JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2018, 1–20
doi: 10.1093/cybsec/tyy002
Research paper

Research paper

Cybersecurity incident response capabilities in the Ecuadorian financial sector

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

[1]Department of Engineering and Public Policy, Carnegie Mellon University, USA and [2]Engineering Department, Universidad Internacional SEK, Ecuador

*Corresponding author: 5000 Forbes Ave., BH 129, Pittsburgh, PA, 15213, USA. Tel: +1 412-268-2672;
E-mail: frankie@cmu.edu; frankie.ec@outlook.com

Received 31 January 2017; revised 28 August 2017; accepted 15 March 2018

Abstract

Cyber-threats have been successfully targeting the financial sector worldwide. While much of the efforts and resources to address the risk imposed by these cyber threats are directed at developed economies, far less attention has been devoted to developing nations. Because many of these nations have modest cyber capabilities, their ability to respond to cyber-attacks can be limited, yet they need to respond to these attacks to protect their critical financial infrastructure.

This study explores the challenges that the Ecuadorian financial industry confronts when dealing with cybersecurity incidents and examines two potential strategies often applied in the developed world—"Computer Security Incident Response Teams (CSIRT)" and "information sharing"—to improve the sector's cybersecurity capabilities to respond to the associated risk. Thirty-three semi-structured interviews with multiple stakeholders (financial security managers and 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 reports on experiences with security incidents, barriers to responding to threats, and stakeholders' desired responses.

We find that the Ecuadorian financial sector already confronts cybersecurity risks, driven by both outsiders and insiders, which result in fraud and operational failures. The sector faces constraints imposed by computer users' lack of awareness, scarcity of financial and technical resources, and challenges imposed by the ecosystem, such as little community support and weaknesses in the legal framework that has only recently been somewhat strengthened. In the pursuit of improvement, stakeholders' postures suggest that there is an opportunity to establish better incident response strategies for the Ecuadorian financial services through the creation of a CSIRT and an information-sharing program. To decrease uncertainty about threats, stakeholders are more likely to share technical information as opposed to quantitative information about security incidents.

Key words: cybersecurity incidents; financial sector; Ecuador; incident response; information sharing; developing nations

Introduction

Many nations recognize that the financial sector as an essential component of their critical infrastructures and economies (see [1] as an example). At the same time, this sector has been repeatedly targeted by cyber attacks with remarkable success. In the USA, widely publicized incidents in the financial and payment services have included data breaches in JP Morgan, Card Services, Target, TJX, and more. Reports by Verizon [2–3] show that relevant threats on the financial sector include Distributed Denial of Service (DDoS) attacks, web attacks, cyber espionage, card skimming, and attacks on point of sale (POS) terminals.

The persistence and sophistication of cyber-attacks has given rise to multiple strategic initiatives for cybersecurity in critical infrastructure

© The Author(s) 2018. Published by Oxford University Press.

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact journals.permissions@oup.com

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

protection (CIP), such as the National Institute of Standards and Technology (NIST) cybersecurity framework, information sharing programs, and other cyber strategies. Worldwide, most advanced nations have adopted similar approaches. To succeed such strategies require a high level of legal, technological, economic development, and a skilled workforce. Unfortunately, developing nations often lack some of these competencies. This can constrain their ability to detect cyber threats and respond appropriately.

If incident response capabilities are to be improved, it is important to understand the types of incidents a critical sector faces and the barriers that prevent stakeholders from appropriately responding. This article 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 Computer Security Incident Response Team (CSIRT) and an information sharing program. We expect that the results of this study will inform courses of action to enhance cybersecurity in this critical infrastructure sector in Ecuador and also in other developing countries facing similar conditions (cultural, economic, demographic) and challenges.

As we detail below, we conducted 33 semi-structured interviews with multiple Ecuadorian stakeholders (financial security managers and security officers, authorities, and managers at Internet service providers). At the time of the interviews, many of the challenges Ecuador faced when responding to cybersecurity incidents were similar to those faced by the financial sector in the developed world. However, there were also some important differences. Attackers used variations of well-known methods (e.g. card skimming and social engineering) to tailor their attacks to computer financial users. Attackers had taken advantage of the opportunities that the domestic financial ecosystem provided them to achieve their goals (e.g. the lack of a cyber crime law and the lack of awareness). Although most of the security incidents reported by respondents in our interviews did not have the sophistication of very aggressive intrusions observed in countries such as the USA, a special case that arose after the interviews, indicates that this is changing. Recently, criminal offenders targeted an Ecuadorian financial institution with the purpose of testing an attack vector (involving malware) that uses the messaging network of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and conducting fraud. This pattern of attack has been also successfully reproduced in Bangladesh and Vietnam [4–5]. Such developments demonstrate that, as in the developed world, cyber threats in the developing world are occurring and causing harm.

When responding to security incidents, stakeholders face barriers that also resemble those faced by developed nations. However, Ecuador confronts additional barriers. Weakness in the legal framework was frequently reported by respondents, as was lack of community support. Internally Ecuadorian financial institutions face constraints due to the limited number of personnel dedicated to security tasks, lack of skilled people, lack of network visibility, and inadequate coordination.

The remaining of this article is organized as follows: 'The Section 'Literature review' reviews related work; The Section 'Method' explains the research method; The Section 'Incidents, attitudes, and approaches' describes stakeholders' experiences with security incidents and their approaches; The Section 'Barriers to incident response' identifies the barriers that stakeholders face; The Section 'Strategies to improve incident response' examines two potential strategies to advance incident response; and The Section 'Discussion and conclusion' discusses the findings and concludes.

Literature review

Literature relevant to this study addresses cybersecurity incidents in the financial sector and cybersecurity research in the critical infrastructure of developing nations.

First, surveys have traditionally been conducted by private and public organizations as a means to learn about security incidents affecting several industries. AT&T, IBM, SANS Institute, Verizon, Center for Internet Security, and security firms typically publish reports describing the trends of cyber-crime incidents, threats, practitioner response strategies, and security investment decisions. Although conflict of interests in non-academic publications can be found (e.g. research to promote sales; see [6]), several industry reports are considered authoritative in certain areas of cyber crime (see [7] citing Verizon as an authoritative source). Other major contributors are government agencies, such as the FBI, the Australian Cyber security Centre, the UK National Cyber Security Centre and more. Many of these studies provide a global perspective that allow us to position risks by types of industry, where the financial services often rank as one of the most targeted sectors by cyber threats.

There have been several recent research initiatives in the financial domain. In a New York State Department of Financial Services (2014) cybersecurity survey [8], 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 Computer Emergency Response Team Coordination Center (CERT/CC) Randazzo et al. (2004, 2005) [9–10] and Cummins et al. (2012) [11] focus on assessing 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) [11].

In the context of cybersecurity in developing countries, prior literature addresses cybersecurity issues in a number of African nations, but in the Americas literature it is very sparse. In the global sphere, a dated International Telecommunication Union report (from 2007) provides an explanatory guide for cybersecurity geared toward developing countries [12]. 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 mentioned, but not seriously addressed.

In Africa, a study by Cole et al. (2008) addresses national cybersecurity practices from a continent perspective [13]. 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. At the time of that review, very few African nations were addressing cybersecurity and, among them, the main focus was mostly legislation related to cybercrime. Most security investments were reported in the private businesses. The report emphasizes the need to improve cybersecurity in Africa. In his CMU Ph.D. thesis, Target (2010) conducts a comparative analysis between two African nations (Rwanda and Tunisia) that investigates the posture of governments regarding cybersecurity threats from a general perspective [14]. The author calls for customized initiatives 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

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

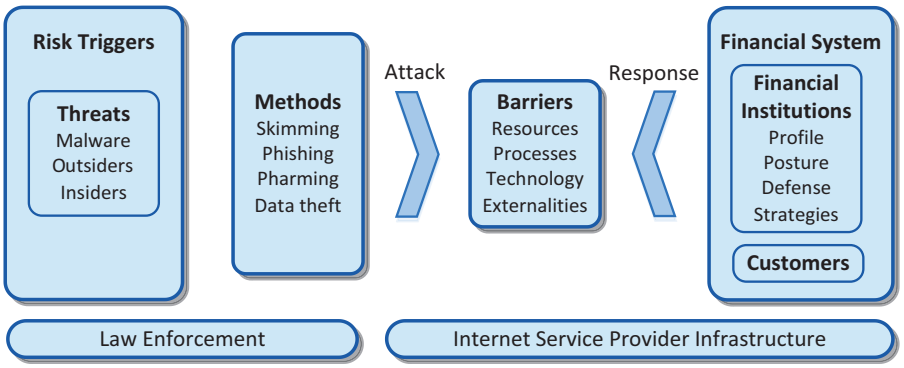

Figure 1: Conceptual framework used to structure this study

nations have higher risk tolerance for cyber-threats than in developed countries. Additionally, in Nigeria, Osho and Onoja (2015) conducted a comparative analysis between the Nigerian National Cyber Security Policy and strategies of other similar and different nations [15]. They found gaps in addressing cybersecurity elements specific to the country's environment.

