular operational goal. Here, stakeholders argue that security awareness is not only challenging to achieve but also insufficient. Awareness training should be supplemented with: (1) development of security culture so that self-discipline of security practices can become a natural attitude, and (2) enforcement of corporate security policies.

> *Awareness is not sufficient—we need to build security culture. Here, even an aware user has fallen into attackers' stratagems* [R21].
> *Investments to raise awareness, by itself, is not enough, security managers need authority* [R3].

General public unawareness—Members of the public are in the learning process about "invisible" cyber-risks inherently imposed by the usage of technology they often are not familiar with. In this process, many have failed to recognize elementary and advanced threats (e.g., phishing and pharming).

> *Until recently, customers only understood about the regular theft, but definitely not cyber* [R21].

Efforts from financial institutions to educate the public have been observed; however, the fact that customers still fall into attackers' traps provides a message—much more public education is needed.

[23] "Organizational, institutional education, general public, computer and ethical behavior, and socio-political." [32]

Computers and ethical behavior—People's behaviors and abilities to disrupt networks called for legal rules. Yet, until August 2014, stakeholders reported that it was nearly impossible to penalize cyber-criminals.

Insufficient size of security team. This is the most frequently mentioned internal barrier[24] among institutions and is driven by budget limitations. This issue does not allow managers to implement security capabilities in the organization. Most organizations establish a temporary and multidisciplinary CSIRT team in the presence of an incident, in which employees across the organization participate.

Lack of security specialists. Even institutions with a reasonable budget or substantial budget face constraints to locally find security specialists because of the scarcity of skilled workforce. This issue is not exclusive for financial institutions as ISPs face the same barrier, so they both often train and prepare their own personnel to handle security [R23, R7].

2.5.3 Processes

Training. High quality security training is mostly available overseas or brought by international instructors, which increases the cost. Lately, security certifications have become common among security professionals; however, high costs restrict people's access to those certifications.

Internal coordination. While mature organizations empower information security management in their institutions, a few medium- and small-sized institutions have not developed their organizational structure to foster incident capabilities. Authority and independence are needed to balance cybersecurity risks and business objectives, such as business departments pursuing business innovations and profit, and IT departments' duties consisting of releasing projects on time and keeping IT operations running.

Physical security provision. There is concern by some authorities about the inadequacy of physical security implemented by institutions that allows criminals to install card skimmers and steal debit cards (exchange of physical cards).

> *Watch the video, the criminal has been in the ATM lobby for about 20 min. Where are the security guards?*[25] [R30].

Provider and vendor support. Institutions need more timely response from vendors, security providers, and security services. Managers feel that not having local vendor representatives of security technology (available overseas) amplifies this limitation.

> *My provider's response time is very slow* [R21].

[24] Mentioned by 13 out of 18

[25] The interviewer had visual access to a video during one interview and pictures during two interviews.

2.5.4 Technology

Technology acquisition. The ability to acquire more advanced technology is limited to organizations with large enough budgets, so it is hard for small and medium sized institutions to automate capabilities for fraud detection and prevention. For instance, sophisticated anti-fraud software designed by developed countries is very expensive in the context of developing nations, so the cost exceeds the estimations of the risk in several cases.

Implementation and updating. Having the resources to acquire security technologies does not guarantee that they can be easily deployed and integrated. Some new technologies have been designed to work in homogeneous environments with high-speed communication networks. However, existing financial systems and architectures were reported heterogeneous, and complex, which includes legacy applications, diversity of (outdated) operating systems, and sometimes communicated over relatively low bandwidth communication links. Additionally, implementation of security best practices and security technology can imply modifications of legacy systems and updating network infrastructure. For example, old versions of Cisco routers require software (iOS) and hardware upgrades (DRAM)[26] in order to support secure protocols such as SSH.[27]

2.5.5 Externalities

Internet service providers' role (ISPs). Financial stakeholders and ISP representatives were asked about the role ISPs (do and should) play in the landscape of cybersecurity challenges faced by financial institutions. Two general concerns were addressed.

To begin with, financial respondents stated they need support from ISPs when confronting incidents, such as phishing, spam, and DDoS.[28] However, financial respondents believe that (1) it is hard to obtain ISPs' security support to respond to incidents and (2) the posture of the ISPs regarding incident security support is neither well defined nor communicated. Also, following legal procedures makes difficult tracking and tracing an attack local. For example, identifying the link between the IP address and the identity of an aggressor can be done, but in practice this procedure takes weeks or months when following legal procedures. Regarding this concern, ISPs reported that actions across domestic cyberspace networks are governed by the domestic legal framework, which does not allow grant an ISP with permissions to monitor or block customers' traffic. In this specific context, it is interpreted that the law privileges customers' privacy and their right to open connectivity.

In addition, there is a particular concern in the financial sector regarding cybersecurity practices of ISPs and the conceptualization of regulation in the sector:

> *Here [in this bank], the financial regulator conducts information security audits ever single year. I would like to know what the definition of regulation in the telecommunication sector is. Does it include cybersecurity?* [R3]

[26] Dynamic Random Access Memory
[27] Secure Shell
[28] Distributed Denial of Service

The fact is that cybersecurity regulatory requirements were not formalized [R5] in the telecommunications sector at the time of interviews. In large ISPs, security practices are implemented by self-initiatives [R7, R23]. A few ISPs have adopted a number of measures to prevent undesired events that could affect ISP network operational infrastructure. For example, they detect patterns of high-bandwidth consumption, and at least one ISP detects piracy copyright violations to take further actions based on contracts signed with its customers. In small ISPs, however, there is uncertainty about security practices. Apparently, small ISPs' business models do not allow them to invest in security [R18]. Informed respondents from ISPs stated that there are 300 small ISPs sharing 1% participations of the local market, and their assessment is that the risk is relatively low [R3, R22]. Nevertheless, even smalls ISPs can provide an attacker with an entry point into the larger financial ecosystem.

Legal framework. Weakness in the legal framework was the most mentioned barrier across all categories and respondent groups. Respondents explained that legislation to effectively punish cybercrime was absent, and, furthermore, administrative procedures to enforce the law need to be improved.[29]

> *Theft cannot be proved –even if we have the skimmer as evidence* [R17].

When dealing with crime, we found three types of institutional postures. First, a few institutions opt for not pursuing legal actions so as to protect their corporate image and save resources and time since they feel justice administration could involve a lengthy and convoluted procedure. Second, institutions pursue legal actions but have difficulties in demonstrating responsibility even when thieves are caught performing cyber-physical attacks on ATMs. Third, and less frequently, some engage in detailed investigations to (1) uncover criminals and (2) bring them to justice—institutions have creatively succeeded in the former objective and failed in the latter.

Foreign influence. Observation of national borders is not trivial when confronting transnational cyber-physical security threats [33]. Respondents observe that particular forms of crime expand and migrate from nearby Latin American countries. Interviewees often linked neighbors to the north with skimming attacks and very often the closest neighbor to the south with the source of phishing attacks. Trends can be identified to predict attackers' next steps by observing cybersecurity-related events in nearby nations [R13]. Additionally, the lack of *international agreements*[30] limits the range of actions that authorities can take to pursue investigation and deterrence [R29]. In this area, OAS[31] recognizes that the nation's ability to strengthen international collaboration in cyberspace needs to be improved [22].

[29] At the time of the interviews, a new legal framework to address cyber-crime was released in the country.

[30] The Budapest convention on cybercrime was cited as an example.

[31] Organization of American States

Barriers to respond are summarized in terms of the *risk class* [34] in which they emerge as follows.

Table 4: Summary of barriers to incident response

	Barriers	Contributory Factors
People	- Lack of Awareness - Insufficient human resources - Insufficient professionals in the market - Employee turnover	- Insufficient budget - Institutional business profile - Insufficient academic education in cybersecurity - Lack of knowledge
Technology	- Lack of technology - Technology implementation and updating	- Insufficient budget - Diversity of systems and legacy systems
Process	- Internal coordination / communication - Effectiveness of security controls - Visibility of the network (detection) - Lack of training	- Business priorities - Lack of empowerment - Operational daily activities - Insufficient budget
Externalities	- Lack of collaboration / sharing - Coordination with financial institutions - External support of Internet providers - Lack of local specialized personnel - Inappropriate legal framework - Response time of providers / vendors - Absence of a CSIRT / SOC	- Lack of international cooperation - Lack of communicative procedures - Lack of trust

There are differences and commonalities when comparing the main barriers we found in Ecuador with barriers reported in a developed nation. In the USA, the New York Financial Services' cybersecurity study (2014) reports the more cited barriers to ensure information security in the financial sector [14]. **Table 5** shows a comparison of barriers between Ecuador and the USA and highlights differences. As seen, there are more similarities than differences. One important difference is in the top-one barrier, which stresses the contrast between developed and developing economy. Although lack of awareness was not the most cited in Ecuador, five respondents emphasized it as the biggest barrier they face. This barrier can be linked to cultural and educational aspects of the population, so different types of institutions face a different biggest barrier.

Table 5: Comparison of barriers by frequency of mentioning

Rank	Ecuador	USA
1	**Weak legal framework**	**Increasing sophistication of threats**
2	Security team size	Emerging technologies
3	Lack of visibility	Lack of sufficient budget
4	**Inadequate internal coordination**	Lack of visibility
5	Technology updating	Inadequate availability of security professionals
6	**Lack of training**	Lack of clarity on mandate, roles and responsibilities
7	**Lack of awareness**	**Inadequate functionality**

A developed economy seems to attract higher level of threat sophistication. Whereas the US financial services already face very advanced threats (e.g., hacking into internal systems that leads to data breach) [35], Ecuador faces cyber threats that is on its way to enhancing its sophistication (e.g., malware attacks to ATMs). This situation indicates that Ecuadorian financial sector necessitates to prepare for even more aggressive attacks than those confronted so far.

2.6 Strategies

Two potential strategies to build incident response capabilities, establishing a *financial CSIRT* and promoting an *information sharing program,* were assessed to find how they may work in this case study.

2.6.1 A Financial CSIRT

Because Ecuador currently does not have a national CSIRT, the financial sector lacks external incident response support of such kind. EcuCERT, a team operating since 2014, focuses its provision on the telecommunications sector and certain areas of government. To address this lack of support, potential services and organizational aspects of a financial CSIRT were discussed during the interviews.

CSIRT capabilities. We elicited external security support needs. First, financial respondents spontaneously explained the external CSIRT services they needed. **Figure 8** shows that the most frequently requested service was information sharing.

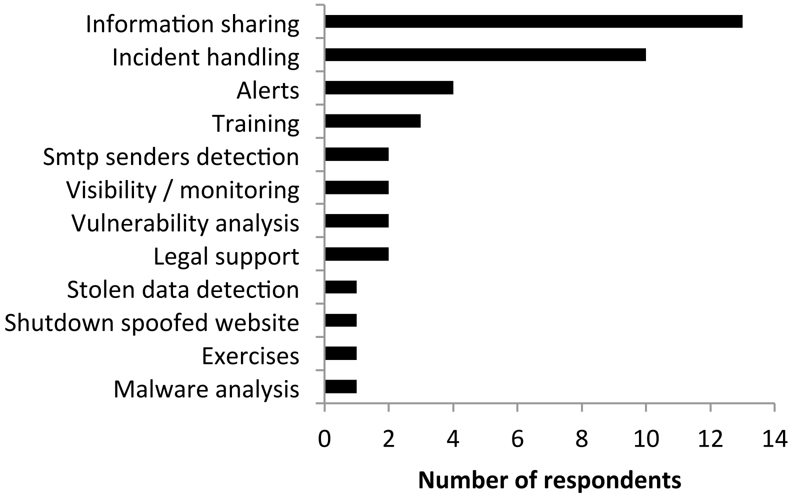


Figure 8: Services brought up by financial stakeholders (spontaneous)

Subsequently, respondents were presented with a list[32] of reactive and proactive services services [36], to which they assigned a *level of importance*[33] and justified their choices. In each case we asked respondents why they needed a particular service and why they assigned the level of importance they chose. This approach provides insights on how to prioritize potential services.

[32] The list was composed of eight services, one reactive and seven proactive.

[33] Likert scale from 1 to 7

Table 6 presents the results from the elicitation and the ranking score. There were four major services that most respondents classified as very or extremely important: *alerts, incident handling, information sharing, and training*. Beyond those, *legal support* was thought of as moderately important.

Table 6: Level of importance of CSIRT services (guided)

N	Incident \ Likert Scale	1	2	3	4	5	6	7	Score*
1	Alerts	0	0	0	0	2	4	11	111
2	Incident handling	0	0	0	0	4	8	6	110
3	Information sharing	0	0	0	0	1	7	8	103
4	Training	0	0	1	0	7	6	4	102
5	Legal support	0	0	1	3	8	3	3	94
6	Exercises	1	0	0	0	4	6	5	92
7	Vulnerability analysis	2	1	3	5	2	3	2	75
8	Malware analysis	1	0	0	3	2	3	3	62

Scale: (**1**) never, (**2**) rarely, (**3**) occasionally, (**4**) sometimes, (**5**) frequently, (**6**) usually, (**7**) every time
* Weighted sum computed as the of number of respondents by the Likert scale respectively

Next, we describe perceptions of these services in rank order.

Alerts—Often, alerts were linked to having relevant information (e.g., threats) to support the function of prevention. They need to be available at the right time and provide actionable information. Respondents envision this service as an outcome of subject matter expert research—analysis of relevant threats and vulnerabilities in the financial sector—as opposed to simply replicating generic information.

Incident handling—Respondents asked for assistance for specific types of incidents based on the following criteria:

- *Expertise:* incidents that require specialized knowledge (e.g., DDoS, phishing). A respondent stated that for some type of incidents external assistance may not provide more knowledge than institution's technicians already have (e.g., technical errors associated with in-house developed systems).
- *External influence:* incidents that require actions from private and government institutions (e.g., phishing, pharming).
- *Spread of the threat*: incidents that have a broad range of impact (e.g., card skimming)
- *Innovation of attacks:* incidents linked to technically sophisticated threats (e.g., advanced malware, card skimming).

A few participants, however, may refrain from requesting assistance for handling incidents that involve very sensitive information (e.g., internal fraud).

Information sharing—Respondents want global and local statistics and patterns about security incidents that include other participants in the sector. They also want information about successful cases of strategies implemented to mitigate or prevent incidents' impact (e.g., customer's awareness).

> *The CSIRT should be the cluster where we could report our experiences and learn from other experiences* [R14].

Training—Areas of desired training include preparation in incident handling, ethical hacking, and digital forensics, and support to educate the public. Some participants also wanted to obtain security certifications directly from the CSIRT so as to reduce costs by avoiding commercial intermediaries.

> *The CISRT should be the entity that authorizes certifications as opposed to commercial firms* [R28].

Legal support—Many ranked legal support as less important. While most respondents say, "*We already have a legal department*," supporters for this service argue that there could be crime-related events in which they may not know how to proceed.

> *If I detect criminals in my infrastructure, should I take picture of them, should I hold them…?* [R20].

Exercises—We described exercises in terms of a simulation of a security emergency with the purpose of validating an incident response plan [37]. Interest in this service is raised by the benefit of evaluating the readiness for a particular type of incident. Local (non-financial) CSIRTs added that greater benefits could be obtained if exercises are coordinated with them.

Vulnerability analysis—Most participants are not interested in this service with exception of a couple of small financial institutions. While large banks have an internal process for vulnerability analysis, small institutions lacking abilities to establish such process showed interest. In general, knowledge about common vulnerabilities for the financial sector is most desired, which is included in *alert services*.

Malware analysis—Respondents in large and medium size institutions stated that they already have technical support from antivirus firms.[34] Small institutions face a bigger challenge in this area since the levels of customized support they can obtain from vendors and providers of security technology are limited.

Finally, some respondents have a broad expectation of a financial CSIRT, including, monitoring of networks, support to shut down spoofed websites, attribution of data disclosure (e.g., individuals selling private data), and identification of senders of spam and scam e-mails.

[34] Although some of the respondents complained about response time during technical support

CSIRT organization

Authority[35]—Assessing what kind of authority the financial CSIRT should have was a controversial topic. Three approaches were discussed: a CSIRT with legal authority over its constituents, one with no legal authority, and one with a different kind of authority (e.g., *shared authority*[36]). **Figure 9** shows the distribution of preferences by group of stakeholder.

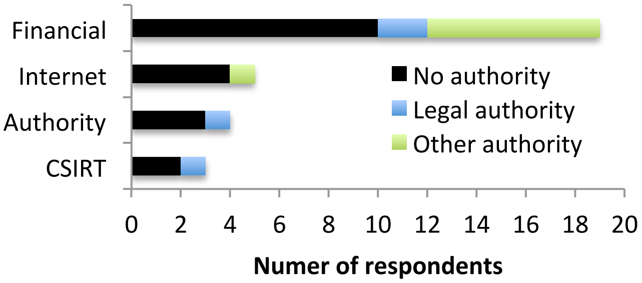


Figure 9: CSIRT legal authority

Most financial respondents envisioned a CSIRT with no legal authority that only recommends and supports because of these reasons: fear of political influence, aversion to establishing a CSIRT with regulatory power, self-determination about risk decision-making, and trust of constituents.

> *Trust is most important than authority so that banks feel they are supported* [R10].

A second group believed legal authority is beneficial and argued that financial institutions occasionally need to be prescribed cybersecurity policies. Others suggested a third approach, in which the CSIRT exercises influence over financial institutions by establishing agreements such as shared authority among institutions. Further discussion incorporating views of additional institutions would be helpful.

Location—We asked where the financial CSIRT should be physically and organizationally located by considering government, academia, and the financial industry. Many reported the ideal option would be academia because a CSIRT needs research capabilities. However, they have concerns about the ability of local universities to address this challenge, including managing financial confidential information. The financial industry establishing a CSIRT is seen as a pragmatic option because of that sector's risk specialization and trust. There is a major concern about undesired political influence when having a CSIRT in the government.

[35] "Authority describes the control that the CSIRT has over its own actions and the actions of its constituents related to computer security and incident handling activities." [111]

[36] "If the CSIRT has shared authority, it works with the constituency to influence the decision-making process concerning what actions should be taken." [111]

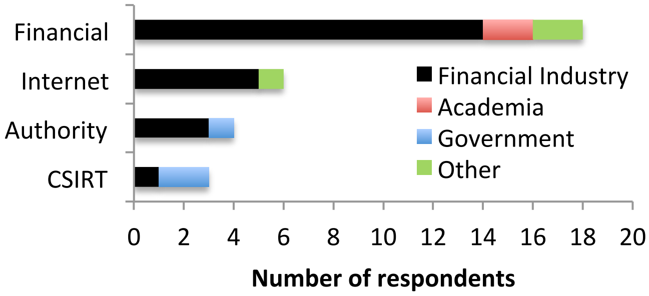


Figure 10: CSIRT location

In the financial industry, respondents of all groups very often linked their choices with the *Asociacion de Bancos Privados del Ecuador* [Ecuadorian Private Banks Association] as a specific place to locate the financial CSIRT. [37] The alternative *other* includes: (1) a hybrid approach between academia and the financial industry, and (2) a private independent CSIRT. Here, a potential successful model should consider the current synergy and empowerment developed by the *National Financial HUB*[38] handling transactional operations of ATMs in the nation.

Funding—Most respondents proposed to distribute the CSIRT operational cost among financial institutions by considering institutions' number of customers, while a couple of respondents state that all should pay equally. The former model is currently working in the telecommunications sector, where costs of telecommunication backbone equipment and services are distributed among ISP corporations according to the network traffic they interchange in the Internet. The latter model is currently working in the financial sector for ATMs operational services, which is based on a fixed fee for standard services without considering institutions' size and a variable cost depending on the additional assistance these institutions request.

2.6.2 Information Sharing Program

A centralized information sharing architecture is often discussed as a means to reduce uncertainty about threats [38]. In this study, we addressed information needs, properties of a sharing program, and respondents' willingness to share (WTS) information.

Information needs. There is interest in information related to the elements surrounding security incidents as follows:[39]

- ***Typology of threats***—classification of threats.
- ***Attack vectors***—modus operandi of (cyber) criminals, including methods of propagation and exploited vulnerabilities.
- ***Defense***—successful techniques that defenders have used to mitigate the threat.

[37] The problem with this approach is that public financial institutions may not be included.

[38] Private institution managing ATMs machines across the nation and administrated by local financial institutions

[39] Types of data listed in order of frequency of mentioning

- ***Weaknesses of controls***—methods, technologies, and other security controls that failed to defend institutions against threats.
- ***Threat intelligence***—identification of fraud trends in the local financial sector and nearby countries.
- ***Economic impact***—quantitative data on losses.

Incentives for information sharing. The factors that potentially can incentivize respondents' participation in a sharing program are as follows:

- ***Confidentiality*** of the shared information. This is the most relevant concern, so respondents expect a confidentiality agreement and ethical behavior by those running the program.
- ***Trust*** developed by the program, which is the strongest incentive.
- ***Security and privacy*** incorporated in collection, storage, processing, and distribution of the data (e.g., data anonymization).
- ***Type of information*** that the program will propose to exchange, which will not conflict with restrictions imposed by internal corporate rules for information classification.
- ***Participation of large banks****,* which will strongly influence participation of other institutions.
- ***Leadership*** to establish democratic rules for the program and develop commitment of participants.
- ***Potential knowledge*** acquisition from the sharing program.
- ***Reciprocity*** based on mutual interchange of information.

> *I would participate only after a non-disclosure agreement to protect our institution and our customers is in place* [R28].

Additional expectations when running the program include accuracy and usability of the information; without these, information reports could be ignored, in which case the program could lose perception of value.

Metrics for sharing. The metric question was one of the most challenging for participants, which reflects the difficulty of objectively measuring benefits when mitigating risks. Respondents mainly described metrics in terms of outcomes that reflect achievement of goals, including:

- Number of incidents detected, prevented, or mitigated in a period of time
- Quantitative estimation of fraud prevented in dollars
- Number of timely reports from the Information Sharing Center
- Number of submissions done by financial institutions
- Percentage of financial institutions reporting information
- Improvement in time to respond against fraud

> *If we obtained information that allows us to reduce the impact of fraud, that information would be the best!* [R3].

Willingness to share (WTS). We assessed WTS by considering the type of information generated during the course of a security incident, which includes technical details from the attack, as well as information about the target and the impact of the attack. By using two threat scenarios, phishing[40] and hacking,[41] we presented respondents with a binary decision (share *versus* do not share). In **Table 7,** the column headings show eight components of information generated as a result of an attack, and the rows indicate a binary outcome representing whether or not stakeholders would share information.

Table 7: WTS of 13 institutions' representatives[42] for scenarios P and H

Data Type / WTS		IP address	Asset type	Attack vector	Malware sample	Mitigation strategy	Qualitative impact	Quantitative impact	Vuln. *
P	Yes	13	10	12	12	12	12	1	6
	No	0	3	1	1	1	1	12	7
H	Yes	10	8	9	9	9	8	1	2
	No	3	5	4	4	4	5	12	11

P: Advanced phishing. **H**: Web hacking.
* Vulnerability

In our sample, WTP exhibits dependency on the type of data involved in a phishing attack. In evaluating hacking attacks, an important difference is that fewer respondents (two out of thirteen) are willing to share information about the vulnerability that was exploited during an incident involving hacking. Thus, different types of incidents[43] also lead to different WTS behaviors.

Overall, most respondents are willing to share technical information with some restrictions (e.g., details about security equipment). Conversely, respondents are not willing to share quantitative data about the impact of an incident to protect their reputation and to prevent misinterpretations. Some argue that the same amount of losses can have different meanings for different organizations [R4].