In the Americas, Newmeyer (2014) conducted a qualitative study to assess the national cybersecurity readiness of Jamaica. This investigator recommends adoption of international best practices [16]. 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 a vision of government supporting the creation of the team in coordination with academia [17]. Similarly, Tunisia is presented as an example of a successful national CSIRT that overcomes resource constraints by using open source tools [18]. In the Latin American context, a report from the Organization of American States (OAS) and Symantec (2014) identifies trends, best practice guidelines for firms, and national efforts toward improving cybersecurity in every country [19]. National cybersecurity posture is described in terms of availability of the following initiatives: a national CSIRT, national cybersecurity governance functions, awareness campaigns, a cybersecurity policy, a program for CIP, and international collaboration capabilities. Further, OAS, the Inter-American Development Bank' and the Global Cyber Security Capacity Center (2016) present cybersecurity initiatives of 32 Latin American and Caribbean nations in the areas of policy and strategy, culture and society, education, legal framework, and technologies. The authors report that the capability to respond to incidents in the region is in early development [20]. Because this report was designed to overview several nations, it does not address any specific critical sector in depth.

In brief, cybersecurity research in financial services has been traditionally 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.

Method

This 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 [21–22]. The goal was to explore the financial stakeholders' experiences with security incidents, to investigate the internal and external limitations they face when handling those incidents, and then to inform strategies for improvement (i.e. a CSIRT and information sharing). Based on these objectives, Figure 1 displays our conceptual framework, which led in turn to our interview guide topics and subsequently to the interview questions. Across sections of the study, we used semi-structured and open-ended questions, cyber-attack scenarios, and printed cross-tabs to elicit responses.

During the interviews, elicitation of security incidents, barriers to respond to security incidents, and preferences regarding CSIRT's attributes were conducted in two stages: (i) spontaneous stage—respondents were asked to tell us about what was already on their minds so that we would not influence their responses; and (ii) guided stage—respondents were presented with a list of choices in order to obtain answers to more specific questions and to capture additional information about a particular topic.

When eliciting security incidents, we started asking open-ended questions about respondents' experiences. This was an opportunity to hear them taking about some incidents and, at the same time, to observe them refraining from speaking about other types of incidents. Next, we presented them with a list of security incidents we had hypothesized were occurring in the financial sector (the sources were local newspapers and the literature) in order to estimate the frequency of incidents occurrence and the level of interviewees' concern. The goal of our approach was to find differences between the two stages of the protocol, and also to collect as much information as possible. Our thesis was that: what was not said in the first stage might come up in the second one, especially because often firms' representatives do not feel comfortable talking about security incidents due to embarrassment and fears of liability [23]. Also, the second stage allowed us to record interviewees' responses in a structured manner by using a Likert scale. Elicitation of barriers to respond to security incidents followed a similar strategy.

We elicited financial stakeholders needs (CSIRT services) and judged relevance (importance of the services) by using the same approach. First, financial respondents spontaneously cited CSIRT services that they desire. Next, respondents were presented with a predefined list of eight CSIRT services, reactive and proactive as defined by CERT/CC in [24], and were asked to assign a *level of importance* using a Likert scale while justifying 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 provided insights on how to prioritize potential services. Moreover, we elicited preferences regarding CSIRT organization, including location, authority, and funding.

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

When eliciting attitudes and preferences regarding information sharing, we supplemented semi-structured with open-ended questions to elicit information needs, willingness to share (WTS), incentives, and metrics for the sharing program. We incorporated two cyber-attack scenarios to assess WTS: "advanced phishing" including malware capabilities (i.e. pharming), and *hacking* of an institution's web server. In this case respondents faced a binary decision, share *versus* do not share, for a specific piece of information involved in a security incident, such as attack vector, impact, vulnerability, and more. In this section on information sharing, we wanted to understand what pieces of information financial stakeholders view as relevant to improving their ability to respond to incidents, what motivations would advocate their participation in an information sharing program, what kind of information they would be willing to share with the financial community, and how they would assess the effectiveness of the information sharing program.

Data collection

Respondents in this study were representatives from financial institutions, government authorities with responsibilities in cybersecurity, Internet service providers (ISPs), and two CSIRTs, one supporting local universities and the other supporting the national telecommunications industry. 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 Chief Information Security Officers, 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 allowed us to perform 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: (i) the size of financial institutions as measured by their number of customers, including large (national coverage), medium, and small size institutions; (ii) the type of financial institutions, such as bank, mortgage institution, credit card institution, and cooperative; (iii) the geographic location of the headquarters of participants' institutions; and (iv) the institution's sector of operations—public and private. Of the 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. Most (31) were conducted in person, one by telephone, and one via voice and video over the Internet. Recordings were allowed for all but two of the interviews. The two exceptions involved authorities. In those cases detailed notes were taken. The average time of all interviews was 87 min (std. dev.: 20.7 min, range: 63–138 min, total: 47.9 h). When potential participants declined to participate, we pursued replacements in other similar institutions. Explanations given by those declining included:

> "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 interviewer and the first author of this article. To ensure accuracy of the data we: (i) used specialized software (F5 Transkript) to assist with transcriptions; (ii) incorporated rules of transcriptions; and (iii) 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.

Data analysis

We conducted a qualitative analysis (category-based analysis) in Spanish, focusing on a thematic analysis as described by Kuckartz (2014) to identify themes related to our research questions [28]. 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 software (Maxqda) 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.

Incidents, 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 standard language (e.g. confidentiality, integrity, and availability) and the 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. Whereas some stakeholders thought that an incident implies an economic or reputational impact, 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 considered this distinction, and adopted Internet Engineering Task Force's (IETF) incident definition specified in the Request for Comments 4949 when eliciting types of incidents. This definition is not substantially different from NIST's definition (in the USA) in the sense that both imply a violation of security rules. IEFT's definition states: "A security event that involves a security violation [29],"

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

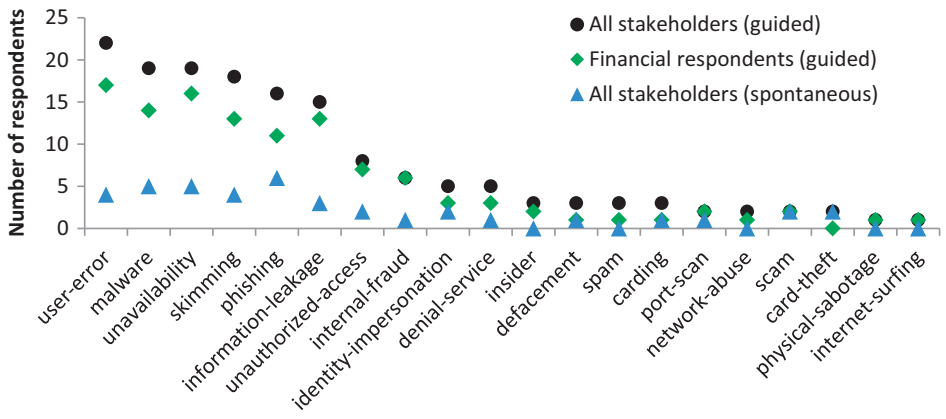

Figure 2: Type of security incidents cited by respondents

"All stakeholders" consider all participants in the study, whereas "financial respondents" (stakeholders) are those whose roles are directly linked to the financial industry (functionaries and authorities). See definitions of security incidents in Appendix A1.

Table 1: Frequency of incidents reported by financial stakeholders

N	Incident\Likert Scale	1	2	3	4	5	6	7	Score[a]
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.
[a]Weighted sum computed as the number of respondents by the Likert scale respectively.

while a security event is "an occurrence in a system that is relevant to the security of the system [29]."

Security incidents

Interviewees narrated security incidents they have been experiencing over the past 4 years as well as consequences (unavailability and fraud). Hence, the collected data are composed of past and current occurrences at the time of the interviews. In specific cases, such as card skimming, respondents made clear that the frequency of occurrence at the time of the interview was changing because the financial sector was implementing smart payment cards, Europay, MasterCard and Visa (EMV). During the transition, some institutions experienced an increase in the number of incidents while others experienced a decrease. Figure 2 reveals two key findings: (i) 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 during guided elicitation; and (ii) there are five major incident types (and the outcome unavailability) that respondents often report, which were confirmed by authorities.

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. These types of incidents are not necessarily exclusive. Table 1 shows the top 10 manifestations of incidents as reported by financial institutions and authorities. In the first row, five stakeholders state that they occasionally see incidents related to users' errors, such as password sharing, data entry mistakes, and falling into social engineering attacks.

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: (i) institution's size measured in number of customers and geographical coverage, (ii) business model characterized by type of financial business, e-commerce capabilities, and (iii) customer market segmentation. Figure 3 shows that both large and small organizations deal with card skimming, whereas phishing appears to be comparatively more serious in large institutions; authorities confirmed that the five local major banks often face phishing that targets customers' e-banking credentials. In the ordinal scale—which was used to protect respondents' privacy—business models of institutions 10 and 11 do not have online banking services.

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 shows that financial respondents are very concerned about incidents that were frequently mentioned, including user error, malware, phishing, and skimming. Nevertheless, respondents are also very concerned about information leakage, which is an incident less often reported. Concern rises because respondents feel they

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

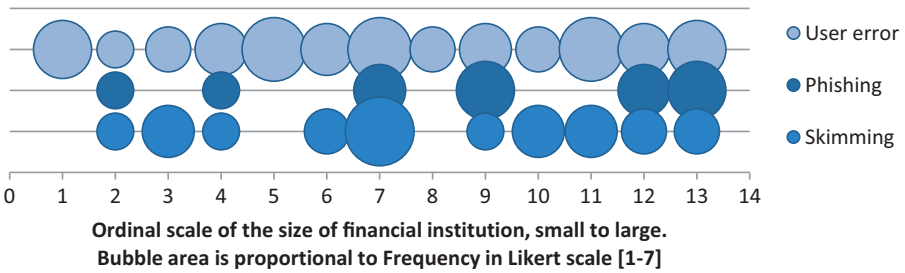

Figure 3: Frequency of incidents by size of institution

Table 2: Level of concern reported by financial stakeholders

N	Incident\Likert Scale	1	2	3	4	5	Score[a]
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.
[a]Weighted sum computed as the number of respondents by the Likert scale.

lack adequate tools to effectively detect and prevent information leakage. Although a number of them have implemented elementary access control schemes (e.g. blocking Universal Serial Bus ports), they admitted uncertainty about detection of data leakage, especially due to lack of visibility in distributed computing 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.

Threat characterization. Financial institutions face threats posed by insiders, outsiders, and even natural hazards. Internally, 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 lead to fraud or failures in confidentiality, integrity, and availability. As seen, "user error" is the most cited source of security incidents and the factor from which most concern arises among financial stakeholders. In this category of incident, respondents related human behaviors affecting information security such as: computer users with high-privileges updating databases by using scripts that contain errors [R1], software coding errors [R25], computer users sharing passwords with co-workers [R11, R12], users facilitating information leakage [R27], failure to follow procedures to authenticate financial customers [R13], entering incorrect (typing error) data in financial applications [R15, R17, R21, R25, R27], and failure to comply with security policies [R16, R33]. Only one financial institution did not label "user errors" related to unintended behaviors, as security incidents, but as a security event.

Beyond user errors, insiders have been detected—eventually with the help of customers—conducting information leakage. An employee which had both a high level of authority and privileged access to financial information operated the most surprising data leaking case. By running SQL queries into a financial database, this actor copied and leaked sensitive information right before leaving his position at a financial institution [R28]. Also, users with regular access have leaked customers' financial data, which subsequently were delivered to other competing financial institutions [R18], and insiders have been detected conducting unauthorized financial transactions that have led to cases of fraud.

In addition, attackers conduct research, obtain partners, develop tools, and perform individual and group focused attacks. 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. Attackers also find partners to facilitate the break-in and materialize a financial gain. Criminal offenders design electromechanical, electronic, cyber tools, and social engineering methods to break into banks' defenses and to take advantage of customers' unawareness. These professional criminals conduct attacks on the cyber financial infrastructure, including card skimmers with relative sophistication (e.g. Bluetooth capabilities). Email scams and phone calls are used in order to impersonate customers to intimidate institutions employees, and initiate unauthorized financial transactions. Tailored malware is employed to stealthily alter the operations of customers' computers (e.g. pharming) and ATMs machines.

Although incidents triggered by natural hazards were reported only once, this type of incidents has an enormous potential to affect availability of IT systems. A flood-related incident involving a datacenter was described to point out that financial institutions have opportunities to improve their physical infrastructure to address natural disasters.

To sum up, financial institutions in Ecuador have to deal with risks resulting from several sources. In Figure 2, one can identify three broad categories of incidents. The first involves unintentional incidents caused by corporate employees, collaborators such as contractors, and financial customers. These incidents are linked to the use of information technology and applying operational procedures to support financial services and interact with them—all types of

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

institutions suffer here. The second category includes adversarial actions motivated by financial gains—card skimming, tailored malware, scams, information leakage and so on. A third category includes adversarial attacks carried due to other motivations, such as recognition and revenge; for instance: defacement and distributed denial of service, respectively. A fourth category—not shown in Figure 2 because of very low frequency of occurrence—comprises natural hazards. Thus, the financial sector not only faces cyber risks but also physical and cyber-physical risks.

Attitudes

Confidence. There were a few cases in which senior stakeholders felt confident enough to talk about additional details of experienced incidents and successful responses. For example, these respondents showed examples of innovative techniques to enhance protection of customer's computers to prevent fraud driven by pharming, and they also talked about practices to conduct advanced investigations in phishing.

Secrecy. A high level of concern for confidentiality was observed when: (i) recruiting participants—it was challenging to obtain respondents, and (ii) interviewing—a respondent explicitly recognized secrecy as an institutional posture, and others cited examples. Authorities have also noticed that some institutions act with reserve when dealing with consequences of phishing attacks to protect their reputation. The following comment illustrates this issue:

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

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 end users' computers. However, the magnitude of concern about malware increases when considering ATM machines as a target.

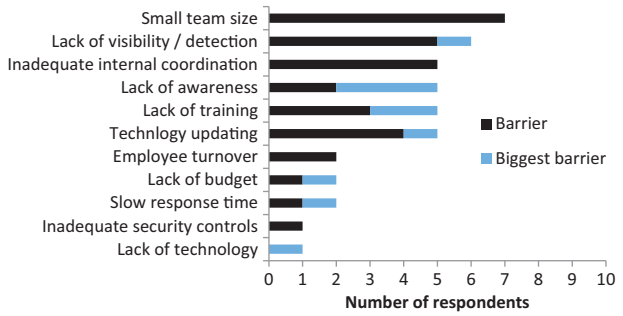

Figure 4: Internal barriers to incident response

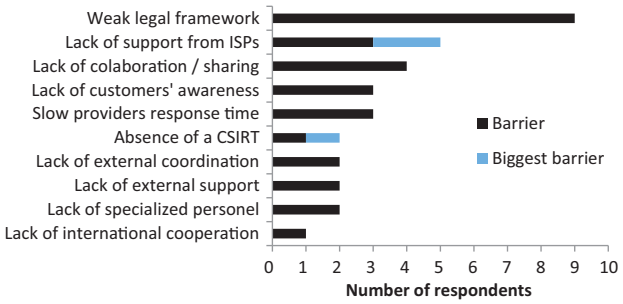

Figure 5: External barriers to incident response

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 security incidents when they suffer negative consequences, so the occurrence of incidents is a powerful instrument of situational awareness, especially when fraud is involved. The same reasoning applies to financial customers. For example, one respondent noted:

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

Ad hoc and formal collaboration. Some stakeholders have developed small, ad hoc circles of trust, in which members collaborate in informal ways. For example, they may share phishing links when they receive them in their inboxes. Furthermore, there is at least one official forum in which institutions formally share information regarding fraud 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 cybersecurity 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]. One respondent (authority) explained:

> "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.

Barriers to incident response

Stakeholders at Ecuadorian financial institutions face barriers that prevent them from properly responding to security incidents. By considering organizational boundaries, Figure 4 and Figure 5 consolidate explicit responses for questions addressing (i) barriers and (ii) the biggest barrier. For instance, lack of "awareness" was cited as a barrier by five participants, three of whom believed it was the biggest barrier. Internally, "small team size" is the most frequently cited barrier and "lack of awareness" is the biggest barrier. Most of the biggest barriers are internal.

Externally, "weakness of the legal framework" was the most frequently reported barrier and "lack of support from ISPs" was emphasized as the biggest barrier by two respondents.

By considering the "risk class" [30] in which these barriers emerge, they can be categorized in four groups: people, processes, technology, and externalities.

People

Lack of awareness. The financial institutions we studied face challenges that lie in at least four of the five "dimensions of awareness" as cited by Siponen, including organizational, institutional education, general public, and socio-political dimension [31]. First, a few executive managers still need to be educated about observing security practices and convinced about the need for investing aspects of security, which directly impact the organization's security posture. For example, one respondent asked:

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

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

Top managers assess the probability of an incident occurrence by using a frequency approach, so it is most likely that they invest in security after an important incident happens. The following is an illustrative exchange:

> "Senior executive E: Why did this event [security 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].

In addition, the financial sector has to deal with security-related human behavior within and outside their borders. Financial employees and other 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. At the same time, general members of the public (i.e. financial customers) 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).

Traditional approaches to delegate security functions to end users encounter two main problems according to Adams and Sasse (1999): (i) lack of security awareness, and (ii) utilization of security means (e.g. passwords) that suffer from usability issues [32]. To address security failures triggered by humans, some have advocated that security awareness training can be a major instrument [33–34]. Stakeholders, however, argue that security awareness is not only challenging to achieve but also insufficient. They report that knowledgeable users have also failed to observe security rules due to lack of concentration when accomplishing security tasks, while others argue that they need authority to enforce security policies through deterrence (i.e. punishment). Two respondents noted:

> "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].

Although insufficient, security awareness is still necessary. Some efforts from Ecuadorian financial institutions to educate the public have been observed. However, the fact that customers still fall into attackers' traps suggests that more public cybersecurity education is needed. One respondent noted:

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

In order to deal with security usability issues, Cranor (2008) argues that systems with automatic and intuitive capabilities that prevent human errors are needed [35], while Sasse et al. (2014) suggests taking measures to minimize the burden that security functions impose on end users, such as consolidating authentication tasks and making them implicit rather than explicit [36].

Lastly, people's behaviors and their abilities to disrupt networks call for legal rules. Yet, stakeholders reported that it was nearly impossible to penalize cyber-criminals (see section Externalities).

Insufficient size of security team. This is the most frequently mentioned internal barrier (by 72% of respondents) among institutions and is driven by budget limitations. Lacking security personnel does not allow managers to implement security capabilities in financial institutions. To overcome limitations and improve response, most institutions establish a temporary and multidisciplinary CSIRT team in the presence of an incident, in which employees across technical and non-technical departments 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 at the national level. 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 [R7, R23].