2.7 Discussion and Conclusion

This study finds that Ecuadorian financial services face challenging cyber-physical risks, have little community security support, and could benefit from information sharing as well as the creation of a CSIRT that provides and supports the adoption of strategies for better protection. While one of the most relevant studies addressing cybersecurity in developing countries stressed that those nations marginally experience cyber-attacks [6], there are specific sectors that do bring attackers attentions at present. In Ecuador,

[40] Advanced phishing—including malware capabilities (pharming)

[41] Hacking of an institution's web server

[42] This table reports the preferences of one representative for each financial institution (the most senior in our sample).

[43] These two scenarios, phishing and hacking attacks, are different in two ways: phishing is a popular attack reported by the population and local press reports, and this type of attack could potentially produce information about both banks and their customers. In contrast, hacking of financial infrastructure is rarely reported and mostly includes information from the financial institution.

financial institutions confront both internal and external security challenges when dealing with security incidents.

Internally, user error, unauthorized access, and information leakage raised general concern among financial institutions. Malware was seen as more harmful when it targets ATMs or customers (e.g., pharming), whereas information leakage caused concern not only because it has often been indirectly detected, but also due to uncertainty about both the frequency of its occurrence and estimations of losses. Externally, card skimming and phishing alarm stakeholders differently. Phishing raised the concern of authorities but not among all institutions because this is an attack focused on selected targets—only major banks across three cities faced it persistently. Skimming attackers take advantage of failures on *interdependent security*, especially financial institutions that had not fully adopted EMV by the time of interviews. Moreover, the human factor as a source of incidents (user error) was omnipresent both inside and outside of institutions.

Stakeholders adopt a diversity of approaches in defending against these threats. However, security incidents still produce harm because (1) financial stakeholders often face these categories of limitations: financial, technological, administrative, and external barriers imposed by the ecosystem; and (2) attackers actively adapt to institutions' defense strategies. There is a life cycle of competition between the attackers that create electronic and cyber tools to conduct fraud and the defenders that develop tools and techniques to protect the financial system.

In terms of legal response to the aggressor, the risk of punishment was very low for (cyber) criminals due to a lack of deterrence. For this reason attackers feel motivated by the potential gains that come with minimal risk [39]. Although no single "doctrine," such as accountability, may be effective to ensure cybersecurity [11], our work supports the belief that law enforcement is an essential element to mitigate the risk of cyber-physical threats [6]. By the time of finishing the interviews, Ecuadorian authorities updated the law to specifically include several forms of cybercrime.

Regarding mitigation strategies, our work takes the first step to assess whether or not collaborative functions of incident response capabilities could work. First, the results from the elicitation of needs for specialized Financial CSIRT security services indicate that alerts, incident handling, information sharing and training as services are all desired and would be most welcome. Organizationally, the financial industry currently seems to be the best place to establish the CSIRT. Further discussion is necessary to define the type of CSIRT authority. Second, assessment of willingness to share suggests that financial stakeholders may share technical details of incidents depending on their types. However, quantitative aspects of the impact of security incidents are viewed today as too sensitive to share by most stakeholders. Sharing could potentially be practiced under formal conditions that foster trust, such as confidentiality agreements and security measures taken to ensure that confidentiality is maintained. In terms of effectiveness, the success of the sharing program will ultimately be measured by its impact on fraud reduction.

While our study obtained empirical data from a diverse group of financial stakeholders across institutions and the country, it obviously does not explicitly capture the views and experiences of those institutions that declined to participate. To partially address this limitation, we included in our study the views of stakeholders (e.g., authorities) who have a broad and firsthand knowledge of incidents occurring in the financial sector, and pursued replacement of potential participants from institutions of similar size.

Our results show some commonality and differences with the results of a survey study conducted with the financial services in the USA [14]. The four biggest barriers to ensure information security in the US financial sector are: increasing sophistication of threats, emerging technologies, lack of sufficient budget, and lack of visibility. In Ecuador, our respondents report that the major *internal* barriers to respond to security incidents are security team size (which can be linked to budget), lack of visibility, inadequate internal coordination, technology updating, lack of training, and lack of awareness. Interestingly, we observe three similarities in the top four barriers and one marked difference. We believe that the difference can be explained by factors related to the higher level of sophistication of attackers targeting the USA and the difficulties found by stakeholders in Ecuador when coordinating cybersecurity operations with IT departments internally.

This work contributes to the literature of cybersecurity incident response in the context of developing countries and to our knowledge is the first study of its kind conducted in South America. Related studies can be found only on the context of cybersecurity strategies for developing African and Caribbean nations [6, 8], and building national cybersecurity response teams [20, 21], but none of them concentrates analysis on a specific critical infrastructure sector in depth. Additionally, to our knowledge this is the first study that collects and reports data by using cyber-security scenarios from financial institutions and elicits willingness to share in a systematic way.

Ultimately, this work should be able to contribute to improving cyber-security practice in Ecuador's financial sector, especially if stakeholders take steps to establish a *Financial CSIRT* and a customized *Information Sharing Program*. Future work will expand this study to identify, refine, and assess strategies that address additional elements of the barriers we have identified.

Acknowledgements

I am thankful for the guidance and advice of M. Granger Morgan and Howard Lipson. I also thank the feedback from Gabrielle Wong-Parodi for her support regarding qualitative analysis, as well as Lorrie Cranor, Jon Peha, and Casey Canfield for feedback in regard to interview questions. This research received economic support from the Department of Engineering and Public Policy at Carnegie Mellon University. The author also received support from the Fulbright-Senescyt Program.

Chapter 3

Policy Treatment of Cybersecurity Incidents in a Critical Infrastructure Sector

Abstract

Cybersecurity policy making in the financial industry has been motivated by advanced threats targeting this critical infrastructure sector. Policies providing guidance are essential to enhance protection. Traditionally security (and privacy) regulations have been studied in order to support compliance; in software engineering understanding regulatory requirements is an input that is crucial to designing software in compliance with regulations. Nevertheless, assessing effectiveness of regulatory requirements has been less often analyzed. Despite recent efforts to reveal the impact of regulations on mitigating security incidents, there is still a lack of understanding concerning security policies' appropriateness, especially in the context of developing nations.

In this paper we assess the effectiveness of the security risk management policy for the Ecuadorian financial sector. Based on data about security incidents obtained from interviews conducted with thirty-three Ecuadorian financial stakeholders (risk managers, security chief officers, security officers, risk officers) and national authorities (managers, supervisors), we conduct a gap analysis to assess effectiveness of regulatory statements in addressing these security incidents. Using a four-stage method, this work: (1) collects and categorizes security incidents; (2) analyzes threat patterns initiated by smart adversaries by using attack trees; (3) identifies countermeasures from security standards and best practices—from ISO, PCI, and CSI—to mitigate the risk; and (4) conducts a gap analysis by mapping security controls to regulatory requirements.

This financial risk management policy has been reasonably successful in including controls that address several incident profiles reported by financial stakeholders. Incidents related to phishing, user error, and information leakage are mostly covered, while incidents in the category of fraud present gaps raging from minor to moderate. Substantial gaps are found with respect to DDoS, spam, and malware infection. We found that while security incidents are focused on mitigating fraud, areas of corporate security, such as network security, are left to financial institutions to manage.

3.1 Introduction

Over the last few years, concerns regarding the ramifications of cybersecurity risks have already reached top-level national and international decision-making. Voluntary and mandatory guidelines have been proposed in the public and private sectors. Both industry and governments advocate for *voluntary* security standards and best practices to manage cyber risk in organizations and, therefore, mitigate the effects of security incidents. Such initiatives include ISO 27002, Common Criteria, NIST framework 2014, COBIT, and more. In addition, because it has been clear that most sectors need incentives to provide better information security, both industry and governments have established *mandatory* baselines to manage cybersecurity risk in IT operations. PCI-DSS, for example, is a self-regulatory initiative in the card payment industry, whereas at the government level regulatory frameworks such as the Bank Protection Act and the US Patriot Act regulate the financial sector in the USA.

Regulatory requirements can impose a burden on the members of society involved due to costs of compliance and enforcement (economic, effort, and time). Regulations can even restrain innovation when it is not specifically mandated [40]. Because cybersecurity regulations are expected to be effective to mitigate risks, it is reasonable to inquire about the adequacy of cyber regulations in achieving their intended goals.

Understanding the potential effectiveness of cyber-regulatory frameworks is crucial to design policies that are more likely to accomplish their envisioned goals and prevent negative outcomes. A first step toward improving this understanding is to assess the potential effect of regulatory statements of cyber policies in preventing security incidents. Hence, this study analyzes security incidents, as reported by Ecuadorian financial stakeholders (institutions and authorities) during 33 interviews, in order to assess the effectiveness of the Ecuadorian financial regulatory framework for IT risks.

Ecuador provides a suitable environment for this study because its regulatory framework does not have the complexity of the regulations enacted in developed nations, such as the USA. Also, data with details about incidents from primary sources (financial institutions) have been collected across the country in our previous study (2014). In Ecuador, the first regulation addressing cyber risks in IT financial operations appeared in 2005. This regulatory framework (JB-834) was created to support operational risk principles as specified by the committee on banking supervision Basel II. Subsequently, the regulation has had two major updates, one in 2012 (JB-2048) and the other in 2014 (JB-3066) [41]. These updates have included a wide range of requirements designed to mitigate operational risks arising in areas of processes, people, and information technology.

Research reported in this paper is intended to provide policy makers with feedback and inform regulation implementers about how investing in such regulatory requirements can impact their efforts to mitigate security incidents and help improve their risk management process. The structure of the paper is as follows: *section 2* provides a literature review; *section 3* describes the method; *section 4* presents a threat, defense, and gap analysis; *section 5* summarizes the results; and *section 6* discusses the research findings and concludes.

3.2 Literature Review

Areas of research addressing the intersection between policy and security issues, which are related to our work, include: (1) extraction of security (and privacy) requirements from regulations; (2) gap analysis of security requirements; and (3) security threat modeling.

First, regulations related to IT security and privacy have been analyzed with the purpose of extracting legal requirements and translating them into technical capabilities for information systems. Such efforts and methods are described by Anton [42], Breaux and Anton [43, 44], Breaux et al. [45, 46], Mellado et al. [47], Haley et al. [48], Islam and Jürjens [49], Siena et al. [50], and Gordon and Breaux [51]. The ultimate intention of these methods is to elicit technical requirements from legal statements to pursue compliance and improve systems security. These techniques are closely related to methods used in software engineering to identify security, privacy, and functional-related requirements, such as SQUARE,[44] NFR,[45] KAOS,[46] and Tropos.[47]

Second, gap analysis of regulatory requirements has been conducted for the networking industry and finance services. Breaux et al., (2008) used section 508 of the U.S. Workforce Investment Act of 1998 to identify compliance gaps in design features (accessibility) in a Cisco product [46]. Based on a semantic framework (FBRAM[48]) [52], the authors extract legal requirements and compare them to technical requirements included in Cisco accessibility standards. A pertinent conclusion emphasizes the need for techniques to reduce ambiguity in regulatory statements.

In our previous work (2010), by using standard mapping, we conducted a gap analysis between JB-834 version 2005 and Cobit 4.1 and also JB-834 version 2005 and ISO 27002:2005. At that time, in the realm of information security, multiple gaps were found, especially in ISO domains referring to access control and acquisition, development, and maintenance of systems [53]. Since then, JB-834 has experienced two substantial updates, and ISO 27002 one update (2013).

In his MS thesis, Kurt (2015) analyzes data breaches on the U.S financial sector [54]. By considering nine vectors of attack reported by Verizon (2014), the study performs a gap analysis to identify differences between best practices (20 Critical Security Controls from CCS[49]) and statements contained in U.S. laws and regulations addressing data breaches. Gaps for each *best practice* are estimated in two levels of coverage (full: 100% and partial: 50%) for those attack vectors.[50] No details are provided to describe how the actual mapping was conducted. Findings for the banking sector indicate that the pattern with less coverage is *Miscellaneous Errors (25%)* and the most

[44] SQUARE: Security Quality Requirements Engineering by CERT/CC

[45] NFR: Non-Functional Requirements by J. Mylopoulos et al. (1992)

[46] KAOS: Knowledge Acquisition in Automated Specification by A van Lamsweerde et al. (1991)

[47] Tropos by A. Susi et al. (2005)

[48] FBRAM: Frame Based Requirements Analysis Method

[49] CCS: Council on CyberSecurity

[50] Gap for one of the attack vectors is not reported (card skimming) since CSC does not address it.

addressed is *Physical Theft Loss* (83%). Overall, lack of effectiveness was found in banking, one of the sectors of the financial services [54].

Third, threat-modeling allows identification of latent threats to IT systems [55] and security requirements [56]. Approaches to threat modeling include, software system models (STRIDE[51]), logic based threat models (Fuzzy Logic), vulnerability-based model (T-MAP), threat scenarios model (attack trees, CORAS), protection-based models (defensive tree), attack graphs, and misuse models. Particularly, attack trees model a security (attack) scenario to analyze adversary strategies against a system, weaknesses of the system, and potential ramifications of the adversary actions.

Work on attack trees is vast. Conceptualization of attack trees has its origin in safety and reliability analysis (e.g., fault trees). Application of this notion to security modeling was advocated by Weiss (1991) [57], Amoroso (1994) [58], and Leveson (1995) [59]. Attack trees were introduced by Salter et al. (1998), and expanded by Schneider (1999).[52]

Attack trees have been further developed and named depending on aggregation of attributes and their particular utilizations in security modeling. Today, attack trees can embrace probabilities, cost, attacker abilities, time of attack, and Bayesian techniques. Some of these capabilities are included in: augmented vulnerability tree, augmented attack tree, OWA[53] tree [60], extended fault tree [61], ACT[54] tree [62], and enhanced attack tree [63]. In addition, by considering components of risk and goals, there are: vulnerability tree [64],[55] protection tree [65], threat tree [66], attack-countermeasure tree [62], and attack-defense trees [67].[56] When envisioning trees for infrastructure assessment, the terms archetypal tree and concrete tree have been introduced [68]. Regarding their application, multiple studies have used attack trees to analyze security properties on systems and beyond, including online banking systems [69–71], metering infrastructure [68], SCADA[57] systems [72], electronic voting system, and homeland security [65].

This paper uses attack-defense trees [67] to assess the effectiveness of the Ecuadorian regulation. Attack trees allow us to incorporate *adversarial thinking* into our analysis, which are a fundamental component of security incidents where attackers are main actors. Additionally, the defense component fits with the essential mission of regulatory statements, which is providing directions to implement *countermeasures* to mitigate risks.

In brief, the examination of relevant literature indicates that most studies focus on understanding regulatory content to advocate compliance whereas our study takes the opposite route by assessing the potential effectiveness of those requirements. In that

[51] Microsoft's Threat Model

[52] A comprehensive survey of literature on attacks trees has been provided by Kordy et al. (2013) [112].

[53] Ordered Weighted Averaging

[54] Attack Countermeasure Tree integrates multi-objective optimization

[55] Formerly known as Threat logic trees (TLT)

[56] This is not an exhaustive list but certainly representative.

[57] SCADA: supervisory control and data acquisition

respect, Kurt's work has taken such direction by considering the U.S. financial sector. Our research differs from previous work in a number of ways: (1) the financial sector is examined in a different context—that of a developing nation; (2) the method for collection of incidents is disparate—while Kurt analyzes Verizon's surveyed data on one type of threat consequence (data breach), we use our own data collected during interviews containing deeper details on incidents, which comprises additional consequences (data breach, unavailability, fraud); and (3) our method for identifying countermeasures considers more than one source of subject matter expert and uses attack tress to model threat and protection.

Despite recent efforts to reveal the impact of regulations on mitigating security incidents, there is still a lack of understanding concerning security policies' appropriateness. Though our study we intend to improve comprehension of regulatory effectiveness in a different geographical context by considering additional details on incidents, incorporating a formal method to analyze threat-response, and covering vectors of attack and consequences that were absent in previous related work.

3.3 Method

The method encompasses four stages, which comprises incident data preparation, threat analysis, defense (protection) analysis, and gap analysis.

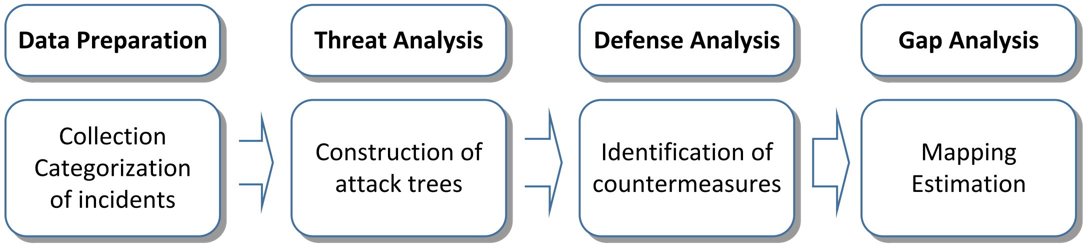

Data Preparation
Threat Analysis
Defense Analysis
Gap Analysis
Collection Categorization of incidents
Construction of attack trees
Identification of countermeasures
Mapping Estimation

Figure 11: Framework for assessing effectiveness

3.3.1 Data Preparation Stage

During the *data preparation stage* we collected, structured, and categorized narrations *of **security incidents***.[58] These security incidents were reported during interviews conducted in 2014 with 33 Ecuadorian financial stakeholders (risk managers, security chief officers, security officers, risk officers, a compliance manager, and an IT manager) and authorities who control, assist, and investigate managerial and technical aspects of security incidents (managers, supervisors, and a police officer). In terms of the trigger of an incident, three classes of incidents were identified and narrated: (C1) attacks by smart adversaries; (C2) involuntary errors by computer systems' users; (C3) and actions of nature, only one incident.

In order to analyze the incidents reported by financial stakeholders, we used another method of categorization of incidents with three levels: (1) a *security incident*[59] is

[58] "A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" - NIST

[59] This paper adopts NIST definition

a narration of security events reported by respondents; (2) an *incident profile* describes a specific pattern that characterizes a security incident. An incident profile can describe a subset of security incidents following the same pattern; (3) an *incident category* is a set of incident profiles grouped by the trigger of the risk (e.g., malware), the attacker's technique (e.g., skimming), or the outcome of the risk (e.g., fraud). **Table 8** summarizes these terms and the associated hierarchy.

Table 8: Terminology hierarchy of security incidents

	Term	**Example**
Hierarchy	Incident category	Unauthorized access
	Incident profile	Unauthorized physical access
	Incident	Outsiders get access to an ATM vestibule
	Incident	Outsiders get access to banks' facilities

Security incident profiles in class C1 were structured by using Howard's Taxonomy [73],[60] which identifies the following elements: attackers, tools, vulnerabilities, actions, targets, results, and objectives. What a respondent reported about an incident often supplemented or overlapped with the details provided by another participant regarding the same incident profile. There is substantial feedback to the categorization stage from the attack-tree analysis because it allows us to place incidents in context of goals within a threat scenario.

3.3.2 Threat and Defense Analysis Stages

The *threat analysis* is performed by applying standard attack trees, whereas the *defense analysis* portion is achieved by using a defense structure. Both stages are integrated into the same schematic representation in an *attack-defense tree* [67]. **Figure 12** presents a tree of an ***incident profile*** with two structures.

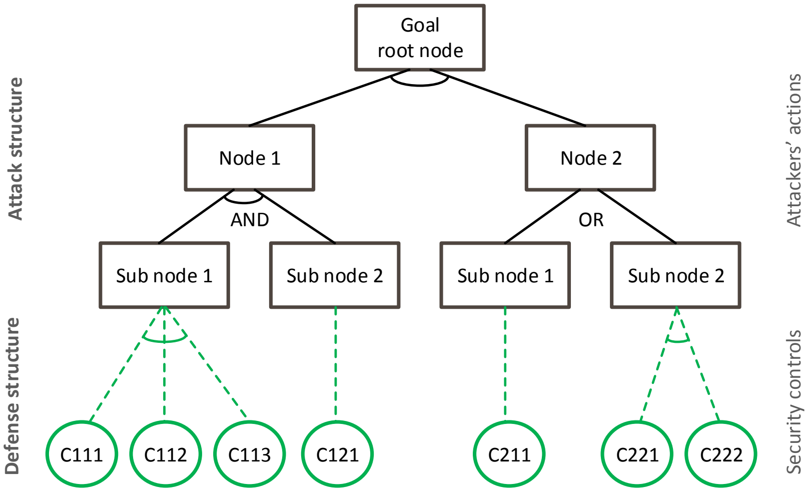


Figure 12: Attack-defense tree for an incident profile

[60] Computer and network incident taxonomy was introduced in John Howard's CMU PhD Thesis and further developed at SANDIA Laboratories.

The *attack structure* is composed of actions (nodes represented by rectangles) and relationships, which are comprised of links and logical operations (AND & OR) that define paths to achieving stepping stones (e.g., Node1) and the ultimate goal. The logical operator AND indicates that two paths are complementary to achieve a goal or sub goal. **Figure 12** represents this relationship through an arc linking two paths to a node (see Node 1). The logical operator OR specifies that two paths are mutually exclusive. **Figure 12** implicitly conveys that situation without any connection between paths as seen in Node 2 [74].

The *defense structure* is comprised of high-level countermeasures acting against adversarial actions. Countermeasures are *standard security controls* (security principles or security objective controls) needed to interrupt paths or make them more expensive for an attacker. ISO 27002:2013[61] is our primary source for countermeasures because of (1) its acceptability in the international spectrum and the industry, and (2) its scope, which spans aspects of risk in information/computer security beyond cybersecurity.[62] When specific security countermeasures are not found in ISO 27002, we also considered security controls from CSC[63] and PCI[64] (see appendix J). For example, controls for card skimming are found in PCI but not in ISO 27002.

It is important to note that attack trees are used for analyzing incidents in class C1, which have been planned by smart adversaries. For incidents in classes C2 and C3 we use best practices to identify countermeasures. A type-tree analysis of incidents in classes C2 and C3 is out of the scope of this paper.

3.3.3 Gap Analysis Stage

The *gap analysis stage* was conducted in two steps: mapping of controls and estimation of gaps. First, we mapped the standard security countermeasures—identified for each incident profile—with regulatory requirements. These countermeasures were summarized as *compound keywords* that convey a main security goal. For example, restriction of traffic between networks to prevent unauthorized access is conveyed by *segregation of networks.* Then, we used these compound keywords as codes to annotate the regulation JB-834 by identifying statements referring to such security objective controls, security controls, or guidelines associated with the countermeasures. Second, the gap was quantified by counting the number of mutually exclusive countermeasures in the protection tree that are not considered by the regulation.

Framing trees. Attack-defense trees have been represented with two major frames. **Table 9** contains the same tree as in **Figure 12**. The left frame contains the attack structure, whereas the right frame depicts the defense structure. This format allowed us to record countermeasures in a structured way and compute gaps for every incident profile.

[61] International Organization for Standardization (ISO), Information Technology – Security Techniques – Code of Practice for Information Security Management

[62] Although cybersecurity and information security cover similar areas, they are not equivalent [113].

[63] CSC: Critical Security Controls from CSI - Center for Internet Security

[64] PCI: Payment Card Industry

Table 9: Attack-defense table for an incident profile

	Attack tree	**Security controls**		
Goal	Node 1 **AND**			
	Sub-node 1 **AND**	C111	C112	C113
	Sub-node 2	C121		
	Node 2			
	Sub-node 1	C211		
	Sub-node 2	C221	C222	

Security requirements. Security controls, such as ISO 27002 controls, are generally composed of *security requirements* (atomic countermeasures), which we actually mapped to regulatory requirements in JB-834. We included only the security requirements needed to mitigate the threat in a sub-node of a tree. An ISO control may have more security requirements than needed for our purpose. **Table 10** illustrates decomposition of the three controls of Sub-node 1 allocated in Node 1.

Table 10: Decomposing security controls

Security control	**Security requirements**		
C111	R_1	R_2	R_3
C112	R_1	R_2	
C113	R_1	R_2	

C111 is a security control in Node 1, Sub-node 1, and with sequence number 1.

Coverage index CI. We introduce the *coverage index (CI),* which represents the degree to which the regulatory requirements address the standard security controls needed to mitigate the threat represented by an ***incident profile***. This index indicates a percentage of security controls covered and is computed in two steps. First, we calculate the coverage for a single standard **security control** (*single coverage index S*) as follows:

$$S = \frac{R_1 + R_2 + R_3 + \cdots R_m}{m} = \frac{1}{m} * \sum_{j=1}^{m} R_j$$

$Where$:
S: $single\ coverage\ index\ for\ a\ security\ control$
R_j: $security\ requirement\ of\ a\ control, which\ are\ fullfiled\ or\ not\ by$
$regulatory\ requirements.\ R_j\ take\ binary\ values\ (0{:}\ absence;\ or\ 1{:}\ fulfillment)$
m: $number\ of\ security\ requirements\ in\ a\ security\ control$

Second, in order to find the total coverage of the security controls for a particular *security* ***incident profile***, we obtain the average of the *single coverage indices* of all controls in the corresponding defense tree.

$$Coverage\ Index\ (CI) = \frac{1}{n} * \sum_{i=1}^{n} S_i$$

$$Gap = 1 - CI$$

$Where$:
CI: $Coverage\ Index\ of\ security\ controls\ for\ an\ incident\ profile$

n: $total\ number\ of\ security\ controls\ in\ the\ defense\ tree$
S_i: $single\ coverage\ index\ for\ a\ security\ control$

Since our ultimate goal is finding the gap between the security controls (needed to manage the threat in an incident profile) and the regulatory requirements, we subtract CI from 1. The CI for every *security incident profile* is reported in Appendix I.

Relative threat exposure. We developed a qualitative estimation of threat exposure for an incident profile due to contributory factors under regulatory jurisdiction. The estimation of the threat exposure uses the measure of the gap as shown in **Table 11**. The rationale is that the larger the number of security controls that are absent (large gap), the greater the surface exposure to an attack that can be expected. This estimation is a way to qualitatively summarize areas of exposure that can be used by decision makers.

Table 11: Threat exposure for an incident profile

CI range	Threat exposure
0 < Gap <1/3	Low
1/3 < Gap < 2/3	Medium
2/3 > Gap < 1	High

We assume perfect enforcement of the regulation under analysis. Also, it is important to mention that success of an attack clearly depends on the ability of the attacker. A very advanced adversary (with highly sophisticated capabilities and virtually infinite resources) would likely surpass many security controls of the defense tree.

3.4 Threat, Defense, and Gap Analysis

This section analyzes 32 security *incident profiles* and conducts the corresponding gap analysis for each incident category. To begin, we identified eight *categories,* six of which are driven by smart adversaries. The seventh category is *user error*, which is composed of non-malicious actions (involuntary errors and conscious actions) that result in security incidents. The eighth category (*others*) spans incident profiles that do not fall in any of the previous seven categories. **Table 12** lists all incident categories with their associated number of incident profiles identified.

Table 12: Incident categories

ID	Incident category	N*
A	Unauthorized **a**ccess	3
L	Information **l**eakage	4
M	**M**alware infection	4
P	**P**hishing and pharming	4
S	Card **s**kimming	2
F	**F**raud	5
U	**U**ser error	4
O	**O**thers	6
* Number of incident profiles		32

3.4.1 Unauthorized Access (Category A)

In this category respondents reported three *incident profiles*, some of which are the starting points (stepping stones) of many incident profiles across other categories.

A1—Unauthorized physical access. This incident profile enables incidents such as card skimming and information leakage. Examples include criminals breaking into ATM lobbies to conduct ATM sabotage and into institutions' facilities to steal portable computers.

A2—Unauthorized software application access. This profile is a steeping stone that further leads to information leakage and (external and internal) fraud. Incidents described in this profile were conducted by insiders who already had credentials to access financial software applications and outsiders who had stolen authenticators.

A3—Unauthorized network access. In this case insiders and outsiders connect (personal) computer devices to internal corporate networks.

Gap analysis of category A. The major gap in the unauthorized access category lies in network access (profile A3), where controls for wireless devices (Wi-Fi and Bluetooth) and Ethernet connections are not addressed, whereas A1 and A2 perform relatively well. Physical security (A1) could improve in terms of preventing insiders' presence in organizations (e.g. screening), and also with respect to physical security provision by third parties. Regarding application or system access (A2), policies for customers' interaction with financial applications are thoroughly addressed; nevertheless, there are some control absences, such as *review of user access rights* and *access to public services*. Controls for *segregation of duties* are comprehensively addressed by the regulation in several areas.

Table 13 presents the *coverage index* for each incident profile and ***control calls***, which is the number of controls required by a particular incident profile. A security control can be counted more than once since it can be required in several sub-nodes of an incident profile. Profile A2 has the highest number of *control calls* of all profiles, which reflects the multiple (reported) ways an attacker targeted an information system.

Table 13: Coverage index for unauthorized access—Category A

ID	Security incident profile	Coverage index	Control calls
A1	Unauthorized physical access	0.77	13
A2	Unauthorized information system access	0.80	51
A3	Unauthorized network access	0.50	9

3.4.2 Information Leakage (Category L)

Although several respondents reported uncertainty about attack vectors used by insiders/outsiders to leak institutional data, some respondents reported incidents allocated within four incident profiles. From the perspective of financial institutions, data leakage, which is a subset of what attackers need to do to achieve their goals, generally occurs in three steps: (1) get access, (2) copy/get data, and (3) ex-filtrate data. Step one is part of an *unauthorized access category*, while the data flow toward outside of the institutions' control occurs in steps two and three. The next profile illustrates these steps.

L1—Information leakage by reusing credentials. By using their access credentials, insiders are the main actors detected leaking data. The most harmful incident was conducted by an employee who had both a high level of authority and privileged access to financial information. By running SQL queries into a financial database, this actor copied and leaked sensitive information right before leaving his position at a financial institution. In addition, users with regular access leaked customers' financial data, which subsequently were delivered to other competing financial institutions. Financial customers have exposed evidence of this incident. Both cases follow the pattern showed by **Figure 13**.

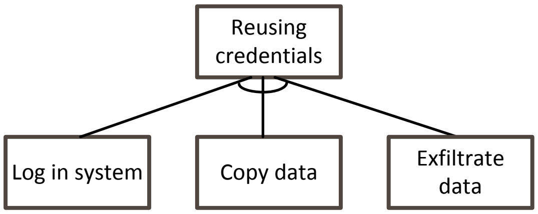


Figure 13: Node re-using credentials

In the worst-case scenario, *logging into a system* cannot be prevented because insiders already have access in order to conduct their operational activities. If insiders want to get in, they will. Countermeasures to minimize the impact and multiple occurrence of this incident can be taken (to minimize the likelihood of such incidents occurring) before employment (e.g., screening) and during employment (e.g., activity monitoring and deterrence through a disciplinary process).

L2—Information leakage by stealing a data container. Data are leaked when an outsider breaks into an institution' facilities to steal portable computers containing confidential information. In one case, an insider' collaboration was suspected because a laptop specifically containing sensitive data was targeted in the bank's facilities. Outside of institutions, data leakage occurs when portable computers are stolen or lost. Other sources of data leakage are USB thumb drivers and mobile devices.

L3—Information leakage by deceiving users (social engineering). Outsiders use *e-mail* and *phone calls* to deceive financial employees and gain financial information about customers. Also, criminals cause malfunctions in ATMs (see card skimming) and then approach customers *in-person* to pretend as if they were providing assistance, but their real intention is to learn customers' personal identification numbers (PINs). Authorities also reported that people familiar with victims (e.g., relatives) have obtained customers' ATM PINs to later conduct fraud. The latter incident is clearly outside of the institutions' domain.

L4—Information leakage by visual access (authenticators). In this case, outsiders without any interaction with customers can learn authentication data (PINs) by simply looking at them when customers are conducting transactions in ATM machines. More advanced techniques use electronic devices to record customers entering their PIN (see profile S2).

Gap analysis of category L. JB-834 does not have many specific controls to deal with data leakage, but it has general requirements such as:

> *"JB 22.10 Protect information in documents, external devices against breach…"*

This regulatory requirement can imply several technical controls, such as blocking and monitoring thumb drivers. Among strong controls to protect data are: encryption, awareness, and education. In contrast, this category lacks *information classification* at the general level. More particularly, L1 lacks *segregation of networks*, while L2 and L4 lack physical security controls. Lastly, controls for *external public services* are absent in L3.

Table 14: Coverage index for information leakage

ID	Security incident profile	Coverage index	Control calls
L1	Information leakage by reusing credentials	0.93	25
L2	Information leakage by stealing a data container	0.91	35
L3	Information leakage by deceiving users	0.83	22
L4	Information leakage by visual access	0.70	20

3.4.3 Malware Infection (Category M)

Four incident profiles describe the paths used by malware to infect IT financial infrastructure.

M1—Infection through removable devices. Computer users employ removable devices to transport (corporate and personal) information inside and outside of the organization. Although USB thumb drivers are more often used, removable devices also include external hard disks, media players, and more. Such devices often get infected when connecting them to external computers (e.g., homes, universities, office of third parties), and the infection subsequently propagates into corporate networks. Outsiders try to recruit employees to transfer malware into an institution's corporate networks (e.g., connecting USB flash drivers into a computer) [R13]. Similar reasoning applies to any other type of removable media (e.g., DVD drivers).

M2—Infection through e-mail attachments. Malware can also infect computers by direct delivery of a payload as an e-mail attachment. Corporate users occasionally receive electronic messaging with infected files embedded in valid messages such as documents. This profile was not reported very often.

M3—Infection through compromised websites. Corporate users also receive messaging with URLs pointing to malicious websites. Unaware (or careless) users click the URLs. Similarly, users browse malicious websites, click on compromised URLs with mobile code or download software to install in their computers [R33]. Although it was not reported, instant messaging uses a similar attack vector. This technique is also used to target financial customers to conduct phishing (see Category P).

M4—Infection by connecting computer systems to the corporate network. Similar to what happens with USB thumb drivers, corporate users working with portable computer systems (e.g., corporate or personal laptops) occasionally get infected outside financial institutions. When users return to the organization, malware is transmitted into the corporate network through conventional connectivity channels, such as Ethernet or Wi-Fi (IEEE 812.11). While it was reported that antivirus tools usually detected malware, such tools obviously would not report undetected malware that manage to pass through. While this profile clearly includes mobile devices, a computer system can be of any type (e.g., desktops, servers, smart-phones). An additional vector of malware infection that was not reported is *instant messaging*, which could become a potential incident profile M5.

There are some special assets targeted by the attack vectors described above:

- **Malware infection of ATM machines.** In one reported case, criminals targeted ATMs by using malware to dispense cash [R13]. It was not known how the malware was planted in the ATM. Possible routes of attacks are profiles M1 and M4, where participation of insiders, such as employees and third parties (e.g., ATMS maintenance technicians) should not be discarded. Currently, ATM machines use Windows XP as an operating system, which does not have security patches supported from Microsoft beyond April 2014.[65] This leaves unprotected ATMs vulnerable to infection and exploitation.
- **Malware infection of corporate customers' computers.** Financial institutions offer corporate users advanced financial services (e.g., employees salary payments) for which authentication credentials are provided (users and passwords). Cyber criminals have targeted these credentials by installing *keystroke loggers*. With the captured information, they later conduct unauthorized transactions to divert funds from banking corporate accounts to compromised personal accounts. While at least one institution used user and password as credentials, others use more advanced authentication techniques, OTP (One Time Password). Detection occurs when customers complain about fraud [R30].
- **Malware infection of personal customers' computers.** See pharming (P4).

Gap analysis of category M. For several malware profiles, the controls *segregation of networks* and *periodic malware scans* are absent. Regular reviews are focused only in e-banking systems. In addition, profile M1 lacks controls for malware propagating through removable devices, policies for mobile devices (although external devices are mentioned), and minimizing administrative privileges (control CSC 5.1). M3 lacks controls for external public services (e.g., web filtering). Several of these controls are also absent in profile M4.

Table 15: Coverage index for malware infection

ID	Security incident profile	Coverage index	Control calls
M1	Infection through removable devices	0.63	19
M2	Infection through e-mail attachments	0.80	41
M3	Infection through compromised websites	0.57	12
M4	Connecting a computer system to the corporate network	0.55	16

3.4.4 Phishing and Pharming (Category P)

Phishing and pharming are techniques to maliciously obtain financial credentials. From the defenders' perspective, these attacks can be conducted as a *combination* of several incidents as follows:

P1 Prior to Phishing or Pharming: creating financial spoofed websites
P2 Phishing: social engineering by e-mail + data leakage

[65] https://www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support

P3 Phishing: P1 + social engineering by e-mail + data leakage
P4 Pharming: P1+ *Host file*[66] alteration by malware + data leakage
P5 Pharming: P1 + manual Host file alteration + data leakage
P6 Pharming: DNS server poisoning + data leakage

Respondents reported P1, P2, P3, and P4, which focus on targeting financial customers. They are addressed next.

P1—Generating spoofed financial websites. To begin, cyber-criminals create multiple copies of e-banking (or e-commerce) websites around the globe. Although these events do not directly take place in financial institutions, they qualify as incidents because they are imitating financial institutions' webpages on the Internet. As a previous step, attackers in some cases use web crawlers to copy institutions webpages before implementing spoofed e-banking websites.

P2—Phishing through e-mail to obtain e-banking login credentials. Cyber-criminals sent emails directly asking financial customers for their e-banking login credentials. Unfortunately, there were people who fell into this trap and submitted the data of the second authenticator factor (as a scan copy), which was a piece of plastic containing a matrix with multiple codes necessary to conduct financial transactions online.

P3—Phishing through spoofed websites and e-mail to obtain e-banking login credentials. Cyber-criminals sent standard e-mails with URLs of spoofed websites to customers. These e-mails mainly have three components: (1) they notify the potential victims that something unusual or usual has occurred—typically an update of banking systems; (2) they urgently ask for the potential victims' actions—sometimes even a deadline is provided (e.g., two days); (3) they include terminology appealing to the sense of security in the potential victims. In what follows, we present a list of themes referring to the three components, which were extracted and translated from a sample of 20 real phishing e-mails written in Spanish and referring to different Ecuadorian institutions between 2013 and 2015.

(1) Explaining what supposedly occurred

- *Our technological processes are operational now.*
- *Your account has been temporarily suspended.*
- *A regular maintenance procedure detected you did not confirm your data.*
- *You are not registered in the new security process of the bank.*

(2) Asking for an action

- *We ask for your collaboration to achieve your data restoration rapidly.*
- *Enter our website and verify your information in our database.*
- *Enter the following link. With this action your account will be restored permanently.*
- *Follow the next steps in an easy, fast, and secure way to complete the process through this link.*
- *Verify your data; otherwise, your banking account will be blocked.*

[66] *Hosts file* is computer file that governs the local resolution of domain names in operating systems.

(3) Appealing to the sense of security

- *Never deliver personal data by phone.*
- *This will substantially improve the security and quality of our service.*
- *This will accomplish the encryption with 128 bits the bank requires.*
- *The bank has up-to-date technology to protect and encrypt your data.*

Lately, criminals have also been appealing to customer's desire to avoid visiting the banks' facilities due to the inherent inconvenience involving time and effort.

> *If you don't verify your data, you will need to come to the bank's facilities to unblock your banking account.*

Over time the sophistication of phishing e-mails has grown. They started with lexical errors and with random (e-mails) destinations. For example, in the past, it was usual to see phishing e-mails reaching people from "banks" where they did not have accounts. Since 2015, criminals have sent emails targeting actual customers and including their complete name (first name, second name, last name, and second last name) in the e-mail's body, which suggests that data leakage of personal information (at least bank name and customer full name) may have occurred at some point at an organization storing sensitive information.

Once the customers have received the e-mails, a number of them clicked the malicious URL, and subsequently revealed sensitive data. This next attackers' step has already been described in the profile *information leakage by deceiving users (L2)***.**

P4—Pharming by malware infection. Pharming is a sophisticated variation of phishing, which in this case uses malicious code to redirect legitimate users' browsing requests to malicious websites. Attackers achieved this goal by modifying the local computers' *DNS resolution service* (*hosts file)*. In fact, evidence showed that *Banking Trojans* modified the *Hosts file* residing in computers' operating systems, in this case mainly MS Windows. Subsequently, customers provided their authenticators to the malicious websites, which is the profile *information leakage by deceiving user (L2)*.

Gap analysis of category P. Regulation has comprehensively addressed controls in this category. In practice, however, there are gaps outside of the span of the regulation because they do not lie within the financial domain.

First, because profile P1 takes place overseas, it cannot be effectively prevented, only mitigated to some extent. Some banks hire external services to shut down spoofed websites once they are discovered around the world. While this approach is clearly reactive, it has been helpful to decrease the number of deceived customers.

Second, bad actors initiate attacks outside the financial domain. P2 and P3 use e-mails to launch the attack and reach customers. Attackers can obtain e-mail addresses outside by crawling websites, harvesting e-mail addresses, buying generic e-mail databases, and randomly generating e-mail addresses. More sophisticated attackers employ a clean e-mail database obtained as a result of data leakage, likely from a primary source. In this last case, financial institutions need to protect their data to prevent criminal usage of customer's personal information.

Third, protection against P4 (pharming) requires technical controls that must be installed in customers' computers. This countermeasure clearly falls outside of the regulatory domain, although we found at least one institution providing specially designed Kaspersky anti-malware to their customers to prevent phishing and pharming.[67]

Thus, in our analysis, the regulation has covered all aspects under its competence to protect financial customers. Some minor gaps can be found when *phishing* targets institutions' employees, but respondents did not report such cases, so **Table 16** does not account for that.

Table 16: Coverage index for phishing

ID	Security incident profile	Coverage index	Control calls
P1	Generating spoofed financial websites	1.00	1
P2	Phishing through e-mail	1.00	2
P3	Phishing through spoofed websites and e-mail	1.00	4
P4	Pharming by malware infection	1.00	4

3.4.5 Card Skimming (Category S)

Incident profiles included here are attack vectors that lead to the attackers' ultimate goal, financial benefit, which we describe in profile F3 (fraud in ATMs).

S1—Installing external devices on ATMs. Criminals conducted sabotage of AMT machines. They installed electronic devices (card skimmers) on ATMs' card readers to copy digital information from magnetic strip cards. They also install very small cameras with the purpose of recording customers' interaction with ATMs' keypad (see S2).

S2—Capturing sensitive data on ATMs. This is a special case of data leakage, in which criminals obtain customers' authenticating credentials, including PINs and data contained in magnetic strip cards. Data are captured by using previously installed skimming devices and digital cameras. This data leakage occurs in two steps: (1) the external devices capture sensitive data on ATM machines; and then (2) these devices are taken by the aggressor or the devices wirelessly transmit the data outside of physical perimeters.

Gap analysis of category S. The substantial gap (physical security and ATM protection measures) in this category is explained by the posture of the regulation towards skimming, which does not concentrate on the attack per se but on the vulnerability that motivates the attacker. The risk imposed by card skimming is addressed by requiring implementation of EMV payment technology. Without a magnetic strip in payment cards the incentive of this specific attack vector is eradicated, so the ultimate goal, mitigating fraud, is targeted here.

Nevertheless, at the time of the interviews[68] the risk persisted because of the compatibility required by the local market (institutions transitioning to full EMV compliance) and international markets (e.g., the USA). ATMs still needed to process both

[67] Banco Pichincha fights banking fraud (2015). Retrieved from http://media.kaspersky.com/en/business-security/case-studies/Kaspersky_case_study_Banco_Pichincha.pdf

[68] From 21 July to 12 September 2014

types of systems magnetic-strip cards and EMV-enabled cards during the transition. Thus, the vulnerability persisted although the attack surface for this skimming vector and associated fraud have been dramatically reduced [R3, R11].

Table 17: Coverage index for skimming

ID	Security incident profile	Coverage index	Control calls
S1	Installing external devices on ATMs	0.33	24
S2	Capturing of sensitive data on ATMs	0.27	15

Given the specificity of this case, most security controls belong to *PCI PTS POI.*[69] Particularly, five security objectives and two sub-controls come from these standards. They are supplemented with three ISO 27002 controls and one CSC 6.0 control addressing wireless security. Absent controls include periodic inspections, anti-skimming countermeasures, CCTV monitoring, and wireless intrusion detection.

3.4.6 Fraud (Category F)

This category includes incident profiles that involved monetary losses for financial institutions and customers.

F1—Unauthorized e-banking transaction. After obtaining authentication credentials of customers, criminals log on into online financial systems and conduct unauthorized transactions. Most likely, they transfer funds from the victim’s account to another financial (compromised) account in the same bank or they may transfer the funds to an external account in another local bank. Typically, this incident profile is the one of the last steps of phishing and pharming—although they may not be the only ones.

F2—Cash withdraw from a bank counter. Criminals use this incident as a route to extract illegal funds from a financial institution as a result of other incident profiles—phishing and pharming. Two patterns were identified; one occurs within the institutions’ domain and the other evolves outside. First, *identity theft* allows criminals activate a fraudulent financial account in institutions (see profile O4). This account is subsequently used to transfer and withdraw illicit funds.

Alternatively, criminals choose third parties with whom they establish a business agreement that appears to be legal to justify a transaction. For example, criminals pretend to buy a car from a third party and electronically pay for it. Then, criminals pretend to change their minds and ask the seller for the money (cash) back—after paying a certain amount for the inconvenience.

F3—Unauthorized ATM transaction (Fraud in ATMs). Once criminals have duplicated credit/debit cards, they make transactions in ATMs as if they were actual customers. Transactions are conducted in ATMs physically located in several cities. Detection occurs when customers complain to institutions about fraudulent transactions, or another institution of the ATM-network detect and reports a compromised ATM. In addition, financial institutions also have to deal with false positives, especially when customer’s relatives use their cards and passwords without customers’ knowledge.

F4—Fraud through social engineering. Criminals learn about their targets’ identity and their financial behavior; then they impersonate customers’ identity to

[69] PCI PIN Transaction Security Point of Interaction Security Requirements

maliciously authorize transactions. In particular, special customers able to authorize transactions remotely are targeted. Outsiders break into personal e-mails accounts of these customers to learn about financial activity, passwords, and operate with this e-mail account. Banks usually send confirmation of transactions to customers' e-mails, so personal inboxes can have plenty of sensitive information. Then, criminals impersonate these financial customers. They call and/or e-mail a bank's representative to authorize transactions. Criminals appeal to financial employees' desire to be supportive with customers by showing discontent with the service provided by the bank and urgency for the transaction.

F5—Internal fraud. Insiders have conducted unauthorized transactions to obtain financial benefit. Respondents did not provide details about this incident profile. Some plausible scenarios, which involve two types of insiders reported by CERT/CC, are as follows:

- Insiders—*entitled independent* [17]—may use their credentials to perform unauthorized transactions (most likely).
- Insiders—*insider ambitious leader* [17]—may use their authority to ask somebody else to conduct (part of the) transactions.
- Insiders may conspire with another employee to use their credentials to perform unauthorized transactions.