Processes

Training. High-quality security training is mostly available overseas or provided via international instructors, which increases the cost. Lately, security certifications have started becoming common among some security professionals; however, high costs restrict people's access to those certifications [R20, R28].

> "Obtaining security certifications is very expensive [R20]. Some security certifications, such as CISSP are only available overseas" [R28].

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 response capabilities. Authority and independence of security functions in institutions are needed to balance cybersecurity risks and business objectives, such as business departments pursuing business innovations and profit [R3, R14], as well as IT departments' duties consisting of releasing projects on time and keeping IT operations running [R14, R15, R16].

> "We [security officers] have delays. We want to implement controls to prevent security incidents, but the IT department has other business priorities. They do not process our requirements" [R14].

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). The interviewer had visual access to videos showing attack operations during an interview and pictures of card skimmers in another one. One respondent observed:

> "Watch the video, the criminal has been in the ATM lobby for about 20 min. Where are the security guards?" [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 makers (available overseas) amplifies this limitation. For example:

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

Technology

Technology acquisition. The ability to acquire more advanced technology is limited to organizations with larger 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 associated costs (acquisition, implementation, and operation) exceed the estimations of the risk in several cases.

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

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 in Ecuador were reported to be 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 (e.g. Internetwork Operating System) and hardware (e.g. Dynamic Random Access Memory) upgrades in order to support secure protocols such as Secure Shell.

Externalities

Internet service providers' role. 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. However, financial respondents believe that (i) it is hard to obtain ISPs' security support to respond to incidents, and (ii) the posture of the ISPs regarding incident security support is neither well defined nor communicated. Also, following legal procedures makes it difficult to track and trace an attack locally. 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 current legal procedures. Regarding this concern, ISPs reported that actions across domestic cyberspace networks are governed by the domestic legal framework, which does not allow an ISP to monitor or block customers' traffic. In this specific context, respondents argued 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 cybersecurity regulation in the sector. For example:

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

Cybersecurity regulatory requirements had not been formalized [R5] in the telecommunications sector by the time we conducted the interviews. Now the Ecuadorian telecommunications regulatory agency is working on a draft regulation that will address ISPs' obligations to support their customers in security incidents. 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 about one percent of participations in the local market, and their assessment is that the risk is relatively low [R3, R22]. Nevertheless, even small ISPs can provide an attacker with an entry point into the larger financial ecosystem.

Legal framework. Weakness in Ecuador's legal framework was the most mentioned barrier across all categories and respondent groups. Respondents explained that legislation to effectively punish cybercrime has been absent, and, furthermore, administrative procedures to enforce the law need to be improved. At the time of the interviews, a new legal framework to address some aspects of cyber crime was being enacted in the country. One respondent explained:

> "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 legal action 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 (i) uncover criminals and (ii) 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 [37]. 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 (e.g. the Budapest convention on cybercrime) limits the range of actions that authorities can take to pursue investigation and deterrence [R29]. In this area, the Organization of American States recognizes that Ecuador's ability to strengthen international collaboration in cyberspace needs to be improved [19].

Barriers to respond are summarized in terms of the *risk class* [30] in which they emerge as shown in Table 3.

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 [8]. Table 4 shows a comparison of barriers between Ecuador and the USA and marks similarities with symbols. As seen, there are more similarities than differences. One important difference is in the top ranked barrier for Ecuador (weak legal framework), 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, and different types of institutions face different biggest barriers.

Equivalent symbols at the end of the Ecuadorian barrier and at the beginning of the US barrier indicate similarities. For example, there are circles adjacent to lack of visibility to indicate this is a barrier in both regions. Security team size is linked to lack of sufficient budget because security budget is the primary constraint in Ecuador.

A developed economy seems to attract a 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) [38], Ecuador faces cyber threats that is on its way to enhancing its sophistication. One example cited by respondents is malware attacks to ATMs, and another case recently reported by the international press is malware attack to conduct fraud by using

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

Table 3: 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

Table 4: Comparison of barriers by frequency of mention

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

the SWIFT network [39]. These two cases as well as the ongoing global development of adversarial cyber capabilities [40] suggest that the Ecuadorian financial sector necessitates preparation for even more aggressive attacks than those confronted so far. As part of such an endeavor, financial institutions could benefit from applying models such as the "adversarial capability chain" to support prediction of threats' movements and their proficiencies [40].

Strategies to improve incident response

This section addresses two collective initiatives to enhance incident response. We conduct a preliminary examination of the role and organizational aspects of a financial CSIRT and the feasibility of an information sharing program among local financial institutions.

A financial CSIRT

Supporting the security function of incident response has typically been addressed by specialized teams operated by CERTs, CSIRTs, and security operation centers (SOCs). Although the term CERT is widely used to describe a team that addresses security incidents, it has been suggested CSIRT is a more appropriate term because it intends to cover aspects beyond emergencies [41]. Differences between a SOC and a CSIRT are addressed by Jacobs et al. [42]. Studies on CSIRTs are indeed extensive. At the high level, existing research primarily addresses CSIRTs creation, operation, and improvement. While some studies address aspects related to these three areas together (see [43–44]), other studies focus on one or two areas.

CSIRT creation focuses on establishing CSIRT capabilities [45–46]. Aspects in this area include: (i) the scope of the CSIRT's constituency, which can be institutional, national, regional, and global when considering geographical and organizational borders; Morgus et al. [47] provides an example. This constituency also can be based on the nature of its business or activities, such as financial, government, and educational operations, (ii) level of CSIRT authority over its constituency (no authority, legal authority, shared authority), (iii) organizational and physical location, (iv) category of incident response services, such as reactive, proactive, and security quality management services [43], (v) description of these services [48–49], and (vi) funding.

CSIRT operations concentrates on aspects related to the functioning of the team when managing incidents. This area involves: (i) organizational models for operations, such as centralized, distributed, and coordinating CSIRTs [24], (ii) operational functions related to managing incidents, which include handling, announcement, feedback, interactions, and information handling [43], (iii) requirements and resources such as human capacity [50–51], skills [52], infrastructure [53], and tools, and (iv) legal issues (e.g. cooperation with police investigations) and media relations.

CSIRT improvement brings attention to the effectiveness of CSIRTs' implementations and operations. This area encompasses: (i) assessments or diagnostics of the functioning of the CSIRTs as well as evaluations of the services provided by these teams. Studies in this area address team work performance [51] of the incident management function in achieving its mission and objectives, for which models such as Management Mission Diagnostic [54] and Mission Risk Diagnostic for Incident Management Capabilities [55] have been proposed, (ii) factors driving effectiveness, such as cooperation, information sharing, and trust [56], and (iii) general best and good practices, which include collaboration with internal areas, with third parties, regulatory agencies, and other nations [56–57].

There are just a few studies on CSIRTs operations addressing human and cultural factors. S. C. Sundaramurthy et al. (2014) used an ethnography approach to learn ways to make a private SOC more effective. The investigators immersed themselves in a SOC team to work and closely observed its operations. They found that suitable tools fitting real SOC team members' needs not only

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

improve SOCs efficiency but also help researchers gain trust of the team and therefore advocate their research goals [58]. Similarly, S. C. Sundaramurthy et al. apply the same method to assess operational tasks and strategies in three SOCs, two of which are corporate and one is academic. Areas of analysis include team structure, training methods, workflows, tools, and metrics of productivity. They find differences in structure and workflows, but similarity in the challenge of justifying the SOCs' value to their organizations [59].

Our study mainly concentrates on "CSIRT creation" in a particular geographic environment. As with Sundaramurthy et al. [58–59], our work is also a human-centric study of a CSIRT, but it differs from those in scope, type of audience, and context. First, the constituency of the CSIRT under analysis is a critical infrastructure sector with multiple stakeholders directly and indirectly involved in the functions of responding to security incidents (response, regulation, enforcement). Also, the sample of our study is diverse, including both technical and non-technical participants (security managers, team leaders, engineers) across financial institutions. Third, our study is conducted in a developing nation, which involves an environment with cultural aspects that are different from the developed world.

Overall, the goal of this section of the article is to identify needs, preferences and human attitudes influencing on the success of the CSIRT creation. Because Ecuador currently does not have a national CSIRT, the financial sector lacks external incident response support of such kind. EcuCERT, a Computer Emergency Response Team in Ecuador operating since 2014, mainly focuses its services on the telecommunications sector and certain areas of government [R5]. To address this lack of support, potential services and organizational aspects of a financial CSIRT were discussed during the interviews.

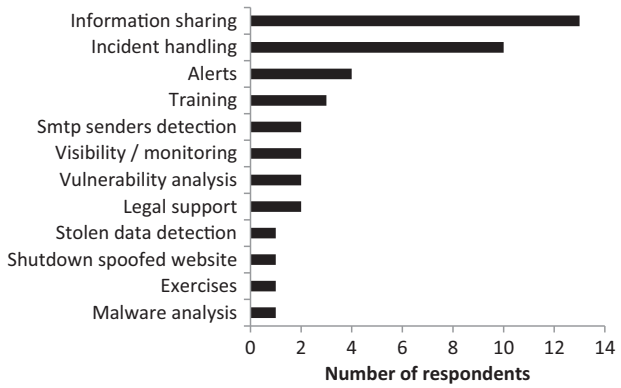

Figure 6: Services brought up by financial stakeholders (spontaneous)

CSIRT capabilities. We elicited external views about the need for security support in two steps. First, financial respondents spontaneously cited CSIRT services that they desire. Figure 6 shows frequency of mentioning, where the most requested service was information sharing.