Gap analysis of category F. In general JB-834 has devoted important attention to mitigating fraud, but there are two attack vectors partially addressed. Both F1 and F2 are fully covered as a result of the regulation's focus on mitigating phishing and card skimming. By contrast, F3 lacks controls to allow effective physical authentication of customers' when opening banking accounts, and one attack vector is outside of the regulatory domain. Profile F4 lacks at least one control against scams targeting employees.

Table 18: Coverage index for fraud

ID	Security incident profile	Coverage index	Control calls
F1	Unauthorized e-banking transaction	1.00	3
F2	Unauthorized ATM transaction	1.00	3
F3	Cash withdraw from a bank counter	0.64	11
F4	Fraud through social engineering	0.75	4
F5	Internal fraud	1.00	3

Until now, most security incidents have had a main actor behind them—an attacker pursuing a goal; nevertheless, several incidents occur due to other triggers. These cases are described in the incident profiles of category U and incident profile O6. We did not use attack trees for such profiles.

3.4.7 User Errors (Category U)

User errors come mostly from unintentional actions or inactions, so there is no a malicious (smart) adversary involved. A respondent considered *no intentional actions* as simply events as opposed to incident [R14]. User errors can occur across several *categories* such as data leakage and malware infection. Incident profiles where user errors take place are: L2, L4, M1, M2, M3, and M4. Such errors lead to unavailability of information systems, and potentially to fraud. Here, we highlight cases that do not fall in the mentioned incident profiles.

U1—Operational error. Financial computer users make mistakes when entering data (typing) in information systems, which cause integrity errors in the information. For example, errors in data entry performed by tellers at counters can make deposits or payments to the incorrect account [R21]. Also, users omit operational procedures to verify customers' identity, which could lead to customers' impersonation [R13].

U2—Password sharing. Users share authentication credentials with another employee for logging into corporate computer information systems. Also, supervisors, without malicious intentions, ask their collaborators to provide their authentication credentials while they are on leave (e.g., vacation time). These sharing behaviors can be motivated by: (1) achieving an operational goal with urgency; (2) valuing convenience over security, especially if obtaining access requires following convoluted or delayed administrative security procedures [R17]; (3) resolving operational tasks when very short temporal employees' absences happen (e.g., a few hours outside of the office); (4) lacking knowledge about such security operational procedures [R11]; and (5) lacking awareness about insider threat and possible consequences, which is highlighted by excessive trust on co-workers [R14]. Overall, this kind of conduct leads to unauthorized access and could potentially lead to fraud.

U3—Inappropriate applications testing. IT engineers have made mistakes when conducting testing in software applications, especially before introducing changes in IT production environments. This type of incidents has caused unavailability of financial applications.

U4—Running scripts in production environments. Users with high administrative privileges run script commands on IT systems working on production environments without following appropriate procedures. In addition, even if these updating processes are authorized, sometimes such instructions contain errors. These incidents have produced information integrity problems.

Gap analysis of category U. The regulation covers most of the controls to mitigate risk due to user errors described in this category. One ISO control absent refers to establishing technical review of applications after changes have been implemented in IT infrastructure.

Table 19: Coverage index for user error

ID	Security incident profile	Coverage index	Control calls
U1	Operational error	1.00	1
U2	Password sharing	1.00	3
U3	Inappropriate applications testing	0.89	3
U4	Running scripts in production environments	1.00	4

3.4.8 Other Profiles (Category O)

Incident profiles that do not fit into previous categories are included here.

O1—Distributed denial of service. Distributed denial of service attacks on e-banking and e-commerce services were reported. Flooding of TCP and UDP packages have been delivered to Internet-facing web servers.

O2—Web defacement. One institution reported alteration of one of its webpages hosted in an Internet-facing web server. This security incident did not occurred recently.

O3—Spam. Internal messaging security controls permanently detect spam reaching financial e-mail gateways.

O4—Customer impersonation. Criminals forged the national Ecuadorian citizenship ID to impersonate citizens and become banks' customers after activating a fraudulent financial account in institutions. Subsequently, criminals impersonate these citizens to conduct financial transactions with such fraudulent accounts (see profile F2).

O5—Exchanging debit/credit cards. Criminals conduct theft when replacing debit/credit cards from customers by using social engineering. They had previously caused malfunctions in an ATM and then pretend to be friendly strangers who want to help customers. In the process, they inadvertently interchange the customers' card with another fake card that looks similar.

O6—Flooding. The rain flooded a financial datacenter, but it did not cause major issues given the actions taken by the institution's personnel to overcome the incident. Since this is a random event, without a smart adversary behind, we did not analyze it with an attack tree. Conducting a deep analysis of this type of incidents is out of the scope of this paper.

Gap analysis of category O. Flooding and malicious exchange of cards are completely addressed, but there is a gap in the rest of the profiles. Although the availability of financial systems is required by regulatory rules, no specific controls are specified to protect IT infrastructure from DDoS attacks. Regarding customer impersonation, controls to improve authentication in person are absent. Lastly, spam is mostly not addressed.

Table 20: Coverage index for other profiles

ID	Security incident profile	Coverage index	Control calls
O1	Distributed denial of service	0.13	4
O2	Website defacement	0.83	21
O3	Spam	0.25	2
O4	Customer impersonation	0.67	3
O5	Exchanging of debit/credit cards	1.00	2
O6	Flooding	1.00	3

3.5 Summary of Results

This section outlines the results by using the *coverage index*, proposes a qualitative measure for summarizing information about the gaps, and provides insights from the utilization of security controls across our analysis.

The global results of the analysis are presented in **Figure 14**. The perimeter of the circle contains a (categorical) nominal scale with labels of the 32 incident profiles under analysis, and the radius of the circle contains a (percentage) numeric scale for the *coverage index*. The eight colored circular sectors represent the security incident categories. In these sectors the gray color indicates a gap, whereas the shaped multicolored areas indicate successful coverage of security controls by the regulation JB-834. The white circular sectors are separating spaces to improve visualization.

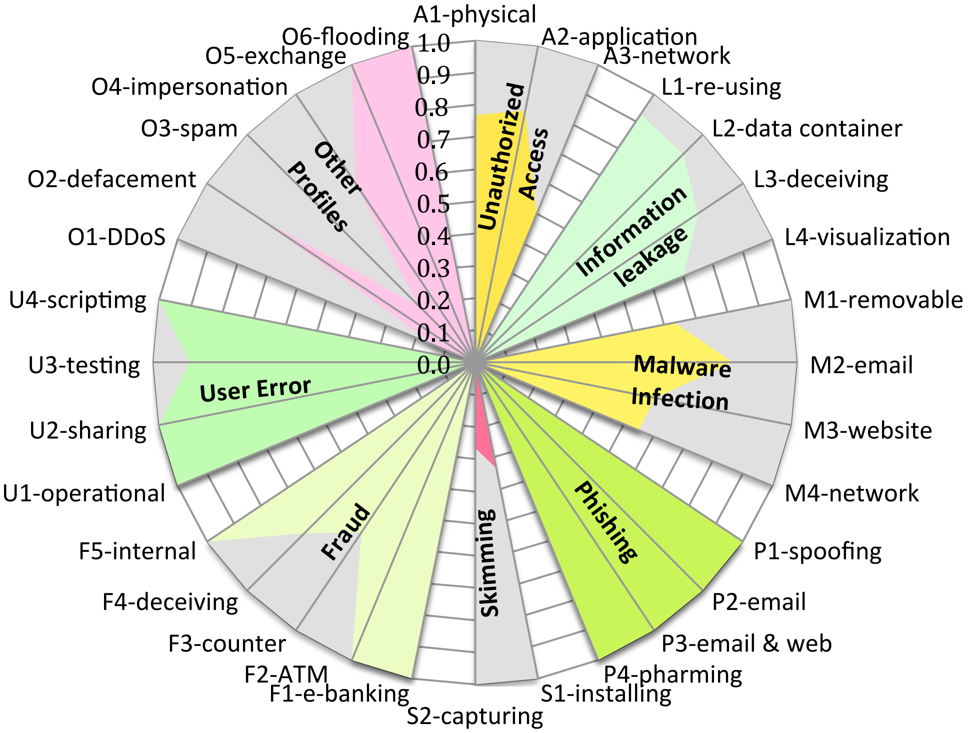


Figure 14: Gap analysis of JB-834 in terms of the coverage index (CI)[70]

Incident profiles *DDoS* and *spam* are not specifically addressed, but they both did not raise concern from most financial stakeholders either. Typically most institutions have security solutions that the regulation does not require (e.g., anti-spam), and DDoS appears not to be a recurrent issue. In the *malware* category, the gap is explained by the absence of network security countermeasures and complementary controls in anti-malware systems. Even though category *skimming* shows gaps (several PCI technical controls are absent), the risk of fraud caused by this attack vector has been addressed. The regulation focuses on the final outcome of skimming attacks (fraud) rather than on the incident profiles leading to it. This gap in skimming also reflects the remaining risk that facing institutions due to the transition from magnetic-strip cards to EMV-enabled cards. Although there are some gaps, the regulation certainly has a strong concentration on mitigating *fraud. Information leakage* is addressed with general regulatory requirements that demand protection, so financial institutions need to identify the specific controls that support this data-protecting goal. This is an advantage for institutions that have freedom to implement countermeasures to the data-leakage risk, but it may introduce subjectivity when assessing compliance because it relies on auditors' criteria to assess the implementation of countermeasures.

[70] See numerical values of CI in Appendix I

The risk involved as a result of the occurrence of all incident profiles has two components. The first component is linked to the contributory factors over which the regulation can exercise control; they are basically the aspects controlled by financial institutions. For example, a factor under such control is implementing stronger authentication systems to reduce fraud triggered by phishing attacks. The second component is due to externalities over which neither regulations nor financial institutions have control, for instance, malware infection of customers' computers, against which financial institutions cannot enforce countermeasures. Unfortunately, this infection is a contributory factor to the occurrence of a security incident.

Total risk = risk managed by policy + out-of-domain risk

In our analytical model these two components (sets of factors) are basically two types of different nodes of a tree. In **Figure 14** we have presented the gap analysis due to contributory factors under control of the regulation, so out-of-the-domain factors still give rise to additional risk in some profiles. For example, pharming has a remaining risk because end-point security in customers' computers is out of the regulation's scope.

We summarize the gap results into a ***relative threat exposure*** measure with the purpose of providing decision makers (industry and regulators) with a measure of effectiveness of the security policy by area of threat (incident profile). This measure is expressed in qualitative terms and derived from the quantitative estimation of the gaps (see section 3.5). This threat exposure has two assumptions: (1) institutions have no implemented controls beyond regulatory requirements, which is unlikely in larger institutions but possible in very small institutions; and (2) institutions have reached full compliance in areas under analysis.

Figure 15 plots data points representing the threat exposure. The external circumference contains a nominal scale with incident profiles. The radius is also a nominal scale with three values: low, medium, and high.

For decision makers in financial institutions one of the interpretations of the gaps is that even after addressing the regulatory requirements, they still need to consider implementing countermeasures for some incident profiles.

All these incident profiles can be considered a major subset of what happens in the real world because it is likely that there may be incidents that stakeholders did not share with us during interviews due to secrecy, which was an organizational posture in some institutions.

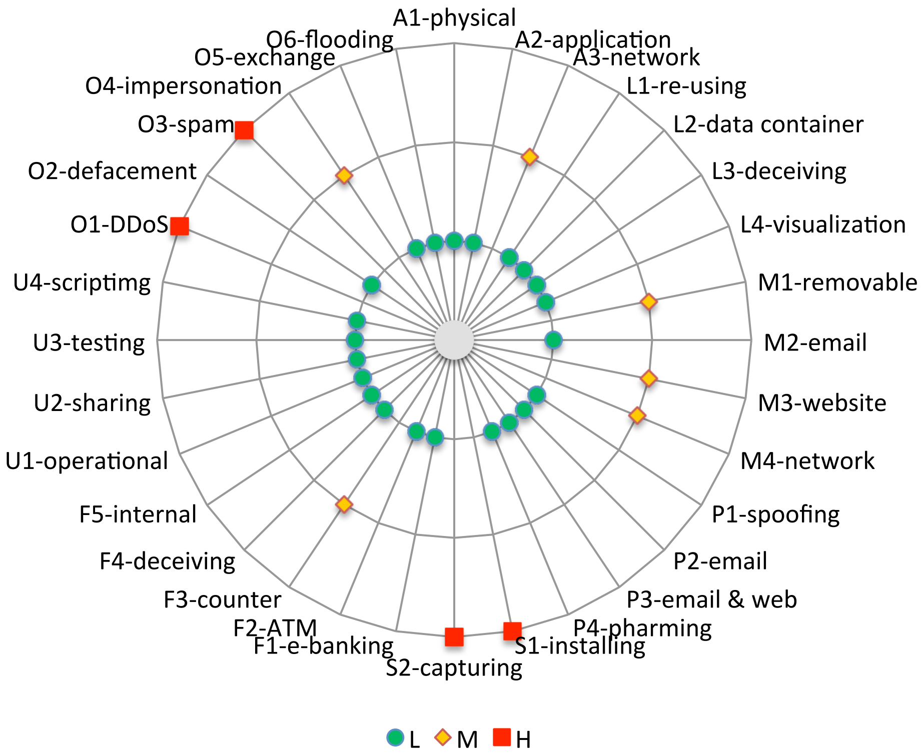


Figure 15: Relative threat exposure

Ultimately, our analysis provides information about the countermeasures involved in the protection goal. Security controls can have several attributes, such as effectiveness to stop incidents, cost of implementation, cost of maintenance, level of inconvenience to operational activities, and more. Here, we present an attribute that we call *frequency of use*, which basically conveys the idea of multiple usage of a control across nodes representing attackers' actions. Using standard security controls allowed us to quantify the frequency with which these controls are required by defense trees across all categories as shown in **Table 21**.

Table 21: Top-ten security controls by frequency of calls across categories

Control ID	Control description	Number of calls
ISO 12.2.1	Controls against malware	38
ISO 7.2.2	Information security awareness, education & training	30
ISO 9.3.1	Use of secret authentication information	15
ISO 13.1.1	Network controls	14
ISO 13.2.1	Information transfer policies and procedures	14
ISO 13.1.2	Security of network services	12
ISO 13.1.3	Segregation in networks	10
ISO 8.3.1	Management of removable media	9
ISO 11.1.2	Physical entry controls	9
ISO 12.4.1	Event logging	9

In the absence of metrics involving monetary estimations, security managers can consider information depicted in **Table 21** to assess the importance of controls when dealing with known incidents and take actions accordingly, for example, prioritizing the monitoring of the performance in those controls.

3.6 Discussion and Conclusion

Although this analysis found gaps in a few areas, the regulation has been reasonably successful at including controls that address the incident profiles reported by financial stakeholders, especially to those incidents whose ramifications have reached the public domain. This performance is due to many security countermeasures incorporated in 2012 and 2014. It is very clear that the Ecuadorian cyber policy has been evolving and has included requirements based on multiple occurrences of security incidents. That is quite evident when observing (the scope and specificity of) security requirements to deal with fraud and associated security profiles such as variations of phishing.

The threat-defense analysis shows that regulatory requirements address most of the nodes on the attack trees. Categories *phishing*, *user error*, and *information leakage* are mostly covered. Incident profiles in category *fraud* are partially covered; while popular incident profiles are effectively considered, two specific cases are somewhat addressed. The substantial gaps are in categories: (1) *others,* which includes profiles DDoS, spam, and customer impersonation (in-person authentication); and (2) *malware infection,* where controls for network security, removable devices, and mobile devices are absent or partially covered. In general, the regulation has devoted a great attention to incident profiles connected somehow with fraud vectors. Information security of processes involving interaction with customers shows to be more relevant than some areas of corporate security (e.g., spam filtering, web filtering), which are left to financial institutions to manage.

The analysis through attack trees shows that *unauthorized access* is part of the foundation of most incident categories (L, M, P, and S). At least one stepping-stone concerning *getting access* is required for attackers to achieve their goals in other incident categories. For this reason, blocking attack vectors in the unauthorized access profile is essential to control negative ramifications in other categories, so financial institutions would benefit from placing strong emphasis on managing risks of unauthorized access.

As expected, this analysis also shows that security countermeasures are not only within the competence of the regulation but outside of its domain, where security measures taken by both customers and society are necessary to control failures in security and cyber-crime respectively. While our analysis concentrates on the regulatory domain, there are incidents where a remaining risk includes actions taken outside of the regulatory jurisdiction.

Regarding security standards, none of them contains all the controls necessary to mitigate nodes representing attackers' or users' actions in attack trees for every single incident profile. As anticipated, whereas ISO has a broad scope, PCI domain is narrower in comparison. CSC controls are technical and direct (mostly cyber), while ISO controls require interpretation for their implementation because they are often expressed in terms of security objectives. Because the regulation uses both languages (technical and managerial), supplementing the standards was suitable. In fact, the regulation contains regulatory requirements that address *security objectives* at several levels of specification. Whereas information leakage is treated with high-level requirements, countermeasures oriented to mitigating phishing are very granular and technical. These controls reach the detail level of *security controls* and *implementation guidelines*.

From the perspective of stopping actions in attack-trees, security controls can be classified in two types. The first type can potentially stop or partially stop incidents from happening, whereas the second type provide information (lessons) so that actions can be taken to prevent future instances of security incidents.

There is some degree of subjectivity in two sections of our analysis: defense analysis and mapping. Selecting countermeasures relies on the judgment of the researcher. One way to partially address this issue was incorporating security standards in our analysis, where specific security controls have been designed to very-well known types of attacks; for example, security controls for physical security in ISO, security controls for ATMs in PCI, and security controls for protecting unauthorized access in CSC. Similarly, mapping security controls to Ecuadorian regulatory statements is challenging because the text and language in both, the standards and the regulation, may not be totally equivalent. We addressed this limitation to some extent by focusing our analysis on security concepts (e.g., segregation of networks) rather than functional words addressing these concepts.

Another limitation is that our method ignores costs of security controls and does not make a distinction of the level of importance of controls among them. A way to supplement the analysis is implementing weights that reflect such importance when calculating a gap. In that case, while the *coverage index* may experience some change, we anticipate that the *relative threat exposure* will likely remain mostly the same.

This paper makes two contributions. We provide a method to assess the effectiveness of a national cybersecurity policy when dealing with security incidents in a critical infrastructure sector. We also present practical results of a gap analysis based on a case study by incorporating (1) objective evidence of security incidents from the real world, and (2) the rationale that has been elicited from groups of subject matter experts in security standards from which we selected security controls to address incidents.

This research informs both policy makers at the societal level and decision makers at financial institutions because the results identify areas of threat that require more attention from them. First, policy makers designing regulations to address cyber-physical security risks can learn how well a policy performs when assessed against real world events it tries to influence. Second, risk managers can learn where to focus their efforts and security investments, and corporate security policies can be adapted to reflect institutional security needs. Financial stakeholders can use our approach and internal data to expand the analysis and cover areas (likely) not reported about internal security. Now, since our approach provides evidence of effectiveness, it can also be useful to influence financial practitioners' behavior. When regulations successfully address security incidents, financial risk managers likely feel motivated to pursue effective and meaningful compliance—beyond just fulfilling typical audit checks.

Future work will consider two directions. Techniques to model *involuntary errors* could be incorporated into the analysis in order to improve the identification of countermeasures for such incidents. In addition, the content of the regulation should be analyzed against emergent threats (global trends) in the financial services, including attacks on EMV (e.g., pre-play attack [75]), POS intrusions, and sophisticated web application attacks.

Developing national cyber security policies that achieve intended goals is challenging. We expect that having a high-level visualization of the potential effectiveness of a cybersecurity policy can assist decision makers in achieving risk-management goals that procure benefit for both financial institutions and the public.

Acknowledgments

I am thankful for the advice of M. Granger Morgan and Douglas Sicker. I also thank the late Howard Lipson for early comments on the study. This research received economic support from the Department of Engineering and Public Policy at Carnegie Mellon University, as well as from faculty-discretionary funds of M. Granger Morgan and Douglas Sicker. The author also received support from the Fulbright-Senescyt Program.

Chapter 4

Challenges in Cybersecurity Education in a Developing Nation: The Ecuadorian Environment

Abstract

Preventing 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. A substantial literature provides strategic guidelines to develop a national cybersecurity workforce. However, relatively little research attention has been devoted to identifying the factors that are responsible for impeding the development of cybersecurity education in developing economies. Based on qualitative data analysis of twenty-eight semi-structured interviews with educational leaders from thirteen Ecuadorian institutions of higher education, this study 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. The level of cybersecurity education is mostly elementary today in Ecuador. Nationwide, interviewees at only four of the thirteen universities studied expressed some confidence about being able to provide students with reasonable preparation. There are no undergraduate academic cybersecurity programs, and only a few graduate initiatives. The challenges that domestic cybersecurity education faces mainly lay in the space of structural capabilities, cybersecurity skills, social integration, economic resources, and governance. To start enhancing current preparation, a national cybersecurity education strategy that bolsters multiple initiatives is urgently needed. Recently, Ecuador has been experiencing major changes in its higher education system that could offer a timely opportunity to advocate for advancing academic cybersecurity competencies.

4.1 Introduction

Numerous reports of cybersecurity attacks have highlighted the prevalence of a wide range of pernicious activity and the growing sophistication of cyber threats, as well as their ramifications for governments, organizations, and individuals across the globe. Frameworks designed to address the cybersecurity challenge at a national level advocate the need to build cybersecurity capabilities to pursue cyber readiness. In these models, developing a cybersecurity workforce is identified as one of the essential prerequisites to developing such capabilities. Confronting cyber challenges requires people with skills to detect and respond to cyber threats, and protect critical infrastructure [76]. Accordingly, nations have designed strategies to build essential human talent, including cybersecurity education, training, and certifications. These strategies are designed to ameliorate current shortages of skilled professionals that even countries with advanced preparation in cybersecurity often face.

Building workforce capacity requires that a nation have the ability to develop strategic and operational structures that may not be readily available in the developing economies context. Hence, understanding the constraints faced by those nations is crucial to identify courses of action to advance cybersecurity. By conducting a qualitative analysis based on the *thematic analysis* of interviews conducted with leaders in higher education, this study explores challenges faced by the higher educational system of Ecuador in the cybersecurity education arena and subsequently examines opportunities for improvement. The results of this investigation are intended to help improve protection of critical infrastructure at the national level.

Ecuador follows the Spanish educational model. The higher educational system is composed of public and *private*[71] institutions, 50% of which are located in two major cities. Over the last six years, 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 [77]. In 2012, fourteen universities were closed down after a second assessment found that these institutions lacked academic quality [78]. Since 2015 universities have been standardizing and updating their academic programs to comply with government requirements. These efforts, however, are not clearly linked to specific cybersecurity strategies, but rather are focused on improving general education. 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 of specialist professors coming from other Latin American countries, such as Chile, and from Spain. This strategy of importing instructional talent continues today.

This paper consists of nine sections: in *section 2* we provide a literature review; *section 3* describes the research method employed; *section 4* presents respondents' perceptions on cybersecurity; *section 5* explains the current situation in cybersecurity education in Ecuador; *section 6* identifies factors driving cybersecurity education in the nation; *section 7* discusses research findings; *section 8* introduces strategies for advancing cybersecurity education; and *section 9* offers some concluding observations.

[71] Private universities often receive partial government support.