Subsequently, respondents were presented with a predefined list of eight CSIRT services, reactive and proactive as defined by CERT/CC in [24], and were requested to assign a "level of importance" using a Likert scale while justifying 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. Table 5 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.

***Alerts*—**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" [43]. In the interviews, alerts were linked to having relevant information (e.g. threats) to support the function of incident 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. Thus, respondents' expectations exceed the simple receipt of data on cybersecurity incidents; they want information that meets specific requirements: relevant, actionable, and valuable. These requirements match information's attributes of cyber threat intelligence (CTI) as cited by [60]. Respondents' expectations are also addressed by CTI definitions, such as: "The process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm" [61].

***Incident handling*—**Respondents asked for external 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 to pursue mitigation (e.g. phishing, pharming).

Table 5: Level of importance of CSIRT services (guided)

N	Incident\Likert Scale	1	2	3	4	5	6	7	Score[a]
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.

[a]Weighted sum computed as the of number of respondents by the Likert scale respectively.

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

- *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).

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

Training—This service "involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials" [43]. Areas of desired training include preparation in incident handling, ethical hacking, and digital forensics, and support to educate financial customers. Some participants also wanted to obtain security certifications directly from the CSIRT so as to reduce costs by avoiding commercial intermediaries. For example:

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

Information sharing—Financial respondents' set of descriptions for this service were very close to the service known as "Security-Related Information Dissemination," which "provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security" [43]. Respondents want global and local statistics and patterns about security incidents provided by other participants in the sector. They also want information about successful cases of strategies implemented to mitigate or prevent incidents' impact (e.g. customers' awareness). For example:

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

While both the services "Alert" and "Training" could involve information sharing, these two services could also be offered even without an "information sharing program" in place. Having discussed discrete CSIRT services with respondents allow us to prioritize these services in a granular way. We expand the conceptualization and issues pertaining to information sharing in the sub-section 'Information sharing program'.

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. One respondent asked:

> "If I detect criminals in my infrastructure, should I take a 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 [62]. Interest in this service is raised by the benefit of evaluating the readiness for handling a particular type of incident. Local (non-financial) CSIRTs added that greater benefits could be obtained if exercises are coordinated with them.

Vulnerability analysis—This service "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" [43]. The main focus, however, is not the exploitation (i.e. penetration testing) but rather the assessment of vulnerabilities. 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 on their own showed interest. In general, knowledge about common vulnerabilities being exploited in the local financial sector' infrastructure is most desired. Such information could be included in both "alert" service and "information sharing" service.

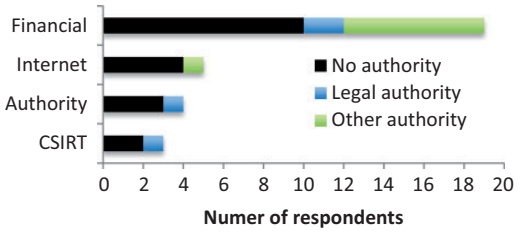

Figure 7: Preference for CSIRT legal authority

Malware analysis—Respondents in large and medium size institutions stated that they already have technical support from antivirus firms, although some interviewees complained about the appropriateness of the providers' response time during technical support. 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.

Lastly, 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.

CSIRT organization. Three organizational aspects to support CSIRT operations were discussed: authority, location, and funding.

Authority—CERT/CC defines authority as: "the control that the CSIRT has over its own actions and the actions of its constituents related to computer security and incident handling activities" [43]. 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"[1]). Figure 7 shows the distribution of preferences by group of stakeholder.

Most financial respondents envisioned a CSIRT with no legal authority that could only recommend and support. This is due to a fear of political influence, aversion to establishing a CSIRT with regulatory power, self-determination about risk decision-making, and trust of constituents. A response from a financial stakeholder was:

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

A second group, mostly non-financial respondents, believed that 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, offering as candidates: government, academia, and the financial industry. Many reported the ideal

1 "If the CSIRT has shared authority, it works with the constituency to influence the decision-making process concerning what actions should be taken" [43].

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

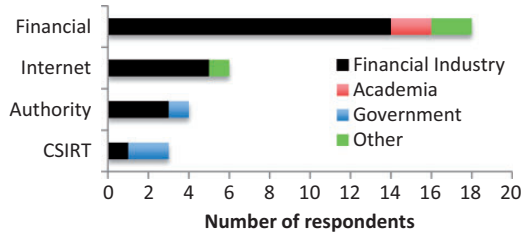

Figure 8: Preference for CSIRT location

option would be academia because a CSIRT needs research capabilities. However, they had concerns about the ability of Ecuadorian universities to address this challenge, including research capabilities and managing financial confidential information. Having a CSIRT in the government raises a major concern among stakeholders because of undesired political influence. Conversely, the financial industry establishing a CSIRT is seen as a pragmatic option due to the sector's risk specialization and, especially, issues surrounding trust. In such a model, financial institutions would be the owners and operators of the CSIRT, so the sector would be responsible for managing and securing the data produced by its services, such as an information sharing program. In this respect, most participants agreed with a model that today is successfully applied by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in the USA; see [63].

When selecting the "financial industry" as the preferred location, respondents of all groups very often linked their choices with the "Association of Ecuadorian Private Banks" as a specific place to locate the financial CSIRT (Figure 8). The problem with this approach, however, is that public financial institutions may not be included. The choice labeled "Other" includes: (i) a hybrid approach between academia and the financial industry, and (ii) a private independent CSIRT. Our analysis indicates that a potential successful model should consider the current synergy and empowerment developed by the "National Financial HUB", which is a private institution handling transactional operations of ATM machines across the nation and is administrated by local financial institutions.

***Funding*—**Most respondents proposed to distribute the CSIRT operational cost among financial institutions in proportion to institutions' number of customers, while a couple of respondents stated 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.

Information sharing program

A centralized information sharing architecture is often discussed as a means to reduce uncertainty about cyber threats [64], and, therefore, to inform cybersecurity decision-making [65]. Approaches to share information include regulatory initiatives,[2] self- and co-regulation,[3] and educational approaches such as cybersecurity training [66]. Globally, these three approaches to promoting information sharing are supported by several governments and specialized organizations that have been established to enable and improve incident response functions. The following paragraphs list the most relevant organizations to our study, some of which have a worldwide scope.

The Anti-Phishing Work Group (APWG) provides a global perspective on phishing and other cybercrime-related events. About 1800 organizations worldwide, including financial institutions, contribute with security-related data. APWG analyzes these aggregated data and distributes trend reports, organizes conferences for cybercrime, and provides public education tools to prevent cybercrime [67].

FIRST (Forum of Incident Response and Security Teams) share best practices, tools, and facilitates information exchange among their members [68]. Although membership procedures seem to follow a restrictive process [69], non-members can also get access to FIRST publications on incident response.

M^{3}AAWG (Messaging, Malware and Mobile AntiAbuse Working Group) is an industry initiative that investigates forms of cyber exploitation (e.g. malware, DDoS) targeting messaging systems and portable platforms. M^{3}AAWG develops educational material, technical best practices, and guidance for policy makers [70].

The NCFTA (National Cyber-Forensics & Training Alliance) is an information sharing organization that concentrates efforts from firms of several industries (e.g. energy, pharmaceutical, telecommunications), US government agencies (e.g. FBI), and academia with the purpose of identifying, mitigating, and neutralizing cyber threats [71]. For instance, NCFTA shares malicious IP addresses and details of spear-phishing emails [72] and provides industry-specific support. The Cyber Financial Program (CyFin) covers cyber threats (e.g. malware, social engineering) to the financial services industry [73]. Because NCFTA is an initiative that feeds the US government with data coming from the industry—without the need of a regulation [72]—it can refrain participation of some US and international actors.

In addition, Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs) are forums advocating partnerships for exchanging relevant information on security threats. ISACs for critical infrastructure include: Electricity Sector ISAC (ESISAC), Telecom ISAC, IT-ISAC, Energy ISAC, and more [74]. Particularly, the Financial Services Information Sharing and Analysis Center (FS-ISAC) was established in 1999 to support banking, finance, and security organizations in the USA [75]. FS-ISAC had expanded operations to cover 72 countries, advised 7000 members as of September 2016 [76], and established partnerships with industry players (e.g. Microsoft) as well as regional organizations, such as the European Threat & Strategy Committee and the European Banking Federation. FS-ISAC provides early warning and expert advice to assists in the protection of critical assets from physical and cyber threats. Disseminated information includes specifics about threats, vulnerabilities, incidents, mitigating measures, and best practices [77]. FS-ISAC is also developing a Security Kit, which is a wiki-based tool that

2 Such as the Cybersecurity Information Sharing Act of 2015 (CISA) in the USA.

3 Co-regulation refers to "a mechanism whereby the legislator entrusts the attainment of specific policy objectives set out in legislation or other policy documents to parties which are recognized in the field (such as economic operators, social partners, non-governmental organizations, or associations)" European Commission, (2015).

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

promises to support small financial institutions with a membership [78]. Here is how a FS-ISAC representative describes the tool.