4.2 Literature Review

Multiple aspects of cybersecurity education have been addressed as part of national capacity building strategies, workforce development, and education-specific studies. Both issues related to the scarcity of cyber security professionals and strategies for improvement have been comprehensively documented in developed economies by DHS, NIST, NSA, GCHQ, RAND, BAH,[72] SANS, UN, EU, among others. On the other hand, literature 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[73] and strategies to develop cybersecurity education and a workforce. The National Initiative for Cybersecurity Education (NICE)[74] was created to improve the cybersecurity posture of the USA in the long term [79]. NICE addresses awareness, formal education, professional training, and workforce structure. In supporting this initiative, NIST developed the National Cybersecurity Workforce Framework,[75] which provides a common language (lexicon and taxonomy) to be used by academia, industry, and government [80]. This includes seven cybersecurity areas of provision, job functions, and associated skills, which some US universities are using to develop academic programs. Here, RAND (2014) reports that academia has not experienced problems incorporating skilled professors into scholarly activities [81].

Enhancing cybersecurity education and skills is one of the four main components of the national program (2011) to secure cyberspace in the UK [4]. Its cyber policy has incorporated cybersecurity at all levels of education starting at the age of eleven. Current strategies include, supporting schools (e.g., “Girls get coding”), providing resources (e.g., The Open University[76]), apprenticeships, undergraduate and postgraduate research, cybersecurity careers, and internships.[77] In 2013, a self-assessment (including interviews in academia) to identify challenges in implementation of their program found that it could take no more than 20 years to overcome gaps in cyber education [82].

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., SCADA[78]). Public education spans awareness and informative campaigns. Conclusions indicate that: (1) countries at the forefront in cybersecurity[79] incorporate cybersecurity education at every stage of the academic instruction; (2) cybersecurity education has strong ties with military and security agencies—predominantly in the USA; and (3) there is a gap in both domains of education (formal and informal), and some countries have not

[72] Booz-Allen Hamilton

[73] Border Patrol Agent Pay Reform Act of 2013, Cybersecurity Enhancement Act of 2014

[74] http://csrc.nist.gov/nice/

[75] https://niccs.us-cert.gov/training/tc/framework

[76] https://www.futurelearn.com/

[77] https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security, updated May, 2015

[78] Supervisory Control and Data Acquisition

[79] The USA, Canada, the UK, and Australia

even started with their cyber educational development [83]. Harasta (2013) in a comparative analysis between Czech Republic and Lithuania—with a focus on cyber legal issues—reports lack of citizens education regarding cyber threats in both countries [84].

Furthermore, M. Lehto (2015) conducted a survey to assess education and research in cybersecurity at nine institutions (universities and research centers) in Finland. Here, approaches and areas of strength per each institution are presented. Findings show that while cybersecurity education is improving in Finland, the educational system needs cyber strategic objectives. Universities provide education based on particular initiatives, but without envisioning national strategic proficiencies, while efficiency in collaboration and a solid structure to bolster cybersecurity research is in place [85].

In the domain of developing nations, 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 [86]. Muller (2015) suggests areas in which developing countries find challenges to build cyber capacity, which includes institutional stability, building knowledge, legal framework, and private sector cooperation. When adopting strategies from advanced countries, nations should consider their ability (knowledge, capacity) to effect those strategies in time [9]. Cyber education is briefly mentioned as a component of the discussion and as an essential need to secure cyberspace. Moreover, Kortjan and R. Von Solms (2012) identify cyber security educational gaps in the South African national cybersecurity strategy based on a high level comparison with the US and UK initiatives. Suggestions include identifying milestones, allocating resources, and establishing a plan with allocation of responsibilities [7]. R. Von Solms and S. 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 [87]. 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 [88]. Lastly, based on an online survey and Oxford's CCMM,[80] together OAS,[81] IDB[82], and GCSCC[83] (2016) report current efforts of 32 Latin American and Caribbean nations in six dimensions of cybersecurity, one of which is cybersecurity education. Some representative educational initiatives are summarized for each nation. Here, Ecuador reaches mostly the second level (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 [89].

[80] Cybersecurity Capability Maturity Model by GCSCC
[81] Organization of American States
[82] Inter-American Development Bank
[83] Global Cyber Security Capacity Center

Ultimately, at present, most related research concentrates on several aspects of education as a component of cybersecurity capacity building, more comprehensively addressed in 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, work remains to be done to uncover particular issues preventing national cyber capacity building. Hence, this study focuses on a deep understanding of the challenges arising in the environment of a specific developing nation in the context of cybersecurity education.

4.3 Method

A case study allows us to focus our analysis on Ecuadorian universities that provide undergraduate and graduate degrees in computer science (CS) and computer networks (CN). Most operational positions addressing cybersecurity issues in information technology (IT) in the local industry (financial and others) are filled with individuals from these backgrounds. Based on the conceptual framework depicted in **Figure 16**, we prepared interview guide topics to conduct semi-structured interviews. We also conducted desk research to inform strategies for improvement that have been implemented by other countries and could be suitable for the Ecuadorian ecosystem.

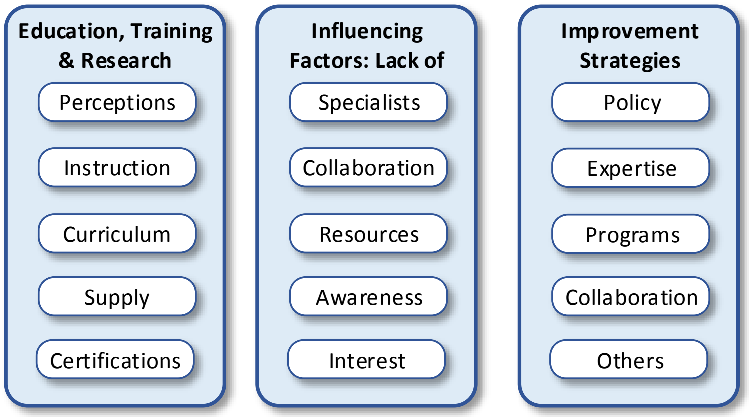


Figure 16: Conceptual framework for cybersecurity education

Accordingly, interviews were supplemented with cross-tabs to explore: (1) perceptions and awareness about cybersecurity in the local ecosystem —the financial sector was selected as a starting point; (2) current practices in cybersecurity education; (3) factors that prevent initiating and improving cybersecurity education in institutions; and (4) potential strategies that the Ecuadorian educational system could pursue.

4.3.1 Data Collection

Throughout one medium-size and the three largest cities in the country, 17 institutions (universities and polytechnic schools)[84] were contacted, 16 agreed to participate, one declined to participate, and 13 actually contributed. In two other cities, although our requests for participation were accepted at first, subsequent communication attempts

[84] In this paper, we use the term 'universities' to describe both.

were ignored. This purposeful sample corresponds to 30.9% of all Ecuadorian universities offering degrees in CS and comprises most representative educational institutions in the nation, including three universities of category A (100%), eight in category B (42%), one in category C (7%), and one in category D (17%).[85] Our analysis mainly focuses on categories A and B 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%) from 16 July to 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 average duration of 62.8 min (std. dev.: 12.6 min, range: 45-93 min). **Table 22** presents respondents' academic background, role, and education.

Table 22: Interview respondents' profile

Background	Respondents %	Role	Respondents %
Computer science	35.7	Director	35.7
Telecommunications	14.3	Professor	35.7
Software engineering	10.7	Coordinator	17.9
Information security	10.7	Dean	7.1
Business administration	10.7	Chief	3.6
Education	7.1		
Business intelligence	3.6	**Education**	**Respondents %**
Informatics	3.6	Master	79
Network connectivity	3.6	PhD	21

Total respondents: 28

Two native Spanish speakers, of whom I was one, transcribed the interviews. We used specialized software, rules of transcriptions, technical and domestic terminology, and timestamps. After transcriptions were finished, they were edited. Steps were taken to keep respondents' participation confidential during recruitment, interview, transcription, and analysis.

4.3.2 Data Analysis

We conducted a standard qualitative text analysis on the data, including text coding (annotating), categorization (themes), interpretation, and reporting. Coding was performed in three stages: (1) coding three interviews on paper to develop our first version of the codebook, (2) performing an inter-coder agreement process on a subset of the interviews, and (3) coding the complete dataset by using qualitative data analysis software (Maxqda).

[85] The Ecuadorian government assessment (2013) has classified (ranked) universities in categories: A (highest), B, C, and D according to quality standards.
http://www.ceaaces.gob.ec/sitio/acreditacion-y-categorizacion-2013/
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. A complete mandatory new assessment has been scheduled for 2018.

The main purpose of conducting an inter-coding agreement analysis, more specifically *consensual coding* [12], 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 [12], in order to be informative about the process we report metrics below. The second coder,[86] 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: (1) creating a first draft of the codebook and an index of the codebook (summary of codes in one page), and training a second coder in both understanding the codebook and coding text; (2) coding interviews to identify disagreements; (3) discussion of disagreements; (4) 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. Next, the results of the study are presented in three interrelated sections.

4.4 Perceptions on Cybersecurity

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

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

Perceptions on cybersecurity of financial services indicate that the sector has been improving security measures lately, but there is need for 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,[87] respondents think 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,

[86] We acknowledge Gabriel Valenzuela's contribution in this section of the study, especially for discussions on the differences when using the codebook.

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

proved to be ineffective in the presence of screen-loggers [90], for customers to login to online banking websites. Areas of improvement were observed in aspects of usability of authentication methods [Respondent R41], 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 leverage situational awareness and, therefore, the posture that universities organizationally, and academics individually, take on addressing security instruction.

4.5 Current Cybersecurity Education

4.5.1 Academic Instruction

Computer science students have traditionally been educated in mixed areas of software engineering and systems engineering. Other 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 considered. Over the last six years, some universities have been progressively incorporating one or two security courses into their programs, but often with some difficulties in practicality. At the time of interviews, universities were updating or re-designing their academic programs because of government compliance requirements. In those updates, participants claimed that security content is being enhanced.

Currently, there are mainly three approaches for teaching security: (1) including one or two formal courses in the entire curricula; (2) teaching security topics in other computer or network courses; and (3) less formal methods, such as seminars and workshops. To begin with, the academic curricula of surveyed academic departments incorporate two security courses (20%), one course (50%) or no courses (30%). **Table 23** depicts the names of the courses offered by 20 different university academic departments where respondents work.

Table 23: 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

*Number of academic departments

Often, security courses are offered during the last semesters. In some cases, a security course is an elective, which produces an unwanted effect because students avoid taking it during the last semester.[88] For this reason, two additional courses have either been only occasionally active (*forensics informatics*) or not active 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 academic courses. This inclusion takes place depending on both the knowledge of professors on the topic and their initiative to address such content in the syllabus, which can drastically change whether a skilled professor leaves the university.

In both approaches, information security content varies among universities and departments. Starting with the most popular, topics mentioned by respondents are presented next. This list collects participants' recalled topics, so it is not an exhaustive enumeration.

- 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

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 much less confident about teaching *incident response.* Occasionally, we observed some overconfidence to address *secure coding*.

The third approach incorporates informal initiatives to promote information security knowledge. Some universities eventually prepare seminars, presentations, and other activities[89] that advocate information security awareness among students by bringing external speakers. This initiative is very well received by students and raises interest in the field. Lastly, some security content is eventually covered in material related to professional certifications.

4.5.2 Professional Certifications

At the time of the interviews, all universities offered some level of support to students for professional training in Cisco networking certifications (CCNA),[90] whereas a few of them have similar support for Microsoft and Oracle products, and less often Linux. Support schemes vary among universities, which include providing content of material 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, while at least in one it is a requirement for

[88] Apparently, students believe this security course may be difficult, so they avoid it.

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

[90] Cisco Certified Network Associate

graduation. Such support from universities has been promoted by labor market demand for certified professionals, availability of instructors, and unpaid access to software. In fact, Microsoft provides educational institutions with educative 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 leading 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 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 they foster learning in professors and students. However, others indicated that such support does not correspond to the role of academia, although it may not hurt having them as supplementary resources.

4.5.3 Research

Although there are particular initiatives, academic cybersecurity research is hardly conducted. Two universities' representatives reported having performed specific research projects in the past (e.g., authentication in a financial application), and another explained 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 a hypothetical scenario: the creation of a CSIRT (with 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 preparation to host this CSIRT, but it was stated that a collaborative initiative with the financial industry would be more viable.

4.5.4 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). Illustrative comments are incorporated here:

> *Very little is taught* [R34, R43]. *There is no a security course* [R40, R49, R57]. *A chapter in another course is taught* [R41]. *We have one 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 it is enough according to the goals and scope of the academic program.

> *Now, it is better; we have had two 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 having two security courses considers it is appropriate, another institution considers security teaching is not solid. Also, while one academic department indicates security teaching is improving, another department at the same university thinks it is not the case, which indicates that some departments (CS, CN, and EE[91]) at the same universities have different levels of 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 organizationally. In summary, 86% of respondents indicated some level of weaknesses in academic security instruction. **Table 24** depicts self-assessment of appropriateness by respondents in Likert scale.

[91] Electronics Engineering, which usually includes computer networks

Table 24: Appropriateness of security education

Likert scale	Respondents %
1 Absolutely inappropriate	0
2 Inappropriate	7
3 Slightly inappropriate	25
4 Neutral	21
5 Slightly appropriate	32
6 Appropriate	14
7 Absolutely appropriate	0

4.5.5 Ongoing Changes

By the time of interviews, as mentioned, all universities had been working to update academic programs because of 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 electronics and telecommunications across the nation have created working networks (e.g., REDSIC,[92] RECIETA[93]). 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 i*tinerary,*[94] which is imparted 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.

4.6 Factors Driving Cybersecurity Education

Cybersecurity education in Ecuador is practiced depending on factors affecting universities' decisions to incorporate security content in CS curricula (e.g., demand) and factors influencing universities' abilities to implement security instruction (e.g., lack of resources). All these factors are addressed next in order of their relevance, highlighted by interviewees.

4.6.1 Lack of Security Specialists

Educators with formal education in cybersecurity are hardly found across the nation. Representatives of twenty 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.

[92] *Red de Sistemas Computacionales*

[93] *Red Nacional de Carreras de Ingeniería en Electrónica, Telecomunicaciones y Afines*

[94] A last-semester course with flexibility to be adapted to specific needs of the curricula

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 quality of security courses is compromised when taught by non-experts since security content is often constrained in scope and integration of theory with practice. Additionally, universities struggle to fulfill demand for cybersecurity. This fact has been evident when: (1) students' requests for advice on undergrad thesis research have exceeded the capacity of universities, given the limited number of qualified advisors [R61]; (2) MS security programs demanded by graduated students have not been feasible [R40]; and (3) government requests for support in cybersecurity have not been fulfilled by a few universities [R55, R59]. The following excerpts illustrate these issues:

> *We do not really have 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].

In order to ameliorate or overcome this professional shortage, several strategies have been adopted. At the undergraduate level, at least three universities have been incorporating professionals holding security certifications from industry as instructors for security courses, especially in the field of security management and auditing. For seminars and talks, two universities reported support from specialists with practical experience coming from the government and two from an academic CERT. At the graduate level, master's cybersecurity programs have been integrating teaching from visiting professors from Spain, Mexico, Chile, and Argentina. Interviewees observed that the industry has followed a similar approach by eventually importing specialists to solve specific needs. Nationally, the government has implemented the *Prometeo Program,* which is an instrument that temporarily brings scientists[95] from around the world to improve general research in the higher education system. Yet, no university in our sample reported having such support in the field of cybersecurity.

4.6.2 Lack of Interaction with Industry

There exists a lack of integration between academia and industry ranging from substantial to minor, which 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 is integrated with academia* [R42].

Additionally, 32% of participants recognized having 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 the industry.

[95] Including Ecuadorians living overseas (return policy)

> *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].

The third group, 7% of respondents, mentioned having achieved agreements with private and public sectors. 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.

> *We have research projects with about five entities, public and private. But, since we have no a security research team, we have been not seen many initiatives in security* [R60]. *We have annual meeting with professionals from industry. We do receive security requests* [R56].

As a result of this lack of communication, opportunities for academia-industrial partnerships and understanding of cybersecurity demand have been undermined. 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.

4.6.3 Insufficient Understanding of Cybersecurity Demand

Comprehensive knowledge about labor market demand for cybersecurity is not available, although there are various 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 the 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 demand for security in the business sector is very low as for today, so they fear that creating security programs for specialists may saturate the labor market rapidly. Others added that more security provision is 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 services in the nation. In addition, from our first study (2014), we found that the financial and telecommunication sectors need 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.

Essentially, 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 [R2, R7]. 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. 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. If needed, the private and public sectors have to make this clear to academia. Otherwise, in several educational institutions cybersecurity will continue to have low priority [R57, R61].

4.6.4 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 influences in their ability to teach security from slightly to moderately.

> *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 pay rates at the same level that the business sector does. On a few occasions, however, a few universities have obtained specialized support—especially for seminars or talks—because some specialists had incentives aside from economic ones that are stronger (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.

4.6.5 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.

Firstly, 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 they have lost their autonomy to make certain decisions. In fact, creation of new undergrad programs requires government authorization, and it could be more difficult to implement them, especially when they are not included in the government framework. At the master's level, participants observe creating a security specialization will be 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].

Barrier to hiring specialists. Over the last few years, university professors have been required to have at least an MS degree in the teaching discipline. Although this policy is generally seen as very positive for improving quality, a couple of universities reported that some industry professionals familiar with security that had been supporting them—before the policy was in place—are not be able to do it anymore. In addition, a policy mandating that professors teaching at universities must hold a PhD degree by 2017 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. [96]

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*.[97] Therefore, modification of current curricula for such programs is not allowed, which prevents incorporation of additional security courses [R50].

Secondly, whether or not the government should actively intervene to advance security teaching in universities is controversial. Supporters (43%) indicated that (1) universities need clear guidelines from the government to establish priorities and (2) 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 (1) there is already too much oversight of the government agencies, and (2) 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*

[96] 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.

[97] Programs not included in the new government framework for higher education.

> *academia. The government may not need specifics about the industry needs* [R48].

Beyond the industry, the fact that the government has widely been advocating usage 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.

4.6.6 Lack of Awareness

Despite the interviewees' argument that institutional awareness exists, a few of them recognized lack of consciousness of the need for addressing cybersecurity education. Before government intervention, two universities reported having academic programs dating from ten years ago, when cybersecurity was not a prominent issue. Nevertheless, they emphasized that this fact has recently been changing. Networking university groups are helpful to raising situational 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 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 extended their views of security awareness into two dimensions. To begin with, suboptimal security practices in the university infrastructure were reported twice to highlight lack of awareness. An interviewee reported cyber attacks to the security academic system that processes students' grades, and another one explained attacks to informational faculty websites. A last interviewee admitted that (unspecified) security incidents have occurred at the university and have been managed with discretion. Furthermore, interviewees observed lack of awareness at the societal level. Although several initiatives have been observed in the financial industry and government, there is the perception that the general population is lacking 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].

4.6.7 Other Factors

Idiosyncrasy. Tendency to take cyber risk was occasionally mentioned, which is consistent with Target (2010) findings regarding attitude toward risk in developing countries [6]. 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 lack of 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 & one private), respondents indicated that they have no ability to replace professors (without formal security education) currently teaching security topics even though there is another professor in place with formal security education. In addition, internal policies require that the university maintain intellectual property on the outcome of research projects conducted by students (e.g., thesis). This rule has been found unacceptable for the 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 hardly 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 exposed above, **Table 25** presents a distribution of the level of influence of factors preventing cybersecurity teaching that we had hypothesized in our study design. Responses are counted in a Likert scale ranging from (1) *not at all influential* to (7) *extremely influential*. Horizontal bars are coded with traffic light colors when counts are greater than six in order to highlight the level of influence. For instance, twelve respondents reported the factor 'student's interest in cybersecurity' as *not influential at all* in the current situation, whereas ten respondents reported 'lack of specialization of professors' as *extremely influential*.

Table 25: Level of influence of factors on preventing cybersecurity education

Factor \ Likert Scale	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**Score***
Lack of specialization of professors		▮	■		■	🟥	🟥	5.7 ■
Lack of feedback from industry	▮	▮		■	🟥	🟥	🟥	5.5 ■
Low availability of professors	■	■	▮	▮	🟥	■	🟥	4.5 ■
Lack of resources		▮	🟩	🟧	🟥	■	■	4.4 ■
Lack of awareness of universities	■	■	▮	🟧	■	🟥	■	4.3 ■
Lack of government intervention	■	▮	▮	🟧	🟥	■	■	4.2 ■
Lack of students' interest in security	🟩	🟩	■	▮	■			2.2 ■

Likert scale: (1) not at all, (2) very low, (3) slightly, (4) neutral, (5) moderate, (6) very, and (7) extremely
Bars in the left frame indicate number of responses, and bars in the right frame represent a calculated score
* Weighted average computed as the number of respondents by the Likert scale respectively

4.7 Discussion of Findings

Recently, it has been suggested that no country is fully prepared to meet the cybersecurity challenge [91]. While some nations with high level of national cybersecurity performance have already started strong workforce and educational programs to foster such preparation, studies suggest that many less developed nations have moved slowly to develop cyber capacity [83, 89]. In this study, we report on the current cybersecurity educational status of Ecuador and specific factors contributing to such condition.

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 of CS and CN, but such integration is informal since, very often, academic instruction depends on instructors' decisions and security skills. In this scenario, 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 as incomplete in scope or depth, especially because of lack of expertise or resources (e.g., labs). Relevant security content for protecting critical infrastructure is being omitted. In fact, pertinent content such as *incident response* was virtually absent. Individual initiatives of universities do not have a common national vision, which is consistent with Lehto's (2015) findings in Finland [85]. Therefore, quality, completeness, and relevance of security content are potentially compromised. At the graduate level, although there were two active MS cybersecurity technical programs (and another one with focus on cyber defense has been announced), they appear to be insufficient.

University priorities, lack of specialists, and lack of understanding of demand prevent academics from advancing cybersecurity graduate preparation. Educating in cybersecurity is not only a matter of having capabilities but also about making decisions to assign higher priority to cybersecurity instruction. 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 born PhD program in CS with information security as one of its research specializations, just a few undergraduate projects, and several undergraduate and graduate theses.

Unsurprisingly, the lack of cybersecurity specialists at universities is one of the biggest issues, which leaves educational institutions with little ability to address cybersecurity instruction. Overcoming this barrier is even harder given strict policies that prevent universities from incorporating industry professionals without graduate degrees, high security professional rates, and, of course, national shortage of skilled cybersecurity professionals. This study also reveals another underlying problem with implications beyond cybersecurity: the lack of communication and collaboration with local industry harms improvement and adaptation of academic programs and initiation of research projects to 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. Geographic triangulation indicates that this issue is much more problematic in larger cities than medium-size or small cities.

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 suggesting low demand, we observe two plausible reasons: (1) some universities do not experience direct demand because the industry often needs to solve specialized problems in a timely manner, so they look for support somewhere else—there is evidence in the financial sector; and (2) the security posture of some sectors in the industry 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.

Other barriers less often reported are the language barrier that impedes access to up-to-date knowledge in cybersecurity, university policies that prevent collaboration, administrative weaknesses, and peoples' attitudes that privilege particular interests over community initiatives [R39].

While this study does not incorporate 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.

Overall, 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.

4.8 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 into these dimensions.

4.8.1 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 strategies (e.g., NICE), cybersecurity capability maturity models (e.g., NICE & CCMM[98]), and sector specific CMMs (e.g., ES-C2M2[99]).

To start, 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 (R&D) 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 can be encouraged [92]. 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 engagement of 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 careers.

Secondary education students should be informed about what CS and cybersecurity careers entail to attract them. Informative campaigns and talks with CS and cybersecurity professionals should be encouraged [85]. Currently, because most students do not have early contact with CS courses in high school, nor an opportunity to hear

[98] The UK Cybersecurity Capability Maturity Model

[99] The US Electricity Subsector Cybersecurity Capability Maturity Model

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 of 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.

Public and private support. Incentives to promote participation in advancing cybersecurity capacity building are needed. Presently, there is a substantial opportunity to improve industry support to the academic environment, including advice and feedback, financial and technical support, and collaborative research projects. Industry commitment to provide qualified answers to surveys would have an important impact on improving understanding about the demand for cybersecurity. A multi-stakeholder space in which government, industry, and academia actively convene to address national cybersecurity educational requirements and strategies is urgently needed.

Institutional policies. Universities need to review and in some cases relax current policies (copy-right rules, 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 considering 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 [93].

CERT support. Computer Emergency Response Teams have been demonstrated to be suitable mechanisms to advance national cybersecurity in different economic contexts and in several *dimensions*.[100] 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* [101] to foster collaboration, and promoting projects that assist colleges and universities [94].

[100] See Appendix N

[101] Group of academic institutions in a US region

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 [95]. 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. This has helped Oman become a leader in cybersecurity readiness in the Arab Region and third worldwide according to the ITU's cybersecurity global index [3]. 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 [R5]. This CERT and the existing academic CERT (CEDIA) 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 could 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*[102] for science and technology represent a challenge in academia, especially because it constrains knowledge transfer for non-native English speaking academics [96]. Although many local academics have English competencies, this 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 [97]. However in the mid-term and long run, there is no substitute for implementing policies that foster English language skills.

4.8.2 Academic Programs

Relevant content must be strengthened in both approaches for formal education in undergrad programs: (1) cybersecurity content integrated across core courses of CS and CN; and (2) 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.

[102] 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 started in a few more major 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, [103] including hiring specialists, because such programs are often self-funded.

> *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].

Now, it is clear that the current lack of specialists is a barrier to exercise the mentioned initiatives, but steps can be taken to ameliorate such deficiency over time. 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: (1) 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 (2) 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. It should be noticed that the current global shortage of cybersecurity professionals [98] 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.

[103] Exceptions are universities that cannot create graduate programs because of its categorization level.

Cross-border education[104] is recognized as an important instrument to achieve higher maturity levels of tertiary domestic education [99], and can be advantageous in the domain of cybersecurity as well. However, when importing academic curricula, care should be taken to adjust designs to the domestic context. Some interview respondents reported that they started following ACM[105] as their reference to incorporate cybersecurity content into CS curricula. 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 [100]. A comprehensive approach requires incorporating expertise from several sectors of society [101]. 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 to teach is important but also how to deliver academic instruction [100]. 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 [92]. In addition, the core principles that allow comprehension of systems vulnerabilities [102] could be supplemented with adversarial thinking to bolster preparation to deal with emergent threats, as opposed to only known types of attacks [100]. 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.

4.8.3 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]

[104] "Students, educators, programs, and academic materials cross national boundaries," OEDC & World Bank, 2006.

[105] Association for Computing Machinery

- Expanding security competitions

Outside of academia, training is also needed to advance the state of the practice in industry, government, and law enforcement. Lastly, because of concerns about the quality of commercial training [R39], controls that guarantee appropriate levels of excellence should be considered.

4.8.4 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 [92] 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 [92].

4.8.5 Research and Development

We find this dimension to present the greatest challenge because quality research in cybersecurity must build upon existing capabilities and structure, including experienced investigators, funding, research centers, and feasible projects. Efforts need to be devoted to 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.

4.8.6 Cybersecurity Awareness and Public Education

The need for addressing social awareness at the national level was raised by interviewees and has certainly been highlighted by OAS and IDB [89]. 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. Many suggest that audience must include children, adults, and the elderly [103]; 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 protection avenues (e.g., patches & passwords good practices). Depending on the audience, means to deliver education already being used in developing countries include school curricula, radio (in Cameroon), TV, and web resources. In this area, based on best practices of developed countries, Kortjan and Von Solms present a framework that provides strategic insights to address cybersecurity awareness and education for South Africa [104]. While such insights are very valuable and many may be applicable to a developing context, its entire replication must take into account availability of national capabilities.

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 [105].

Of course, awareness alone will not solve the problem of insecurity because: (1) ICT users will fail to accomplish what is expected from them in their roles anyway [29]; and (2) 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 N we summarize relevant practices of other countries highlighted by the literature.

4.9 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. In this respect, there are remarkable differences when comparing this nation 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 paper begins to fill this gap by collecting the views of educators in several geographic areas across a developing country—Ecuador. In doing so, this study explains why lack of cybersecurity professionals has been observed in the local labor market as cited by stakeholders in the financial industry, and identifies where opportunities for improvement appear to be. In that regard, this study is one of the very few presenting evidence about factors driving cybersecurity education in a developing nation.

This study intends to inform public policy to improve critical infrastructure protection in the nation. Understanding barriers in detail is a first step to developing beneficial courses of action. In 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. More urgent initiatives are in the dimensions of governance, academic programs, training, and awareness. 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.

Further research is needed to assess which strategies are most suitable for developing nations. 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.

Acknowledgments

I am thankful for the advice of M. Granger Morgan and Douglas Sicker. This research received economic support from the Department of Engineering and Public Policy at Carnegie Mellon University, as well as from faculty-discretionary funds of M. Granger Morgan and Douglas Sicker. The author also received support from the Fulbright-Senescyt Program.

Chapter 5

Conclusion

Cyber attacks on financial infrastructure can cause disruption and significant losses for society. This fact is applicable for any country heavily using ICT as a pillar for financial operations. In this thesis, I focused on exploring the challenges that financial services confront when dealing with cybersecurity incidents in a developing nation, as well as exploring opportunities to enhance cybersecurity capabilities, one of which is developing academic cybersecurity instruction.

5.1 Findings

Chapter two explores cybersecurity incidents arising in the Ecuadorian financial sector; investigates the ability of the Ecuadorian financial sector to deal with those incidents; and evaluates how two strategies supporting cybersecurity capabilities would work.

Financial institutions confront both incidents due to actions of bad actors and errors introduced by humans involved in IT operations. *Phishing* focused on the major banks in the country and *card skimming* targeted almost all institutions having ATMs in our sample. Implementation of EMV has been effective in reducing fraud but has not completely eliminated it because of compatibility requirements of magnetic-enabled cards. Malware attacks on ATMs are a harmful attack vector. Although we report four incident profiles related to information leakage, there is uncertainty among several stakeholders about which attack vectors were actually employed by attackers. In addition, user error is ubiquitous among financial institutions, inside (collaborators) and outside (customers) of institution's borders.

By considering institutional boundaries, barriers to respond to security incidents lay in two dimensions. Internally, barriers include security team size, lack of visibility, inadequate internal coordination, technology updating, lack of training, and lack of awareness. Externally, lack of legal response to the aggressor (weak legal framework) was a major limitation; others barriers are lack of support from ISPs and lack of collaboration. In particular, lack of skilled personnel and lack of awareness lay in both dimensions. When comparing barriers between the USA and Ecuador, major differences are legal framework, inadequate internal coordination, lack of awareness, and lack of training, which are not cited as main barriers in the literature for the USA [14]. In terms of threat sophistication, reported incidents in Ecuador confirm that, in comparison, adversaries with higher skill-levels have targeted the financial services in the USA.

Starting a financial CSIRT to support this critical sector will face challenges associated with location, funding, authority, and availability of skilled professionals. Most financial stakeholders and academics agree with the financial sector as the best place to establish a financial CSIRT. Evidence suggests that the Ecuadorian *National Financial Hub* can take advantage of existing financial-collaborative work in terms of ATMs operations across the country and could expand this effort to additional areas of cybersecurity. Also, funding can consider applying the current economic model managed by the Financial Hub to operate ATMs. As for the CSIRT authority, while many respondents suggest *no-authority* as a desired model, further discussion incorporating additional institutions is necessary to deliberate the benefits of *shared authority*. Establishing a financial CSIRT would face the challenge to incorporate trained professionals in incident response. These professionals would likely have to be trained by requiring international specialized support.

Information sharing could mainly be driven by the type of information involved, the current practice of secrecy in several institutions, trust, and effectiveness of this sharing initiative. Financial stakeholders most likely share technical information as opposed to quantitative losses resulting from incidents. Several institutions would likely be reluctant to share information involving internal fraud, or very sensitive information, or information containing intellectual property. Ultimately, the benefit of information sharing would be evaluated with metrics indicating fraud reduction.

The application of two approaches to elicit information about incidents (spontaneous and guided) shows an important difference (see section 2.4.1). Many financial stakeholders revealed (to a certain extent) restricted information about security incidents when they were asked to spontaneously talk about the type of incidents they confront. However, additional types of incidents or complementary details of an incident are revealed when they are specifically asked about a particular type of incident.

Another finding is that financial institutions of different sizes closely follow what the biggest banks in the country pursue in terms of cybersecurity practices. This behavior happens, for example, when selecting security technology for implementation. Evidence also shows that if major financial institutions started collective cybersecurity initiatives, such as a CSIRT or an ISAP, other institutions would feel strongly motivated to participate in such initiatives.

Chapter three assesses the effectiveness of the cyber policy governing the risk imposed by reported cybersecurity incidents and identifies opportunities for improvement with respect to incidents reported.

Despite the existing gaps in a few areas, the cyber regulation has covered most controls that address the incident profiles reported by financial stakeholders. Many controls associated to incident profiles have been incorporated during the last two updates (2012 and 2014). Important gaps lay in the areas of network security (unauthorized network access, connecting computers to corporate networks, and infection through malicious websites), physical security (installing unauthorized devices on ATMs), information leakage (capturing sensitive data on ATMs), fraud by physically impersonating customers; and security incidents related to spam and distributed denial of service (DDoS). Although spam and DDoS reported the largest gap in terms of number of absent countermeasures, spam is very likely addressed by financial institutions, and DDoS was not reported as a chronic problem at the time of interviews.

The content of the regulation addresses controls with a disparate specificity and scope across incident profiles. This policy is very prescriptive for certain types of incidents (e.g., phishing) but flexible for others (e.g., information leakage). In the former case, security controls are very specific, which occasionally includes particular types of security technology; this approach could make the cyber policy become outdated over time. In the latter case, implementation of controls requires interpretation. In addition, some security controls occasionally only focus on specific types of systems—those reporting most incidents (e.g., e-banking) but ignore others systems. Finally, there is a strong emphasis in security controls mitigating risk of fraud. Overall, policy makers may have intended this level of specificity and concentration because of prioritization of risk areas and complexity of addressing certain types of security incidents.

The analytical method, which is based on standard threat modeling, used in this chapter provides additional insights when analyzing attack and defense in the context of security incidents. The analysis through attack trees shows that *unauthorized access* plays the role of a stepping-stone in four other categories of incidents involving a smart adversary. This attack tree analysis also provided a visualization of threat scenarios that incorporated multiple incident profiles in a unique representation. This visualization and analysis allowed us to classify security incidents and define incident profiles. Also, the analytical method was capable of reveling the frequency of usage of security controls, which is an important insight when making managerial decisions about implementing, operating, and maintaining these security controls. Lastly, none of the security references we consider (standards and best practices) covered all the incident profiles we analyzed, so supplementing multiple references is essential.

Chapter four explores the challenges that the higher education faces to develop cybersecurity skills that support the critical infrastructure protection and provides policy options to advance cybersecurity education and cybersecurity capacity building.

In the academia, the field of cybersecurity is perceived as an emergent issue for which a substantial preparation is needed. Most respondents believe that the security practices in the financial services have improved lately, but there were those who pointed out the need for improvement in some areas, including usability of authentication methods, internal security practices, propagating advanced authentication methods among smaller institutions, and willingness to pay for security.

Cybersecurity education is at the initial stage in Ecuador. Nationally, respondents at only four out of thirteen universities feel some confidence about having made reasonable preparations. Furthermore, no undergraduate academic cybersecurity programs exist and there are just a few graduate initiatives. Including security content in computer science (CS) and computer networks (CN) curricula depends on both the availability of *knowledgeable professors* in the field of cybersecurity and their initiative to address such content in the syllabus. Most academic activity related to cybersecurity has traditionally been addressed in undergraduate and graduate thesis.

The three major barriers that impede advancing cybersecurity education in Ecuador are (1) lack of cybersecurity specialists at universities, (2) lack of communication with the local industry, and (3) lack of understanding of cybersecurity demand. As expected, many universities do not have specialists that allow them to incorporate security courses in their curricula. There is a shortage of cybersecurity experts in the market as it happens in the developed world. Also, lack of communication with the industry in cybersecurity matters prevent collaboration and funding of potential projects. Some university policies regarding intellectual property of students' research (thesis) also prevent collaboration. Additional barriers include lack of resources, and lack of awareness. Government intervention has resulted in both outcomes, barriers for several cases (e.g., hiring specialists, dropout rate) and support for other specific cases (e.g., providing speakers for talks).

While universities with the most advanced preparation have developed strategies to address aspects of cybersecurity (e.g., MS programs, research initiatives), substantial efforts to strengthen cybersecurity education need to be pursued nationwide.

In order to improve the current cybersecurity educational situation, we have framed policy options and insights in six dimensions: (1) *cyber national policy and strategies* that provide planning and guidance to prioritize areas of cybersecurity knowledge and roles required for CIP[106]; (2) *academic programs* that better respond to societal needs; (3) *cybersecurity training* that provides human talent needed to establish and improve cybersecurity instruction in universities; (4) *cybersecurity certifications* that supplement academic preparation with professional instruction; (5) *research and development,* which seems the more challenging area to address given the lack of experts in cybersecurity; and (6) *cybersecurity awareness and public education* that extend instruction to the Ecuadorian population.

5.2 Contributions

While there is considerable literature providing strategic guidelines to inform trends about cybersecurity incidents, and address cybersecurity education, there has been little research in regard to actually identifying the factors that influence the ability of (1) a critical infrastructure sector of developing nations in responding to those incidents, and (2) the ability of a national academic body to support cybersecurity capacity building in developing nations. This thesis tries to fill this gap by collecting the views of security professionals in the industry, law enforcement, and educators in multiple geographic areas of Ecuador. This thesis provides understanding of the challenges that particularly arise in developing countries to enhance cybersecurity capabilities in a critical infrastructure sector, and comprehension of strategic areas that can support cybersecurity capabilities in the sector and potentially cybersecurity at the national level.

More specifically, this thesis provides or improves understanding of/about:

- the types of security incidents, some of which are hardly revealed to third parties, that occur in a critical sector of a developing nation
- the Ecuadorian financial sector's ability to deal with security incidents
- two cybersecurity strategies supporting capabilities in the context of a developing nation

[106] Critical infrastructure protection

- the effectiveness of a cybersecurity policy regulating the financial sector and opportunities for improvement
- the current state of the practice of cybersecurity education in Ecuador
- the Ecuadorian high educational institutions' ability to provide cybersecurity education
- the policy options that can potentially foster cybersecurity capacity building in Ecuador

Based on standard security modeling (attack-defense trees) available in the literature, this thesis also provides a method to assess effectiveness of a cybersecurity policy. Risk managers at financial institutions can use our approach and internal data to expand the analysis and cover areas of internal security (that were probably not reported). While this thesis is based on a study focused on a particular country, issues found in this work can be used to analyze whether or not any reported issues are present in developing environments similar to or different from Ecuador.

5.3 Limitations

While this thesis does not explicitly capture the views and experiences of those financial institutions that declined to participate, we included the views of stakeholders (e.g., authorities) who have a broad and firsthand knowledge of incidents occurring in the financial sector, and pursued replacement of potential participants from institutions of similar size. We also applied person, organization, and site triangulation to avoid effects of issues particular to specific groups or locations. Additionally, this thesis does not incorporate many views from universities with weaker academic standards (categories C: 7% & D: 17% in 2015). However, 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.

In Chapter 3, there is some degree of subjectivity in the defense analysis and mapping. Identifying countermeasures relies on the judgment of the researcher, which was partially addressed by incorporating security standards and best practices for addressing mitigating very-well known types of attacks. Similarly, mapping security controls to regulatory statements is challenging because the text and language in both, the standards and the regulation, may not be totally equivalent. We addressed this limitation to some extent by focusing our analysis on security concepts (e.g., segregation of networks) rather than functional words addressing these concepts. Another limitation is that our method does not make a distinction of the level of importance of each security control in the defense-tree analysis.

5.4 Implications for Policy and Practice

This thesis informs both public and organizational cybersecurity policy by using a multi-stakeholder approach, which integrates views from individuals managing, planning, responding, investigating, auditing, and controlling aspects of cybersecurity incidents as well as individuals with the responsibility to plan, manage, and provide cybersecurity education at the national level.

The first study provides insights on security incidents and incident response. Learning about the details on incidents, such as relative frequency, and concern about incidents arising in financial institutions, fosters situational awareness among participants of the financial sector. Also, understanding the barriers can allow practitioners to focus on the problems that matter when pursuing a course of actions. In addition, reports on stakeholders' preferences regarding potential strategies (CSIRT and ISAP) inform further steps to improve incident response in the financial sector.

The second study elucidates cyber policy-making and risk management. First, providing policy makers and designers of cyber regulations with feedback about policy performance has the potential to contribute to producing national policies that are better aligned towards their intended goals. Furthermore, risk managers can learn where to focus their efforts when addressing security incidents. Gaps in regulatory requirements can imply lack of a third-party control in an institution, which means that such areas should be incorporated under the check of the *internal control* function. Evidence of effectiveness—provided by this thesis—can influence financial practitioners' behavior, especially when regulations successfully address security incidents because financial risk managers likely feel motivated to pursue effective and meaningful compliance.

The third study illuminates areas of developing cybersecurity education and some aspects of building cybersecurity workforce. Similar to what happens in the first study, learning about the current practices in cybersecurity education potentially enables situational awareness among universities' authorities and professors. Likewise, understanding the factors that drive cybersecurity education informs universities and government about courses of actions needed to improve the current situation.

The above findings and insights have the potential to influence the practice of financial cybersecurity, development of cybersecurity capabilities, and hopefully beyond. A potential desired effect of this study is that it crosses the borders of financial security to inform strategies for CIP and national cybersecurity.

5.5 Future Work

Future work can procure understanding of internal barriers, such as internal coordination between security and IT functions (or departments when they are separated). Additional security scenarios could be designed to better understand willingness to share information about security incidents by including more participants. Regarding effectiveness of cyber policies, this study could be expanded to incorporate formal modeling to analyze security incidents that are not triggered by smart adversaries. In addition, the content of the Ecuadorian cyber regulation should be analyzed by considering incidents triggered by emergent threats (global trends) in the financial services, including attacks on EMV (e.g., pre-play attack [75]), POS intrusions, and sophisticated web application attacks. This proposed work is necessary since such attacks have been reported already in other latitudes and it is clear that threats migrate from other foreign countries over time, as occurred in Ecuador.

5.6 Recommendations

Most of the important barriers faced by financial institutions are internal, so that implies that institutions would significantly benefit from establishing enforceable agreements regarding cybersecurity practices among organizational departments. Conflicting objectives/interests arising between areas managing cyber risk (security) and IT departments (productivity) should be carefully planned and implemented to find the balance between these two frequently competing objectives. Institutions should clearly define their cybersecurity posture and communicate to employees and collaborators.

Although collaborative work has occurred regarding ATM machines, financial institutions have been traditionally working by themselves to confront most cybersecurity incidents. It is clear that criminals used the same vectors to successfully target more than one institution. To prevent adversaries' success, important collective benefit can be achieved when sharing information, even if this sharing is initially only limited.

Policy treatment of security incidents has taken a reactive approach, which is often what happens in the regulatory arena [106]. Most countermeasures have been enacted after losses have occurred. In the case of phishing, the policy response took about three years since the first phishing incidents occurred. A few major institutions had already taken a set of measures to address the problem by the time regulation was in place but not all. In this context, regulatory requirements are important to establish a security baseline in the financial sector. Regulation plays an essential role in managing cyber risk in small institutions because it is likely that investments in cybersecurity is mostly driven by regulatory requirements as reported by R29.[107]

At the national level, Ecuador needs to take further steps to plan and execute strategies to increase its cybersecurity capabilities that prepare the nation to confront present and future cyber challenges. A cybersecurity national plan that provides direction and support to universities is urgently needed. Also, strong links between the local industry and educational institutions need to be developed. With appropriate incentives, such partnership could foster understanding of cybersecurity demand, funding of university projects, and promoting research initiatives.

CERTs are now recognized as an essential element of national and international cybersecurity and as a key player in cybersecurity policy-making [107]. Oman is a clear example of a developing nation implementing a successful CERT that effectively supports cybersecurity capabilities beyond incident response. Nevertheless, creating a specialized CERT in a developing nation can be a significant challenge. In Ecuador, it has taken more than three years to start EcuCERT[108] since the executive order promoted its creation. Still, a national CERT that provides support nationwide across industries is needed. While the creation of a national CERT may be deliberated, initiatives to support capacity building in universities should be supported by the existing academic (CEDIA) and the telecommunications (EcuCERT) CERTs.

Finally, it is clear that developing internal capabilities in financial institutions is not enough to confront cyber-physical, multi-dimensional threats. Intelligent adversaries not only take advantage of institutional weaknesses but also exploit opportunities that the entire societal ecosystem may offer them. Therefore, industry, government, academia, and law enforcement need to be involved to develop policies and foster practices towards the development of cybersecurity capabilities. In that respect, our research provides a three-fold visualization of the problem and insights for improvement.

[107] Financial respondent 29

[108] A CERT in the telecommunications sector

References

[1] Verizon, “2014 Data Breach Investigations Report,” 2014.

[2] Verizon, “2015 Data Breach Investigations Report,” 2015.

[3] International Telecommunication Union (ITU) and ABI Research, “Global cybersecurity index,” 2014.

[4] UK Cabinet Office, “The UK Cyber Security Strategy Protecting and promoting the UK in a digital world,” 2011.

[5] International Telecommunication Union (ITU), “Cybersecurity guide for developing countries,” 2007.

[6] A. C. Tagert, “Cybersecurity Challenges in Developing Nations,” Carnegie Mellon University, 2010.

[7] N. Kortjan and R. Von Solms, “Cyber security education in developing countries: A South African perspective,” 2012, no. November, pp. 289–297.

[8] K. P. Newmeyer, “Cybersecurity Strategy in Developing Nations: A Jamaica Case Study,” Walden University, 2014.

[9] L. Muller, “Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities,” *Nor. Inst. Int. Aff.*, no. 21, pp. 1–4, 2015.

[10] J. W. Creswell, *Research design: Qualitative, quantitative and mixed methods approaches*, 4th ed. SAGE, 2014.

[11] D. K. Mulligan and F. B. Schneider, “Doctrine for Cybersecurity,” *Daedalus*, vol. 140, no. 4, pp. 70–92, 2011.

[12] U. Kuckartz, *Qualitative Text Analysis. A Guide to Methods, Practice and Using Software*. SAGE, 2014.

[13] *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*. USA: The White House, Office of the Press Secretary, 2013.

[14] New York State Department of Financial Services, “Report on Cyber Security in the Banking Sector,” 2014.

[15] M. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore, “Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,” 2004.

[16] M. R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore, “Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,” 2005.

[17] A. Cummings, T. Lewellen, D. McIntire, A. Moore, and R. Trzeciak, “Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U . S . Financial Services Sector,” 2012.

[18] K. Cole, M. Chetty, C. LaRosa, F. Rietta, D. Schmitt, and S. Goodman, “Cybersecurity in Africa: An Assessment,” *ResearchGate*, 2008.