> "The idea behind the Security Kit was to provide security ideas for our members from security professionals in the financial industry. Periodically, we update the Security Kit when members pose questions about topics that are not in the kit" [FS-ISAC representative].

FS-ISAC advertises global information sharing in its website; nevertheless, we may wonder whether FS-ISAC's scope is effectively global or mostly for the developed-world community. Although membership is now open to financial institutions outside of the USA, institutions with headquarters in a number of countries do not qualify to become members. Such nations include: countries without cybercrime legislation, countries listed on the OFAC database, and countries engaged in terrorism or espionage targeting the USA [63]. If this first exception rule is drastically applied, many countries in the onset of developing legal measures to address cyber crime—which is the case of several developing nations—do not qualify to become members.

Starting on May 2017, a new player in the global ISAC community is the SWIFT ISAC, which is sharing threat intelligence data with the purpose of preventing fraud cases. According to the Society for Worldwide Interbank Financial Telecommunications, these data include "Yara rules, Indicators of Compromise, as well as details on the Modus Operandi used by the cyber-criminals." Members have access to such information in several formats, including PDF, Open IOC, and XML [79].

Additional pertinent sources of threat intelligence include services provided by cybersecurity-related companies (e.g. Crowdstrike, FireEye, Kaspersky), government and regional entities (e.g. FBI, ENISA), cybersecurity professionals (e.g. B. Krebs, B. Schneier), and other public sources (e.g. Spamhaus, SURBL, Shadowserver). In particular, the Spamhaus Domain Block List (DBL) is a database of domains, IPs, and sites related to cyber offenses, including: spam (payload URL, sources, and senders), phishing, and malware [80]. Similarly, the Shadowserver Foundation—composed by volunteers specialists worldwide—obtains security intelligence data "on the darker side of the Internet," according to its website [81].

Participation of Ecuadorian financial institutions in most of these global forums is very rare. During the interviews, none of these supporting organizations' names came up nor did respondents recognized the term ISAC when we explicitly inquired about it. This suggests that none of the financial institutions participating in our study had a FS-ISAC membership. Nevertheless, as stated in the subsection 'A financial CSIRT', many respondents believed information sharing would help improve their ability to respond to incidents.

While several of the global initiatives for threat intelligence are capable of providing very valuable support, there are still reasons that suggest building a local platform for information sharing in Ecuador would be beneficial. First, it has been demonstrated that cyber data intelligence obtained from multiple sources often does not overlap—blacklists constitutes a practical example, so rapidly obtaining shared intelligence from several parties increase the likelihood of establishing effective defenses [82].

Second, although some types of threats are truly global, others may not have high relevance in developing country environments, and some attack vectors may be absent from international data feeds. From our interviews, tailored attacks and banking fraud schemes also develop domestically and systematically replicate to several financial institutions. Thus, having timely and actionable information about these types of threats will increase incident response proficiencies in the Ecuadorian financial industry.

Third, initiatives to develop cybersecurity capabilities can encounter language barriers in some developing countries (see [83]). While FS-ISAC has introduced support in Japanese and Spanish [84], multilingual capabilities among supporting organizations is not very common. A local program could provide related language assistance as well. Therefore, a local Ecuadorian coalition can contribute to address these issues and supplement potential international sources of threat intelligence to provide banks with more relevant (related to the enterprise and environment), actionable (inform a decision), and valuable (contribute to a useful outcome) information [60].

In this section of our study, we provide details on how respondents envision a local information sharing program, including: information needs, respondents' willingness to share information, incentives, and metrics.

Information needs. There is interest in information related to the elements surrounding security incidents, including attack, response, and impact. In order of frequency of mentioning by respondents, the categories of desired data are listed as follows:

- *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.
- *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.

Traditional methods of modeling cyber threats that inform defense initiatives include attack-trees and their multiple variations [85–86], misuse cases [87], risk profiles, as well as security and risk taxonomies [88–89]. In particular, John Howard's work on a taxonomy for computer and networks attacks registered at CERT/CC [90], which was supplemented later in [91], provides a set of terms to analyze security incidents and classify cyber attacks. With the emerging of "advanced persistent threats", new approaches to understand attackers' behavior have also emerged. Lockheed Martin's cyber kill chain (CKC) allows us to recognize the stages taken by advanced adversaries' during cyber intrusions and helps identify discrete attacks connected to intrusive campaigns [92]. The "global adversarial capability chain model" intends to expand the time-frame in which security analysts can investigate and predict adversaries behavior against a particular software system [40]. The *diamond model* for intrusion analysis [93] identifies and analyzes granular, essential elements (e.g. infrastructure, capabilities) as well as characteristics (e.g. methods, resources) of actions that adversaries often take during cyber intrusions. These types of approaches to intrusion analysis can be used together; in fact, the diamond model can supplement kill-chains-based methods such as CKC [94] to provide a deeper insight on each stage of an attack chain.

While these methods support an understanding of the *modus operandi* of attackers, financial stakeholders still sought information related to a typology of threats. We see two plausible explanations, which are not necessarily mutually exclusive. First, stakeholders did not mention terminology associated with any of the models we cited

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

Table 6: WTS of 13 financial institutions' representatives for scenarios P and H

Data Type/WTS		IP Address	Asset type	Attack vector	Malware sample	Mitigation strategy	Qualitative impact	Quantitative impact	Vulnerability
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 targeting institutions' customers. **H**: Web hacking.

above during deep interviews because it is likely that many respondents do not recognize them. Having this kind of knowledge requires training, and this is indeed a local issue that needs to be addressed. Second, cyber criminals have developed customized attack vectors for Ecuadorian financial institutions, and therefore timely information of those types of attacks would assist incident responders more effectively. In fact, customized malware targeting ATMs and financial customers' computers have been detected. Also, cyber criminals have used tailored methods to withdraw money from banking accounts. If information related to these types of attacks had been readily available, fewer financial institutions would have been successfully targeted.

Willingness to share. Although there exists several private and public benefits when firms engage in information security sharing, there are also pragmatic obstacles to overcome. The literature shows that security information sharing can augment firms' profitability and optimize social welfare while increasing the overall level of information security among participants [95–96]. At the same time, security information sharing confronts challenges that undermine its effectiveness, such as: legal liability [97], lack of effective incentives [96], privacy concerns [98], and free riding [99]. Powell (2004) highlights two major failures when sharing information in the financial security market: (i) a firm reports data on a security incident, but the firm receives no compensation. Some firms may keep incident data for themselves that if shared would help other players; and (ii) free riders may wait for other firms to innovate on security defenses in the hope to benefit from such innovations [100]. All of these barriers influence individuals' perception of an information sharing program value, and therefore, impact on their WTS information.

Recent work has addressed WTS to assess implications of data sharing on computer users' privacy. By using data from participants recruited online, J. Bhatia et al. (2016) analyzed the tradeoff between sharing sensitive data and the privacy risk associated with sharing these data. Results show that participants are more willing to share information that could potentially identify them (e.g. IP, address, MAC address) and less prone to share information about their activities online (e.g. browser history, websites visited) [98].

Our study examines how WTS among Ecuadorian financial institutions can be impacted by both the types of security incidents and types of data generated during the course of a security incident. Furthermore, we summarize factors that interviewees think would promote usable information sharing across financial institutions in the Ecuadorian environment.

By using two threat scenarios: advanced phishing including malware capabilities (i.e. pharming), and hacking of an institution's web server, we presented respondents with a binary decision, share *versus* do not share, for a specific piece of information. Phishing targeting financial institutions' customers 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.

The two threat scenarios have similar categories of information, which include details about the attacker (e.g. IP address), the target (e.g. asset type), the response (e.g. mitigation strategy), and the impact of the attack (e.g. quantitative impact). Table 6 reports the preferences of one representative for each financial institution, the most senior in our sample. The column headings show eight components of information generated as a result of an attack, and the rows indicate the counting of a binary outcome representing whether or not stakeholders would share information.

Among our respondents, WTS depended on the type of data involved in attack scenarios. In the case of phishing attacks against customers, respondents are willing to share several types of security incident data, whereas in the hacking case most respondents are willing to share technical information with some restrictions (e.g. details about security equipment). Another 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. This occurs because in this case the vulnerability would be allocated within the banks' infrastructure. In both scenarios, 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]. Thus, different types of incidents and different types of information about incidents lead to different WTS behaviors. Herein, an information sharing initiative should consider that certain types of security incident data would have sharing restrictions and other data types will likely not be shared.

Incentives for information sharing. In the security market, if rational individuals are left to decide, they will choose to share the minimum amount of information [95]. Addressing market failures that discourage information sharing requires incentives mechanisms [96]. Some suggest: establishing a closed group through membership [100], detecting and excluding members who do not share data [101], authenticating and verifying the shared data [99], considering monetary incentives, such as cost savings [102], and promoting fines avoidance. These are some potential strategies that an Ecuadorian information sharing initiative could consider. In our interviews, factors that can incentivize respondents' participation in an information sharing program were explicitly inquired. Here are some themes:

- *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.

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

- *Trust* developed by the program, was cited by respondents as 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 should 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.
- *Accuracy and usability* of the reported information; without these, information reports could be ignored and their value undermined.

Regarding confidentiality, one respondent stated:

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

Participation in an information sharing program can also be encouraged by individuals' perception of the program value, so we elicited ways to measure whether financial functionaries' expectations could be satisfied.

Metrics for the sharing program. Our question addressing ways to assess effectiveness of the information sharing program 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 indicate 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 Organization
- Number of submissions done by financial institutions
- Percentage of financial institutions reporting information
- Improvement in time to respond against fraud

Among all these metrics and measures, impact on reduction of fraud was found to have substantial relevance for financial stakeholders, especially senior respondents. For example:

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

Finally, we asked participants whether the financial CSIRT and a hypothetical institution running the information sharing program—A Financial Security Based Information Sharing Organization (SB/ISO)—should be consolidated or separated. Two thirds of participants stated that these two institutions should be one. Arguments supporting this preference are: centralization of incident response functions, operational resources optimization, avoiding duplication of related cybersecurity efforts in a small country, respondents' inability to identify conflict of functions, and having similar organizational goals for cybersecurity. Conversely, supporters of separating the CSIRT and the SB/ISO based their judgments on: segregation of the CSIRT's and the SB/ISO's functions, segregation of information handled by both organizations, and fears that operational resources of the CSIRT could be diverted by SB/ISO's duties. From these insights, most financial institutions prefer to merge the financial CSIRT and the SB/ISO in a unique organization.

Discussion and conclusion

The Ecuadorian financial services face challenging cybersecurity risks, confronts difficulties to properly respond to those risks (e.g. 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 stresses that those nations marginally experience cyber-attacks [14], our analysis indicates that there are specific critical sectors that do gain attackers attention, and as time passes, more sophisticated attacks across borders are likely to reach domestic financial infrastructures.

In Ecuador, financial institutions confront both internal and external security challenges driven by malicious and benign actors. Internally, user error 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 because of 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. The human factor as a source of incidents (user error) was omnipresent across different type of institutions, both inside and outside of their organizational borders.

Stakeholders adopt a diversity of approaches in defending against these threats, but security incidents still produce harm due to both the existing barriers to respond and attackers' abilities to adapt. Financial stakeholders often face these categories of limitations: financial, technological, administrative, and external barriers imposed by the ecosystem. Most representative barriers are internal, but external barriers still have negative effects. Particularly, the risk of punishment for (cyber) criminals was very low due to a lack of legal deterrence. For this reason attackers feel motivated by the potential gains that come with minimal risk [103]. Although no single doctrine, such as accountability, may be effective to ensure cybersecurity [104], our work supports the belief that law enforcement is an essential element to mitigate the risk of cyber-physical threats [14]. By the time of finishing the interviews, Ecuadorian authorities updated the law to specifically include several forms of cybercrime. Future work should evaluate effectiveness of such enacting.

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 who develop tools and techniques to protect the financial system. Such tools and defenses have an expiration time, which is a function of the attackers capabilities to research and undermine such protection means. Unfortunately, not all institutions have the capabilities to keep up with the attackers adaptation to prevent their success.

Regarding mitigation strategies, our work takes a first step in assessing how collaborative functions of incident response capabilities could work in the Ecuadorian financial community. The results with respect to a specialized Financial CSIRT security services indicate that

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

alerts, incident handling, information sharing, and training as services are all desired and would be most welcome. Organizationally, respondents agreed that currently the best place to establish the CSIRT is the financial industry because of the sector's specialized knowledge about risk and trust when handling confidential information. Conversely, fear of political influence (recognized even by some authorities) and lack of cybersecurity research capabilities stand as arguments against establishing the CSIRT in the government or in the academia respectively. We believe that a potential successful model should consider establishing incident response capabilities at the *National Financial HUB* handling transactional operations of ATMs in Ecuador, especially due to the current synergy and empowerment already developed by this entity. Further discussion incorporating views of additional financial institutions is necessary to define the type of CSIRT authority.

Our assessment of willingness to share suggests that financial stakeholders may be prepared to share technical details of incidents depending on the types of incident and types of information involved in the incident. 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 four cities of Ecuador, 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 both commonality and differences with the results of a survey study conducted with the financial services in the USA [8]. 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: small size of their security teams (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 this top four barriers and one marked difference. We believe that the difference can be mostly explained by: (i) motivations that make the USA an attractive target for sophisticated adversaries, such as large-scale information, substantial monetary gains, and geopolitical incentives, and (ii) the difficulties found by Ecuadorian stakeholders when internally coordinating cybersecurity operations with IT departments [R28, R31].

As stated by Hutchings and Holt (2016), responsibility for strategies to develop crime prevention not only resides with organizations trying to protect themselves, but also with additional stakeholders [105]. While some strategies to respond to incidents involving cyber crime activity (e.g. exfiltration of financial data) must be taken by financial institutions, other measures need to be taken by users (e.g. developing awareness of cyber fraud methods) and, of course, by public policy and lawmakers (e.g. measures of deterrence). Ecuador needs to advance in such direction as well.

This work contributes to the literature of cybersecurity incident response in the context of developing countries and is, to our knowledge, 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 [14–16], and building national cybersecurity response teams [17–18], but none of them concentrates analysis on a specific critical infrastructure sector in depth. Additionally, this study collects and reports data by using cyber-security scenarios from Latin American financial institutions and elicits willingness to share in a systematic way.

Ultimately, insights from this work should 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

This work benefited from the contribution of the late Howard Lipson. We also thank the feedback from Gabrielle Wong-Parodi, Lorrie Cranor, Jon Peha, and Casey Canfield for feedback in regard to interview questions. We thank all of the anonymous respondents from Ecuadorian financial institutions, authorities, and CSIRTs for their participation in this study.

Funding

This work was supported by the Department of Engineering and Public Policy at Carnegie Mellon University as well as from M. Granger Morgan's and Douglas C. Sicker's faculty-discretionary funds. Frankie Catota also received support from the Fulbright-Senescyt Program.

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

Appendix A1: Terms

Term	Definition	Source
Carding	Unauthorized use of credit and debit card account information to fraudulently purchase goods and services.	Peretti K, 2008
Defacement	Web defacement is the act of altering the contents of a web site with malicious intent, sometimes associated with vandalism and sabotage.	Cooks A, Olivier M, 2004
Information leakage	Data loss. The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.	NIST SP 800-16
Insider	Malicious insider. A current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.	CERT, 2009
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
Skimming	Card 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.	NIST 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.	NIST SP 800-61
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.	NIST 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
User error	Human error. Failure in human performance by an unintentional insider threat. Conditions that contributed to errors and adverse outcomes are: employee readiness, work planning and control, work setting, and data flow.	CERT, 2013

References

1. The White House, Office of the Press Secretary, Presidential Policy Directive – Critical Infrastructure Security and Resilience, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (19 August 2017, date last accessed).
2. Verizon, 2016 Data Breach Investigations Report, 2016.
3. Verizon, 2017 Data Breach Investigations Report, 2017.
4. Bloomberg, *Ecuador Bank Says It Lost $12 Million in Swift 2015 Cyber Hack*, 2016. https://www.bloomberg.com/news/articles/2016-05-20/ecuador-bank-says-it-lost-12-million-in-swift-2015-cyber-hack (18 March 2018, date last accessed).
5. Trend Micro, *High-Profile Cyber Theft Against Banks Targeted SWIFT Systems*, 2016. http://blog.trendmicro.com/trendlabs-security-intelligence/high-profiled-cyber-theft-against-banks-targeted-swift-systems (11 July 2017, date last accessed).
6. Scientific American, *Crime Ring Revelation Reveals Cybersecurity Conflict of Interest*, 2014. https://www.scientificamerican.com/article/crime-ring-revelation-reveals-cybersecurity-conflict-of-interest/ (2 May 2017, date last accessed).
7. Tehan R. Cybersecurity: Authoritative Reports and Resources. Library of Congress, 2012.
8. New York State Department of Financial Services. Report on Cyber Security in the Banking Sector, 2014.
9. Randazzo M, Keeney M, Kowalski E, *et al*. *Insider threat study: illicit cyber activity in the banking and finance sector*. Carnegie Mellon University, Software Engineering Institute, 2004.
10. Randazzo M, Keeney M, Kowalski E, *et al*. *Insider threat study: illicit cyber activity in the banking and finance sector*. Carnegie Mellon University, Software Engineering Institute, 2005.
11. Cummings A, Lewellen T, McIntire D, *et al*. *Insider threat study: illicit cyber activity involving Ffaud in the US financial services sector*. Carnegie Mellon University, Software Engineering Institute, 2012.
12. International Telecommunication Union (ITU). Cybersecurity guide for developing countries, 2007.
13. Cole K, Chetty M, LaRosa, *et al*. Cybersecurity in Africa: an assessment, ResearchGate, 2008.
14. Target AC. Cybersecurity challenges in developing nations. PhD Thesis. Department of Engineering and Public Policy, Carnegie Mellon University, 2010.
15. Osho O, Onoja A. National cyber security policy and strategy of Nigeria: a qualitative analysis. *Int J Cyber Criminol* 2015; **9**:120–43.
16. Newmeyer K. Cybersecurity strategy in developing nations: a Jamaica case study. PhD Thesis. Walden University School of Public Policy and Administration, 2014.