[19] O. Osho and A. D. Onoja, “National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis,” *Int. J. Cyber Criminol.*, vol. 9, no. June, pp. 120–143, 2015.

[20] CERT/CC, “Colombia Case Study.” [Online]. Available: https://www.cert.org/incident-management/publications/case-studies/colombia.cfm. [Accessed: 20-Dec-2014].

[21] CERT/CC, “Tunisia Case Study.” [Online]. Available:

http://www.cert.org/incident-management/publications/case-studies/tunisia.cfm. [Accessed: 20-Dec-2014].

[22] Organization of American States and Symantec, “Latin American Security + Caribbean Cybersecurity Trends,” 2014.

[23] A. Galletta, *Mastering the SemiStructured Interview and Beyond: From Research Design to Analysis and Publication*, vol. 53. New York University Press, 2013.

[24] A. Adams and A. Cox, “Questionnaires, in-depth interviews and focus groups,” in *Research Methods for Human Computer Interaction.*, Cambridge University Press, 2008, pp. 17–34.

[25] M. Patton, “Qualitative evaluation and research methods,” Beverly Hills, CA: Sage, 1990, pp. 169–186.

[26] J. Van Maanen, “The Fact of Fiction in Organizational Ethnography,” *Adm. Sci. Q.*, vol. 24, no. 4, pp. 539–550, 1979.

[27] A. K. Shenton, “Strategies for ensuring trustworthiness in qualitative research projects,” *Educ. Information, IOS Press*, vol. 22, pp. 63–75, 2004.

[28] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology.” Gaithersburg. MD, Aug-2012.

[29] L. F. Cranor, “A Framework for Reasoning about the Human in the Loop,” in *Proceedings of the 1st Conference on Usability, Psychology, and Security, (UPSEC ’08)*, 2008.

[30] S. Talib, N. Clarke, and S. Furnell, “An Analysis of Information Security Awareness within Home and Work Environments,” in *International Conference on Availability, Reliability, and Security (ARES)*, 2010, pp. 196–203.

[31] European Union Agency for Network and Information Security (ENISA), “The new users’ guide: How to raise information security awareness,” *Information Security*. p. 140, 2010.

[32] M. T. Siponen, “Five dimensions of information security awareness,” *ACM SIGCAS Comput. Soc.*, vol. 31, no. 2, pp. 24–29, 2001.

[33] F. Hare, “The Cyber Threat to National Security: Why Can’t we Agree?,” in *Conference on Cyber Conflict*, 2010, pp. 211–225.

[34] J. J. Cebula and L. R. Young, “A Taxonomy of Operational Cyber Security Risks,” no. December, 2010.

[35] E. Glazer, “J.P. Morgan’s Cyber Attack: How The Bank Responded,” *The Wall Street Journal*. [Online]. Available: http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded/. [Accessed: 21-Dec-2014].

[36] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, “Organizational Models for Computer Security Incident Response Teams (CSIRTs),” 2003.

[37] T. Grance, T. Nolan, K. Burke, R. Dudley, G. White, and T. Good, “Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities,” 2006.

[38] C. Johnson, L. Badger, and D. Waltermire, “NIST Special Publication 800-150. Guide to Cyber Threat Information Sharing (Draft),” 2014.

[39] B. W. Lampson, “Computer Security in the Real World,” *Microsoft Research*. 2004.

[40] L. Stewart, “The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review,” 2010.

[41] Superintendencia de Bancos y Seguros, “Normas Generales para la Aplicación de la Ley General de Instituciones del Sistema Financiero, TITULO X.-De la Gestion y Administracion de Riesgos , CAPÍTULO V.-De la Gestión del Riesgo Operativo (JB-2005-834, updates JB-2012-1248 and JB-2014-3066).” Quito, 2005.

[42] A. Antón, “Goal Based Requirement Analysis Anton,” in *IEEE 2nd International Requirements Engineering Conference*, 1996, pp. 136–144.

[43] T. Breaux and A. Antón, “Deriving Semantic Models from Privacy Policies,” in *Sixth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY’05)*, 2005.

[44] T. Breaux and A. Antón, “Analyzing regulatory rules for privacy and security requirements,” *IEEE Trans. Softw. Eng.*, vol. 34, no. 1, pp. 5–20, 2008.

[45] T. Breaux, M. Vail, and A. Antón, “Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations,” in *14th IEEE International Requirements Engineering Conference (RE’06)*, 2006.

[46] T. Breaux, A. Anton, K. Boucher, and M. Dorfman, “Legal Requirements, Compliance and Practice: An Industry Case Study in Accessibility,” in *Proceedings of the 16th IEEE International Requirements Engineering Conference (RE’08)*, 2008, vol. 56, no. 104, pp. 43–52.

[47] D. Mellado, E. Fernández-Medina, and M. Piattini, “A common criteria based security requirements engineering process for the development of secure information systems,” *Elsevier Comput. Stand. Interfaces*, vol. 29, no. 2, pp. 244–253, Feb. 2007.

[48] C. Haley, R. Laney, J. Moffett, and B. Nuseibeh, “Security Requirements Engineering: A Framework for Representation and Analysis,” *IEEE Trans. Softw. Eng.*, vol. 34, no. 1, pp. 133–153, 2008.

[49] S. Islam and J. Jürjens, “Incorporating Security Requirements from Legal Regulations into UMLsec model,” in *Modelling Security Workshop (MODSEC08)*, 2008.

[50] A. Siena, A. Perini, J. Mylopoulos, and A. Susi, “From Laws to Requirements,” in *IEEE Requirements Engineering and Law, RELAW’08*, 2008.

[51] T. Breaux and D. Gordon, “Regulatory Requirements Traceability and Analysis Using Semi-formal Specifications,” in *International Working Conference on Requirements Engineering: Foundation for Software Quality*, 2013, pp. 141–157.

[52] T. Breaux and A. Anton, “A Systematic Method for Acquiring Regulatory Requirements: A Frame-Based Approach,” in *International Workshop on Requirements for High Assurance Systems (RHAS-6)*, 2007, vol. 1936, no. 104, pp. 1–6.

[53] F. Catota, “Análisis de la Regulación de Riesgo de las Tecnologías de Información en el Ambito Financiero Ecuatoriano [Analysis of Information Technology Risk Regulation in the Ecuadorian Financial Sector],” Escuela Politécnica Nacional, 2010.

[54] A. Kurt, “Effectiveness of Cyber Security Regulations in the US Financial Sector: A Case Study,” Carnegie Mellon University, 2015.

[55] S. Hussain, A. Kamal, S. Ahmad, G. Rasool, and S. Iqbal, “Threat Modelling Methodologies: a Survey,” *Sci. Int.(Lahore)*, vol. 26, no. 4, pp. 1607–1609, 2014.

[56] S. Myagmar, A. Lee, and W. Yurcik, “Threat Modeling as a Basis for Security

Requirements," in *Symposium on requirements engineering for information security (SREIS)*, 2005, pp. 1–8.

[57] J. D. Weiss, "A system security engineering process," in *14th Annual NCSC/NIST National Computer Security Conference*, 1991, pp. 572–581.

[58] E. G. Amoroso., *Fundamentals of computer security technology*. Prentice-Hall, 1994.

[59] N. G. Leveson, *Safeware: System Safety and Computers*. Addison-Wesley, 1995.

[60] R. R. Yager, "OWA trees and their role in security modeling using attack trees," *Inf. Sci. (Ny).*, vol. 176, no. 20, pp. 2933–2959, 2006.

[61] I. Nai Fovino, M. Masera, and A. De Cian, "Integrating cyber attacks within fault trees," *Reliab. Eng. Syst. Saf.*, vol. 94, no. 9, pp. 1394–1402, 2009.

[62] A. Roy, D. S. Kim, and K. S. Trivedi, "Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees," *Secur. Commun. Networks*, vol. 5, no. 8, pp. 929–943, Aug. 2012.

[63] B. Ivanc and T. Klobu, "ESM: an enhanced attack tree model for critical infrastructure," *J. Control Eng. Appl. Informatics*, vol. 17, no. 4, pp. 102–113, 2015.

[64] S. Vidalis and A. Jones, "Using vulnerability trees for decision making in threat assessment," 2003.

[65] K. S. Edge, G. C. Dalton, R. a. Raines, and R. F. Mills, "Using attack and protection trees to analyze threats and defenses to homeland security," in *IEEE Military Communications Conference MILCOM*, 2006, pp. 1–7.

[66] A. Marback, S. Kondamarri, and D. Xu, "Security test generation using threat trees," in *Automation of Software Test, AST'09. ICSE Workshop on*, 2009, pp. 62–69.

[67] B. Kordy, P. Kordy, S. Mauw, and P. Schweitzer, "ADTool: Security analysis with attack-defense trees," in *International Conference on Quantitative Evaluation of Systems*, 2013, pp. 173–176.

[68] D. Podkuiko, "Vulnerabilities in Advanced Metering Infrastructure," Pennsylvania State University, 2012.

[69] K. Edge, R. Raines, M. Grimaila, R. Baldwin, R. Bennington, and C. Reuter, "The Use of Attack and Protection Trees to Analyze Security for an Online Banking System," in *IEEE, System Sciences (HICSS'07). 40th Annual Hawaii International Conference on*, 2007, p. 144b–144b.

[70] N. Kaur, "A Survey on Online Banking System Attacks and its Countermeasures," *Int. J. Comput. Sci. Netw. Secur.*, vol. 15, no. 3, p. 57, 2015.

[71] C. K. Dimitriadis, "Analyzing the security of Internet banking authentication mechanisms," *Inf. Syst. Control J.*, vol. 3, p. 34, 2007.

[72] T. Chee-Wooi, G. Manimaran, and L. Chen-Ching, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst. Man, Cybern. Part A Syst. Humans*, vol. 40, no. 4, pp. 853–865, 2010.

[73] J. D. Howard and T. A. Longstaff, "A Common Language for Computer Security Incidents." Sandia National Laboratories, 1998.

[74] B. Schneier, "Attack Trees - Modeling security threats," *Dr. Dobb's J.*, 1999.

[75] M. Bond, O. Choudary, S. Murdoch, S. Skorobogatov, and R. Anderson, "Chip and skim: Cloning EMV cards with the pre-play attack," in *2014 IEEE Symposium*

on Security and Privacy, 2014, no. May, pp. 49–64.

[76] C. Paulsen, E. McDuffie, W. Newhouse, and P. Toth, “NICE: Creating a cybersecurity workforce and aware public,” *IEEE Secur. Priv.*, vol. 10, no. 3, pp. 76–79, 2012.

[77] CEAACES, “Ecuador: el modelo de evaluación del Mandato 14.” Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior, Quito, 2013.

[78] CEAACES, “‘Suspendida por falta de calidad.’ El cierre de catorce universidades en el Ecuador.” Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior, Quito, 2013.

[79] NICE, “National initiative for cybersecurity education (NICE). Relationship to president ’s education agenda.” 2010.

[80] National Institute of Science and Technology, “The national cybersecurity workforce framework.” 2013.

[81] M. C. Libicki, D. Senty, and J. Pollak, *H4CKER5 WANTED: An examination of the cybersecurity labor market*. Rand Corporation, 2014.

[82] GENERAL AUDITOR, “The UK cyber security strategy: Landscape review.” 2013.

[83] Tempus, “Report on EU practice for cyber security education,” 2013.

[84] J. Harašta, “Cyber security in young democracies,” *Jurisprudencija*, vol. 20, no. 4, pp. 1457–1472, 2013.

[85] M. Lehto, “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. Academic Conferences Limited*, 2015, p. 179.

[86] K. Newmeyer, “Elements of national cybersecurity strategy for developing nations,” *Natl. Cybersecurity Inst. J.*, vol. 1, no. 3, pp. 9–19, 2015.

[87] R. Von Solms and S. Von Solms, “Cyber safety education in developing countries,” *Syst. Cybern. Informatics*, vol. 13, no. 2, pp. 14–19, 2015.

[88] A. Curbelo and A. Cruz, “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*, 2013, pp. 1–8.

[89] Organization of American States and Inter-American Development Bank, “Cybersecurity. Are we ready in Latin America and the Caribbean?,” 2016.

[90] A. Parekh, A. Pawar, P. Munot, and P. Mantri, “Secure authentication using anti-screenshot virtual keyboard,” vol. 8, no. 5, pp. 534–537, 2011.

[91] M. Hathaway, C. Demchak, J. Kerben, J. Mcardle, and F. Spidalieri, “Cyber readiness index 2.0.” 2015.

[92] M. A. Wright, “Improving cybersecurity workforce capacity and capability,” *ISSA J.*, vol. 13, no. 10, pp. 14–20, 2015.

[93] M. Pollack, “Chile transition to a knowledge based economy role of Chilean professionals abroad,” 2004.

[94] C. Sledge, “Building information assurance educational capacity: Pilot efforts to date,” Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 2005.

[95] International Telecommunication Union, “ITU cybersecurity work programme to assist developing countries 2007-2009.” 2009.

[96] S. Montgomery, “English and science: realities and issues for translation in the age of an expanding lingua franca,” *J. Spec. Transl.*, vol. 2003, no. 11, pp. 6–16, 2009.

[97] K. Michael and D. Weidemann, *Internationalization of the social sciences Asia – Latin America – Middle East – Africa – Eurasia*. Verlag, Bielefeld, 2015.

[98] Raytheon, “Securing our future: Closing the cybersecurity talent gap,” 2015.

[99] S. Vincent-Lancrin, R. Hopper, and M. Geloso, “Cross border higher education for development.” OEDC & World Bank, pp. 1–88, 2006.

[100] F. B. Schneider, “Cybersecurity education in universities,” *IEEE Secur. Priv.*, vol. 11, no. 4, pp. 3–4, 2013.

[101] M. Dark, “Advancing cybersecurity education,” *IEEE Secur. Priv.*, vol. 12, no. 6, pp. 79–83, 2014.

[102] M. Bishop and C. Taylor, “A critical analysis of the centers of academic excellence program,” in *13th Colloquium for Information Systems Security Education*, 2009.

[103] A. Klimburg, (Ed.), “National cyber security framework manual.” NATO Cooperative Cyber Defense Center of Excellence, 2012.

[104] N. Kortjan and R. Von Solms, “A conceptual framework for cyber-security awareness and education in SA,” *South African Comput. J.*, no. 52, pp. 29–41, 2014.

[105] B. S. Susanne Furman, Mary Theofanos, Yee-Yin Choong, “Basing cybersecurity training on user perceptions,” *IEEE Secur. Priv.*, vol. 10, no. 2, pp. 40–49, 2012.

[106] J. Bayuk, J. Healey, P. Rohmeyer, M. Sachs, J. Schmidt, and J. Weiss, *Cyber Security Policy Guidebook*. John Wiley & Sons, 2012.

[107] R. Morgus, I. Skierka, M. Hohmann, and T. Maurer, “National CSIRTs and Their Role in Computer Security Incident Response,” no. November. 2015.

[108] International Telecommunication Union (ITU) and ABI Research, “Global cybersecurity index & cyberwellness profiles,” 2015.

[109] Business Software Alliance, “EU cybersecurity dashboard. A path to a secure European cyberspace,” 2015.

[110] T. Feakin, J. Woodall, and L. Nevill, “Cyber maturity in the Asia-Pacific region.” Australian Strategic Policy Institute, 2015.

[111] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, “Handbook for Computer Security Incident Response Teams (CSIRTs),” *SEI Digital Library*, no. 2nd Edition. Carnegie Mellon University, Software Engineering Institute, 2003.

[112] B. Kordy, L. Piètre-Cambacédès, and P. Schweitzer, “DAG-based attack and defense modeling: Don’t miss the forest for the attack trees,” *Comput. Sci. Rev.*, vol. 13–14, pp. 1–38, 2014.

[113] E. A. Fischer, “Cybersecurity issues and challenges: In Brief,” *Cybersp. Threat Landsc. Overview, Response Authorities, Capab.*, pp. 45–54, 2015.

Appendices

Appendix A: Acronyms and Abbreviations

ACM	Association for Computing Machinery
ATM	Automated Teller Machine
CCNA	Cisco Certified Network Associate
CCTV	Closed Circuit Television
CERT	Community Emergency Response Team
CSIRT	Computer Security Incident Response Team
CI	Coverage Index
CN	Computer Networks
CS	Computer Science
CIP	Critical Infrastructure Protection
CIT	Computer Information Technology
CSC	Critical Security Controls from
CSI	Center for Internet Security
DDOS	Distributed Denial-of-Service
EMV	Europay MasterCard and VISA
FBRAM	Frame Based Requirements Analysis Method
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISP	Internet Service Provider
ISAP	Information Sharing and Analysis Program
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
JB-384	*Junta Bancaria – Resolución* JB-2005-834
JB-2148	*Junta Bancaria – Resolución* JB-2012-2148 (update)
JB-3066	*Junta Bancaria – Resolución* JB-2014-3066 (update)
NIST	National Institute of Standards and Technology
OAS	Organization of American States
PCI	Payment Card Industry
PCI-DSS	Payment Card Industry - Data Security Standard
PCI PTS POI	PIN Transaction Security Point of Interaction Security Requirements
PKI	Public Key Infrastructure
POS	Point of Sale
SCADA	Supervisory Control And Data Acquisition
SQUARE	Security Quality Requirements Engineering
SMS	Short Message Service
WTS	Willingness to Share

Appendix B: Definition of Terms

Term	Definition	Source
Attack	Attempt to violate a security policy	CERT, 2004
Constituency	Defined user community supported by a CSIRT	CERT, 2004
Incident	In this thesis implies security incident or computer security incident or cybersecurity incident	CERT, 2004
Incident Profile	Describes a specific pattern that characterizes (1) a security incident or (2) a set of similar security incidents having a common goal.	This thesis
Information Sharing	The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.	SP 800-16
Keylogger	Any piece of software or hardware that has the capability to intercept and record input from the keyboard of a compromised machine.	Kaspersky, 2013
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.	NIST SP 800-83
Pharming	An attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct web address.	CPNI, 2010
Phishing	A form of electronic deception where an individual is persuaded to perform actions or divulge information by an attacker impersonating a trustworthy entity.	CPNI, 2010
Situational Awareness	Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension / meaning of both taken together (risk).	CNSSI-4009
Skimming	The unauthorized use of a reader to read tags without the authorization or knowledge of the tag's owner or the individual in possession of the tag.	SP 800-98
Social Engineering	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.	SP 800-61
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.	SP 800-53
Unauthorized Access	Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.	FIPS 191
Vulnerability	Existence of a software weakness, such as a design or implementation error that can lead to an unexpected or undesired event compromising the security of a system, network, application or protocol.	CERT, 2004

Appendix C: Definitions of CSIRT/CERT Services

Service	Definition	Source
Alerts and Warnings	This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem.	CERT, 2003
Awareness Building	CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies.	CERT, 2003
Education / Training	This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials. CERT	CERT, 2003
Exercises	An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.	SP800-84
Incident Handling	This service "involves receiving, triaging (sorting, categorizing, and prioritizing), and responding to requests and reports, and analyzing incidents and events.	CERT, 2003
Information Sharing	Incident response teams often participate in information sharing groups, such as ISACs or regional partnerships. Accordingly, incident response teams often manage the organization's incident information sharing efforts, such as aggregating information related to incidents.	SP800-61
Monitoring / Visibility / Watch	The CSIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies	CERT, 2003
Shutdown Spoofed Websites	*Online fraud shutdown services* --addresses online fraud threats. Ensure blocking and shutdown of phishing sites across countries.	RSA, 2011
SMTP Senders Detection	Detection and tracking of SMTP servers relaying spam and scam.	Respondent 11
Stolen Data Detection	Detection and tracking of financial data that has been stolen from financial institutions.	Respondent 11
Vulnerability analysis	The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software.	CERT, 2003
Vulnerability analysis	The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited.	CERT, 2003

Appendix D: Interview Guide Topics for Incident Response

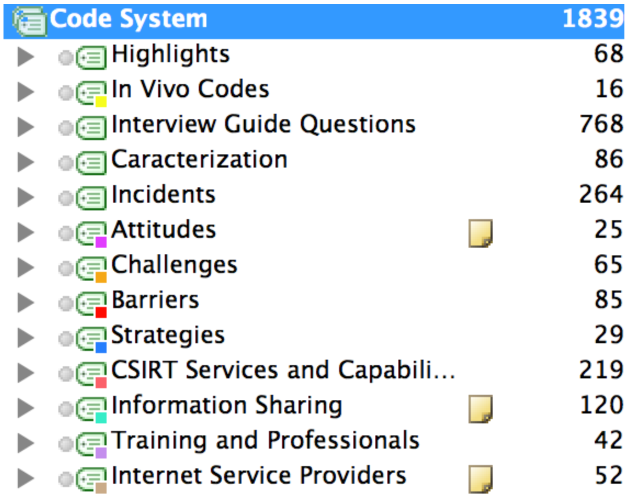
(Left column were used more extensively)

Financial Stakeholders and Authorities	ISPs, CSIRTs & One Authority
A. Demographics section --- B. Cybersecurity concept C. Incident concept D. Type of incidents E. Frequency of incidents F. Level of concern G. Changes over time H. Targeted infrastructure I. Criteria for incident severity -- J. Internal barriers K. External barriers L. People’s idiosyncrasy M. The biggest barrier N. Internal desired resources O. External desired resources P. ISPs Role Q. Internal CSIRT availability -- R. CSIRT services S. Level of importance of CSIRT services T. CSIRT authority U. CSIRT location (organizational/physical) V. CSIRT funding --- W. Information required X. Usability of the information Y. Criteria for sensitive information Z. Sharing information – scenarios AA. Consolidating or splitting CSIRT/ISAC BB. Overcoming lack of personal CC. Incentives for sharing – trust develop DD. Metrics for sharing -- EE. Availability of qualified personal FF. Type of training required GG. Comments	A. Demographics section --- B. Cybersecurity concept C. Incident concept D. Type of incidents E. Frequency of incidents F. Level of concern G. Changes over time H. Targeted infrastructure -- I. Inner limitations of constituents J. External limitations of constituents K. The biggest barrier L. Involving additional stakeholders M. ISPs Role N. CSIRT services O. Level of importance of CSIRT services P. CSIRT authority Q. CSIRT location (organizational/physical) R. Barriers to make CSIRT visible S. CSIRT funding -- T. Information required U. Criteria for sensitive information V. Barriers for information sharing W. Incentives for sharing – trust develop. X. Metrics for sharing Y. Consolidating or splitting CSIRT/ISAC -- Z. Availability of qualified personal AA. Overcoming lack of qualified personal BB Deterrence collaboration CC. Provisioning of training DD. CSIRT creation and operation barriers EE. Comments

Appendix E: Categories and Coding Example for Incident Response

Categories—Taken from the QDA Software (MAXQDA 11)**,** Figure E1 lists the main categories included in our analysis. While the original codebook is in Spanish, we renamed the categories to illustrate them in English. On the right, the numbers indicate the number of instances of coding that each category contains.

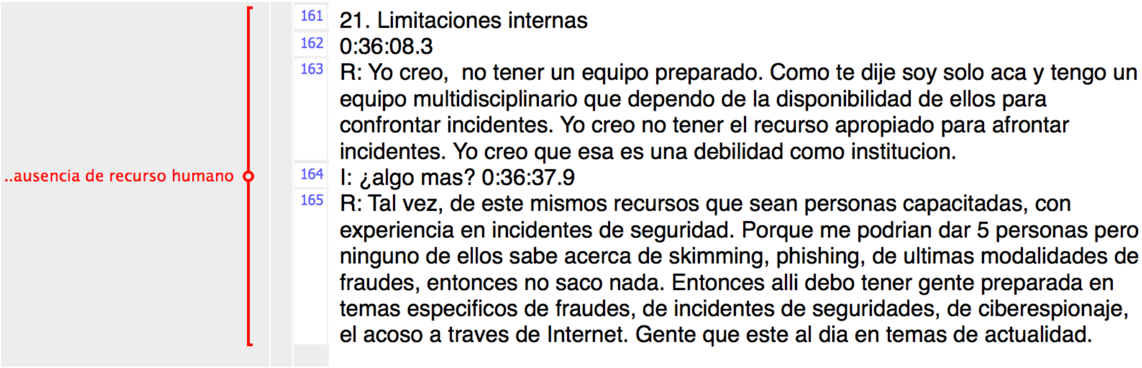
From the top, *Highlights* and *In Vivo Codes* were used to inform and refine the codebook. Next, the *Interview Guide Questions* category contains the codes for every single question. Finally, we have ten main categories, from *Characterization* to *Internet Service Providers*, which include 64 codes used to index each interview.



Code System	1839
Highlights	68
In Vivo Codes	16
Interview Guide Questions	768
Caracterization	86
Incidents	264
Attitudes	25
Challenges	65
Barriers	85
Strategies	29
CSIRT Services and Capabili...	219
Information Sharing	120
Training and Professionals	42
Internet Service Providers	52

Figure E1: Categories of the Codebook in English

Prototypical example—The next example is taken from the original data, which illustrates the assignment of a code to a segment of text in Spanish. The numbers in blue indicate the number of the paragraph in the transcript. Also, the content includes timestamps to listen to the audio when needed.



161 21. Limitaciones internas

162 0:36:08.3

163 R: Yo creo, no tener un equipo preparado. Como te dije soy solo aca y tengo un equipo multidisciplinario que dependo de la disponibilidad de ellos para confrontar incidentes. Yo creo no tener el recurso apropiado para afrontar incidentes. Yo creo que esa es una debilidad como institucion.

164 I: ¿algo mas? 0:36:37.9

165 R: Tal vez, de este mismos recursos que sean personas capacitadas, con experiencia en incidentes de seguridad. Porque me podrian dar 5 personas pero ninguno de ellos sabe acerca de skimming, phishing, de ultimas modalidades de fraudes, entonces no saco nada. Entonces alli debo tener gente preparada en temas especificos de fraudes, de incidentes de seguridades, de ciberespionaje, el acoso a traves de Internet. Gente que este al dia en temas de actualidad.

Figure E2: Illustration of Coding in Spanish

Appendix F: Frequency of Incidents and Concern

Numbers in the main frame of the two next tables represent the number of times stakeholders selected a particular value in the Likert scale on the cross tabs. For example, in row number one, "*user-error,*" five stakeholders said they *occasionally* see incidents related to users' errors.

Table F1: Reported Frequency of type of incidents (institutions and authorities)

	Frequency	**Never**	**Rarely**	**Occasionally**	**Sometimes**	**Frequently**	**Usually**	**Every time**		
N	**Likert Scale & Incident**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**Score**	**Normalized Score**
1	User error	0	1	5	7	4	3	1	90	0.17
2	Phishing	8	2	3	3	5	3	0	76	0.14
3	Skimming	3	5	4	3	3	0	3	73	0.14
4	Malware	5	7	4	3	1	2	0	60	0.11
5	Unavailability	1	7	8	1	3	0	0	58	0.11
6	Information leakage	1	6	0	6	2	0	0	47	0.09
7	Unauthorized access	0	4	0	4	0	0	0	24	0.04
8	Internal fraud	0	1	4	1	0	0	0	18	0.03
9	Carding	0	1	0	1	0	1	0	12	0.02
10	Insider	3	1	2	0	0	0	0	11	0.02
11	Identity impersonation	0	2	2	0	0	0	0	10	0.02
12	Port scan	0	0	0	0	2	0	0	10	0.02
13	Denial service	2	3	0	0	0	0	0	8	0.01
14	Scam	0	1	0	0	0	1	0	8	0.01
15	Card theft	0	0	1	0	1	0	0	8	0.01
16	Network abuse	0	0	0	0	0	1	0	6	0.01
17	Pharming	1	0	1	0	0	0	0	4	0.01
18	Internet surfing abuse	0	0	0	1	0	0	0	4	0.01
19	Spam	0	0	1	0	0	0	0	3	0.01
20	Defacement	0	1	0	0	0	0	0	2	0.00
21	Physical sabotage	0	1	0	0	0	0	0	2	0.00
22	Hacking	1	0	0	0	0	0	0	1	0.00

Table F2: Reported Level of Concern of Financial Stakeholders (Institutions and Authorities)

	Concern	Not at all	Slightly	Somewhat	Moderately	Extremely		
N	**Likert Scale & Incident**	**1**	**2**	**3**	**4**	**5**	**Score**	**Normalized Score**
1	User error	0	2	7	9	2	71	0.13
2	Information leakage	0	2	2	6	7	69	0.13
3	Malware	0	8	4	9	1	69	0.13
4	Phishing	0	8	5	7	2	69	0.13
5	Skimming	0	4	6	7	2	64	0.12
6	Unavailability	1	5	4	5	4	63	0.12
7	Unauthorized access	0	0	1	3	3	30	0.05
8	Internal fraud	0	1	3	0	2	21	0.04
9	Insider	0	4	0	1	1	17	0.03
10	Identity-impersonation	0	2	0	1	1	13	0.02
11	Denial service	0	3	1	1	0	13	0.02
12	Carding	0	0	1	0	1	8	0.01
13	Port scan	0	0	1	1	0	7	0.01
14	Pharming	0	1	0	1	0	6	0.01
15	Internet surfing	0	0	0	0	1	5	0.01
16	Card theft	0	1	1	0	0	5	0.01
17	Hacking	0	0	0	1	0	4	0.01
18	Scam	0	2	0	0	0	4	0.01
19	Defacement	0	0	1	0	0	3	0.01
20	Network abuse	0	0	1	0	0	3	0.01
21	Spam	0	1	0	0	0	2	0.00
22	Physical sabotage	1	0	0	0	0	1	0.00

$$Score = \sum_{i=1}^{n} w_i * f_i$$

$w_i = weight\ given\ by\ the\ Likert\ scale\ (\ i = 1\ to\ n)$
$f_i = elicited\ frequency\ (or\ concern) from\ respondents$
$n = 7\ for\ frequency\ and\ 5\ for\ concern$

Appendix G: Relevant Quotations

Awareness

People may know about security incidents, but they think that these incidents are never going to happen to them [several respondents].

Priorities

IT does not resolve our [security] requirements. They have business priorities [R1].

Training and experience

I need people with incident security experience [R20].
I had to hire a specialist from another country [R3].

Insufficient size of security team

We are only a few people here [R1].
I need a dedicated team for incident handling [R14].
We have no people to implement projects of this nature [R17].
They come, learn, work two years, and then leave [R33].

Appendix H: Interview Protocol for National Stakeholders (Financial and Authorities[109])

(Translation from Spanish)

Thank you for participating in this interview. The purpose of this research study is to investigate the needs, limitations, and desired actions from national stakeholders when handling cybersecurity incidents. As part of this study, we will be asking you questions that are related to your experiences with handling security incidents and desired ways to handle such incidents. Based on this information, we will conduct an analysis to propose technological and policy strategies in order to improve cybersecurity incident response capabilities of the financial sector.

In order to protect your privacy, we will protect your identity by neither requiring personal identifiable information nor revealing the organization for which you work. Finally, if you feel uncomfortable, you are free to not answer any questions or to stop the interview at any point.

We greatly value your participation.

Demographics

1. Approximately, how old are you?
2. What is your gender?
3. What is your education?
   1 High school 2 Bachelor 3 Master4 Doctorate
4. What is your degree in? (e.g., economics, IT, or other)
5. What is your role in the organization you work with?
6. How long have you been working in cybersecurity?
7. How long have you been working in banking and finance?
8. Approximately, how many customers does your organization have?
9. Approximately, how many of those customers use electronic means to conduct financial transactions?
10. What is the size of your information security team?

Incidents

11. Would you please define cybersecurity?
12. Would you please define security incident? [pause] What is the difference between incident and event?
13. What are the most common types of incidents your organization deals with?
14. Would you rank the frequency with which these incidents arise?
    1 Never
    2 Rarely (less than 10%)
    3 Occasionally (about 30%)
    4 Sometimes (about 50%)
    5 Frequently (about 70%)
    6 Usually (about 90%)
    7 Every time

15. Would you rank the level of concern (impact) of these types of incidents on your organization? What are the ranking criteria?
    1 Not at all concerned
    2 Slightly concerned
    3 Somewhat concerned
    4 Moderately concerned
    5 Extremely concerned
16. Over the last 5 years, would you say it has changed? How?

[109] When interviewing authorities, we paraphrased the questions so that it makes sense for them to answer. For example, since they do not represent financial institutions, they may not experience incidents directly, but they regulate, investigate, observe, analyze, and so forth.

17. What are the transactional means (channels) that are the most attacked or targeted by (professional) criminals? Would you rank them according to their frequency of occurrence?
    1 Never
    2 Rarely (less than 10%)
    3 Occasionally (about 30%)
    4 Sometimes (about 50%)
    5 Frequently (about 70%)
    6 Usually (about 90%)
    7 Every time
18. What are the potential sources of infection of attacks?
19. What are the criteria to classify incidents as critical?

Response Capabilities

<Current>

20. What are the limitations/difficulties inside your organization when confronting incidents?
21. How does the idiosyncrasy of individuals impact your ability to handle incidents?
22. What are the problems you cannot solve because of lack of external support (e.g., technical, legal, policy)? Please explain.
23. From those just mentioned, what would be the biggest problem(s) you face when responding to incidents?

<Desired>

24. In your organization, what resources would you like to have when confronting incidents?
    [checkpoint]
25. Outside of your organization, what resources would you like to have?
    [checkpoint]
26. Where should the CSRIT be physically and organizationally located? Why?
    1 Academia 2 Government 3 Financial industry 4 Other
27. How should a Financial CSIRT be funded?

Information Sharing

<Consuming>

28. What types of information do you need or would you like to consume from other stakeholders to better respond to incidents?
29. How would you use this information?

<Providing>

30. What type of information do you consider sensitive? What are the criteria you use to define it as sensitive?
31. In the following scenarios, please indicate whether or not you would share information that has been generated during the course of a security incident. Please explain why you make such decision.
    Description of SCENARIO 1: Phishing involving pharming techniques.
    [Describe data involved and identify willingness to share]
        1 IP Address (source of attacks)
        2 Type of asset targeted
        3 Vector of attack
        4 Malware sample
        5 Mitigation strategies (methods / technology used to mitigate the incident)
        6 Attack impact in qualitative terms
        7 Attack impact and quantitative terms
        8 Vulnerability of the target
    Would your decision change, if the incident were different?

    Description of SCENARIO 2: Hacking a Web Server (similar description of options)

32. Should the CSIRT and the information sharing analysis center (ISAC) be a unique organization or two separate organizations? Why?

<Effectiveness>

33. What conditions would incentivize you to participate in an information sharing program?
34. What should the metrics be to measure the effectiveness of the information sharing program?

<Training>

35. Do you feel that Ecuador produces or has enough professionals prepared in cybersecurity? Why?
36. What kind of training is needed?

Others

<Closure>

37. Is there any question I did not ask that you would have liked to answer?
38. Do you have any other comments or questions about any topics we covered today?

Thank you for your time!

Table H1: Example of Cross-tabs for eliciting CSIRT services

Likert Scale	Alerts and warnings	Incident handling	Awareness building	Training	Exercises	Legal support	Information sharing	VA	MA
1. Not at all important 2 Low importance									
3. Slightly important 4 Neutral									
5. Moderately important 6. Very important 7. Extremely important									

VA: Vulnerability Analysis; **MA**: Malware Analysis

Appendix I: Coverage Index (CI)

ID	Security incident profile	Label	CI	Control calls
A1	Unauthorized physical access	A1-physical	0.77	13
A2	Unauthorized software application access	A2-application	0.80	51
A3	Unauthorized network access	A3-network	0.50	9
L1	Information leakage by reusing credentials	L1-re-using	0.93	25
L2	Information leakage by stealing a data container	L4-data container	0.91	35
L3	Information leakage by deceiving users	L2-deceiving	0.83	22
L4	Information leakage by visual access	L3-visualization	0.70	20
M1	Infection through removable devices	M1-removable	0.63	19
M2	Infection through e-mail attachments	M2-email	0.80	41
M3	Infection through compromised websites	M2-website	0.57	12
M4	Connecting a computer system to the network	M3-network	0.55	16
P1	Generating spoofed financial websites	P1-spoofing	1.00	1
P2	Phishing through e-mail to obtain credentials	P2-email	1.00	2
P3	Phishing through spoofed websites and e-mail	P3-email & web	1.00	4
P4	Pharming by malware infection	P4-pharming	1.00	4
S1	Installing external devices on ATMs	S1-installing	0.33	24
S2	Capturing of sensitive data on ATMs	S2-capturing	0.27	15
F1	Unauthorized e-banking transaction	F1-e-banking	1.00	3
F2	Unauthorized ATM transaction	F2-ATM	1.00	3
F3	Cash withdraw from a bank counter	F3-counter	0.64	11
F4	Fraud through social engineering	F4-deceiving	0.75	4
F5	Internal fraud	F5-internal	1.00	3
U1	Operational error	U1-operational	1.00	1
U2	Password sharing	U2-sharing	1.00	3
U3	Inappropriate applications testing	U3-testing	0.89	3
U4	Running scripts in production environments	U4-scriptimg	1.00	4
O1	Distributed denial of service	O1-DDoS	0.13	4
O2	Website defacement	O2-defacement	0.83	21
O3	Spam	O3-spam	0.25	2
O4	Customer impersonation	O4-impersonation	0.67	3
O5	Exchanging of debit/credit cards	O5-exchange	1.00	2
O6	Flooding	O6-flooding	1.00	3

Appendix J: Standard Security Controls

These tables present the list of security controls (objective security controls) and frequency of calls across attack trees. ISO controls often include several sub controls.

ISO 27002:2013	N*
ISO 12.2.1	38
ISO 7.2.2	30
ISO 9.3.1	15
ISO 13.1.1	14
ISO 13.2.1	14
ISO 13.1.2	12
ISO 13.1.3	10
ISO 8.3.1	9
ISO 11.1.2	9
ISO 12.4.1	9
ISO 6.2.1	8
ISO 11.1.3	8
ISO 9.4.2	7
ISO 10.1.1	6
ISO 11.1.1	6
ISO 12.4.3	6
ISO 12.6.2	6
ISO 13.2.3	6
ISO 11.1.6	5
ISO 11.2.9	5
ISO 9.1.1	4
ISO 11.2.8	4
ISO 9.1.2	3
ISO 11.1.5	3
ISO 11.2.6	3
ISO 6.1.2	2
ISO 7.2.3	2
ISO 8.1.4	2
ISO 9.4.3	2
ISO 11.2.5	2
ISO 12.4.2	2
ISO 7.1.1	1
ISO 7.1.2	1
ISO 7.3.1	1
ISO 8.2.1	1
ISO 8.2.3	1
ISO 8.3.2	1
ISO 8.3.3	1
ISO 9.2.1	1
ISO 9.2.2	1
ISO 9.2.3	1
ISO 9.2.5	1
ISO 9.2.6	1
ISO 9.4.1	1
ISO 11.1.4	1
ISO 11.2.1	1
ISO 11.2.7	1
ISO 12.6.1	1
ISO 13.2.2	1
ISO 14.2.5	1
ISO 15.1.1	1
ISO 15.1.2	1
ISO 15.1.3	1
ISO 15.2.1	1
ISO 18.2.1	1

CSC 6.0	N*
CSC 1.2	1
CSC 5.1	1
CSC 7.4	1
CSC 13.1	1
CSC 13.2	1
CSC 13.3	1
CSC 13.4	1
CSC 13.5	1
CSC 13.6	1
CSC 13.7	1
CSC 13.8	1
CSC 13.9	1
CSC 1.5	0
CSC 8.3	0
CSC 9.2	0
CSC 11.2	0

PCI PTS POI	N*
4.1-A1	4
4.1-A2	4
4.1.2-k	5
4.1.2-o	4
Chapter 2	4

***N:** Number of calls

ISO: International Organization for Standardization, Information Technology – Security Techniques – Code of Practice for Information Security Management
CSC: Critical Security Controls from CSI - Center for Internet Security
PCI PTS POI: Payment Card Industry PIN Transaction Security Point of Interaction Security Requirements

Appendix K: Summarization of Regulation JB-834

Regulatory requirements to address IT risks in the financial sector are contained in Chapter V (Operational Risk) of JB-2005-834 (here abbreviated JB-834). This framework comprises nine parts, six of which encompasses most requirements to mitigate risks. Part I provides scope and definitions of terms.

Part II addresses factors of risks, primarily processes, people, and technology, which are called risk class by CERT/CC.[110] This part begins with requirements for strategic processes, operational processes, and supporting processes. Next, security concerns prior, during, and upon termination of employment are covered. Then, requirements focus on: (1) IT governance principles; (2) policy and procedures to address operational tasks, security incidents, IT inventory, backup and physical preservation of information; (3) acquisition, development, and maintenance of systems; (4) administration, monitoring, capacity planning of IT infrastructure, and migration of IT infrastructure; (5) security countermeasures in electronic means supporting financial transactions, such as credit cards, IVR, ATM machines, point of sale devices (POS), and online banking; and, lastly, (6) risk in external events are briefly mentioned.

Part III provides requirements regarding *operational risk management,* including external and internal fraud, credit operations, information availability, and compliance. Part IV addresses *business continuity planning* to minimize loses when an interruption of operational services occurs. Part V defines responsibilities for *operational risk management*, including those for the board of directors, integral risk administration committee, and financial institutions' risk department. Part VI mandates requirements for dealing with third parties. This comprises policies, processes, and procedures for: (1) selecting and evaluating providers; (2) contracting with providers; (3) leasing critical services; and (4) implementing resilience for providers of critical services.

Part VII addresses information security, which includes: (1) conditions for an *information security management system* (ISMS*),* such as implementation, monitoring, documentation, and performance. Here, having the series of standards ISO/IEC 27000 as a reference is mandatory; (2) change management and direct access to databases; (3) security control systems (e.g., firewall, IDS/IPS[111], WAF[112]), security testing and auditing of IT infrastructure, and controls for non-authorized software; (4) information inventory, security requirements by type of information, and information protection (e.g., encryption); and (5) records for incident management. Finally, part VIII and part IX provide general dispositions and deadlines for the regulation's implementation respectively.

[110] J. Cebula and L. Young, CMU, A Taxonomy of Operational Cyber Security Risks, 2010

[111] Intrusion Detection and Prevention Systems

[112] Web Application Firewall

Appendix L: Interview Protocol for Academic Respondents

(Translation from Spanish)

<Demographics >

1. Approximately, how old are you?
2. What is your gender?
3. What is your degree on?
4. What is your role and specialization in the organization you work with?
5. How long have you been working in academia?

<Perception>

6. What do you think about the state of practice of cybersecurity in the local financial industry?

<Current situation>

7. How would you rate the level of appropriateness of cybersecurity in the local financial industry? Please use the following scale (*See Appendix M*).
8. What do you think about the level of education in cybersecurity provided to students of CS or CN at this university?
9. How would you rate the level of appropriateness of education in cybersecurity provided to students who graduate from CS or CN at this university?
10. Do you think the university is providing enough graduates with knowledge in cybersecurity?
    The following statement was obtained from the financial industry. Would you rate the level of agreement or disagreement you have with this statement?
    Universities provide insufficient graduates with knowledge in cybersecurity [Financial respondents]

<Factors, barriers>

11. Why do you think financial institutions report problems in finding/hiring professionals with knowledge and training in cybersecurity?
12. What are the factors that prevent this university from providing education in cybersecurity?
13. How would you rate the level of influence of the following factors according to the scale?

<Enhancing education>

14. How many cybersecurity courses does the curriculum incorporate and in which semester?
15. How can the university improve the quality and quantity of educators in cybersecurity?
16. What does this university need in order to design and implement cybersecurity programs aligned with the industry needs?
17. From these initiatives, what do universities should do in the short, medium, and long term?
18. How can we incorporate experts from the industry to join the university to provide knowledge and real-world experience?
19. How would you rate the level of feasibility to teach the following areas of cybersecurity in this university?

<Enhancing training and others>

20. How the university should educate students in cybersecurity, a bachelor in information security or in computer science with knowledge in cybersecurity?
21. What do you think about incorporating foreign guidelines to the Ecuadorian university curricula?
22. What do you think about the effectiveness of professional certification programs?
23. Does this university support professional certification programs in cybersecurity?
24. Do you think that the academia could host a CSIRT to support the financial industry? Why?
25. The following statement was obtained from the financial industry. Would you rate the level of agreement or disagreement you have with this statement? Please explain.

    > *The local academia is not prepared to host a CSIRT because it lacks research capabilities [Financial respondents]*

26. Should the university incorporate cybersecurity content in business programs (e.g., MBA)? Why?

<Closure>

27. Is there any question I did not ask that you would have liked to hear?
28. Do you have any other comments or questions about any topics we covered today?
    Thank you for your time!

Note: to deeply address factors driving cybersecurity education, redundancy was incorporated in several questions on purpose.

Appendix M: Cross-Tabs Answer Sheet

7. Level of Appropriateness of cybersecurity practice in the financial sector

1. Absolutely inappropriate
2. Inappropriate
3. Slightly inappropriate
4. Neutral
5. Slightly appropriate
6. Appropriate
7. Absolutely appropriate

9. Level of appropriateness of education in cybersecurity provided to students who graduate from universities

1. Absolutely inappropriate
2. Inappropriate
3. Slightly inappropriate
4. Neutral
5. Slightly appropriate
6. Appropriate
7. Absolutely appropriate

10. Level of agreement with statement: "Universities provide insufficient graduates with knowledge in cybersecurity"

1. Strongly disagree
2. Disagree
3. Neither agree or disagree
4. Agree
5. Strongly agree

13. Level of influence of the following factors in the current situation

Likert Scale	Low number of professors	Lack of security specialization in professors	Lack of students' interest in cybersecurity	Lack of universities' awareness	Lack of feedback from the industry	Lack of government intervention	Lack of economic resources
1. Not at all influential							
2 Low influence							
3. Slightly influential							
4 Neutral							
5. Somewhat influential							
6. Very influential							
7. Extremely influential							

19. Degree of feasibility to teaching the following areas of cybersecurity in this university

Likert Scale	Secure software coding	Network security	Incident response	Security administration	Security management
1. Absolutely infeasible					
2. No feasible					
3. Slightly infeasible					
4. Neutral					
5. Slightly feasible					
6. Feasible					
7. Absolutely feasible					

25. Level of agreement with: "The local academia is not prepared to host a CSIRT due to lack of research capabilities"

1. Strongly disagree
2. Disagree
3. Neither agree or disagree
4. Agree
5. Strongly agree

Appendix N: Strategies for Capacity Building

This appendix summarizes strategies for capacity building highlighted by the literature from twelve countries, eight of which are developing (Oman, Rwanda, Cameron, Colombia, Uruguay, Chile, Malaysia, India), and four developed (USA, UK, South Korea, Finland). They meet at least one of these criteria: (1) relative high ranking in cybersecurity preparation according to ITU [3] [108] and others indices/models [89], [109], [91], and [110]; (2) good general education; and (3) geographic similarities with Ecuador.

D	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 - Promote 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 to 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	

D: Dimension