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

17. Software Engineering institute CERT. *Colombia Case Study*. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484981 (18 March 2018, date last accessed).
18. Software Engineering institute CERT. *Tunisia Case Study*. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484985 (18 March 2018, date last accessed).
19. Organization of American States, Symantec. Latin American Security + Caribbean Cybersecurity Trends, 2014.
20. Organization of American States and Inter-American Development Bank, Cybersecurity. Are we ready in Latin America and the Caribbean? 2016.
21. Galletta A. *Mastering the SemiStructured Interview and beyond: From Research Design to Analysis and Publication*. New York: New York University Press, 2013.
22. Adams A, Cox A. Questionnaires, in-depth interviews and focus groups. In: Cairns P, Cox A (eds). *Research Methods for Human Computer Interaction*. Cambridge, UK: Cambridge University Press, 2008, 17–34.
23. Hoo KJ. *How much is enough? A risk management approach to computer security*. Stanford University, 2000.
24. Killcrece G, Kossakowski K, Ruefle R, *et al*. Organizational models for computer security incident response teams (CSIRTs), Carnegie Mellon University, Software Engineering Institute, 2003.
25. Patton M. *Qualitative Evaluation and Research Methods*. Beverly Hills, CA: Sage, 1990, 169–186.
26. Van Maanen J. The fact of fiction in organizational ethnography. *Adm Sci Q* 1979; **24**:539–50.
27. Shenton A. Strategies for ensuring trustworthiness in qualitative research projects. *Educ Information* 2004; **22**:63–75.
28. Kuckartz U. *Qualitative Text Analysis: A Guide to Methods, Practice and Using Software*. London: Sage, 2014.
29. Shirey R. Internet security glossary. Version 2, RFC 4949, 2007.
30. Cebula J, Young L. *A taxonomy of operational cyber security risks*. Carnegie Mellon University, Software Engineering Institute, 2010.
31. Siponen M. Five dimensions of information security awareness. *Comput Soc* 2001; **31**:24–29.
32. Adams A, Sasse MA. Users are not the enemy. *Commun. ACM* 1999; **42**: 40–46.
33. Talib S, Clarke N, Furnell S. An analysis of information security awareness within home and work environments. In: *International Conference on Availability, Reliability, and Security (ARES), Krakow, Poland*, 2010. pp. 196–203. IEEE.
34. European Union Agency for Network and Information Security. The new users' guide: How to raise information security awareness, 2010.
35. Cranor LF. A framework for reasoning about the human in the loop. In: *Proceedings of the 1st Conference on Usability, Psychology, and Security, (UPSEC '08). Berkeley, CA, USA*, 2008. p. 1–15. USENIX Association.
36. Sasse MA, Steves M, Krol K, *et al*. The great authentication fatigue–and how to overcome it. In: *International Conference on Cross-Cultural Design. Crete, Greece*, 2014. p. 228–39. Springer.
37. Hare F. The cyber threat to national security: why can't we agree? In: *Conference on Cyber Conflict*, Tallinn, Estonia, 2010. pp. 211–225, CCD COE Publications.
38. Morgan's Cyber Attack: How The Bank Responded. *The Wall Street Journal*. http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded (20 August 2017, date last accessed).
39. Now It's Three: Ecuador Bank Hacked via Swift. *The Wall Street Journal*. http://www.wsj.com/articles/lawsuit-claims-another-global-banking-hack-1463695820 (19 May 2016, date last accessed).
40. Spring J, Kern S, Summers A. Global adversarial capability modeling. In: *eCrime Res. Summit*, 2015, pp. 1–21. Anti-Phishing Working Group. IEEE.
41. Internet Governance Forum. Best practice forum on establishing and supporting computer security incident response teams (CSIRT) for internet security, 2014.
42. Jacobs P, von Solms S, Grobler M. E-CMIRC: towards a model for the integration of services between SOCs and CSIRTs. In: *15th European Conference on Cyber Warfare and Security*, (*ECCWS2016*), 2016. p. 350. Academic Conferences and publishing limited.
43. West-Brown M, Stikvoort D, Kossakowski K, *et al*. Handbook for computer security incident response teams (CSIRTs), Carnegie Mellon University, Software Engineering Institute, 2003.
44. Maj M, Reijers R, Stikvoort D. Good practice guide for incident management, European network and information security agency (ENISA), 2010.
45. Haller J, Merrell S, Butkovic M, *et al*. Best practices for national cyber security: building a national computer security incident management capability, Version 2. Carnegie Mellon University, Software Engineering Institute, 2010.
46. Mooi R, Botha RA. Prerequisites for building a computer security incident response capability. In: *Information Security for South Africa (ISSA)*, 2015. pp. 1–8. IEEE.
47. Morgus R, Skierka I, Hohmann M, *et al*. National CSIRTs and their role in computer security incident response. New America, 2015.
48. Ruefle R, Van Wyk K, Tosic L. *New Zealand security incident management guide for computer security incident response teams (CSIRTs)*. Developed in cooperation with the CERT Division of the Software Engineering Institute at Carnegie Mellon University, 2013.
49. Bronk H, Thorbruegge M, Hakkaja MA. Step-by-step approach on how to set up a CSIRT. European Network and Information Security Agency (ENISA). 2006.
50. Sawicka A, Gonzalez JJ, Qian Y, Managing CSIRT. Capacity as a renewable resource management challenge: an experimental study. In: *23rd International Conference of the System Dynamics Society*, 2005.
51. Wiik J, Gonzalez JJ, Kossakowski KP. Limits to effectiveness in computer security incident response teams. In: *23rd International Conference of the System Dynamics Society*. Boston, MA, 2005.
52. Mclaughlin M, Arcy JD, Cram WA, *et al*. Capabilities and skill configurations of information security incident responders. In: *50th Hawaii International Conference on System Sciences*, 2017. pp. 4918–927.
53. Penedo D. Technical infrastructure of a CSIRT. In: *International Conference on Internet Surveillance and Protection, (ICISP'06)*, 2006. p. 27. IEEE.
54. Dorofee AJ, Killcrece G, Ruefle R, *et al*. *Incident management mission diagnostic method, Version 1.0*. Carnegie Mellon University, Software Engineering Institute, 2008.
55. Alberts C, Dorofee A, Ruefle R, *et al*. *An introduction to the mission risk diagnostic for incident management capabilities (MRD-IMC)*. Carnegie Mellon University, Software Engineering Institute, 2014.
56. Bada M, Creese S, Goldsmith M, *et al*. *Improving the effectiveness of CSIRTs. Global cyber security capacity centre*. University of Oxford, 2014.
57. Organization of American States (OAS). Best practices for establishing a national CSIRT, 2016.
58. Sundaramurthy SC, McHugh J, Ou XS, *et al*. An anthropological approach to studying CSIRTs. *IEEE Security & Privacy* 2014; **12**:52–60.
59. Sundaramurthy SC, Case J, Truong T, *et al*. A tale of three security operation centers. In: *ACM Workshop on Security Information Workers (SIW '14)*, 2014. pp. 43–50.
60. Dalziel H. *How to Define and Build an Effective Cyber Threat Intelligence Capability*. Waltham: Syngress, 2014.
61. Intelligence Defined and its Impact on Cyber Threat Intelligence. http://www.robertmlee.org/tag/cyber-threat-intelligence. (2 August 2017, date last accessed).
62. Grance T, Nolan T, Burke K, *et al*. Guide to test, training, and exercise programs for IT plans and capabilities. NIST Special Publication 800-84, 2006.
63. FS-ISAC. Financial services information sharing and analysis center - Operating Rules, 2016.
64. Johnson C, Badger L, Waltermire D. Guide to cyber threat information sharing. NIST Special Publication 800-150, 2014.
65. Bipartisan Policy Center. Cyber security task force: public–private information sharing, 2012.
66. ENISA. *Cyber security information sharing: an overview of regulatory and non-regulatory approaches*, 2015. https://www.enisa.europa.eu/pub

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018

lications/cybersecurity-information-sharing (5 August 2017, date last accessed).
67. Anti-Phishing Working Group. *About APWG*. https://www.antiphishing.org/about-APWG/APWG/ (15 July 2017, date last accessed).
68. Forum of Incident Response and Security Teams. *FIRST vision and mission statement*. https://www.first.org/about/mission (15 July 2017, date last accessed).
69. Forum of Incident Response and Security Teams. *Information exchange policy*. https://www.first.org/iep/ (15 July 2017, dtae last accessed).
70. Messaging, Malware and Mobile Anti-Abuse Working Group. *Why M3AAWG?* https://www.m3aawg.org/about-m3aawg (15 July 2017, date last accessed).
71. National Cyber-Forensics & Training Alliance. *NCFTA in the News*. https://www.ncfta.net/Home/News. (15 July 2017, date last accessed).
72. Forbes. *The FBI workaround for private companies to share information with law enforcement without CISPA*. https://www.forbes.com/sites/kashmirhill/2012/04/26/the-fbi-workaround-for-private-companies-to-share-information-with-law-enforcement-without-cispa/#74c49d805009 (18 March 2018, date last accessed).
73. National Cyber-Forensics & Training Alliance. *The Cyber Financial Program*. https://www.ncfta.net/Home/Cyfin (15 July 2017, date last accessed).
74. ISAC Council. Reach of the Major ISACs, 2004.
75. Eckert S. Protecting critical infrastructure: the role of the private sector. In: Dombrowski P. (ed.). *Guns and Butter: The Political Economy of International Security*. Boulder, CO: Lynne Rienner Publishers, 2005.
76. FS-ISAC. *European banking federation and the financial services information sharing and analysis center (FS-ISAC) partner on trans-Atlantic initiative to fight cyber crime*, 2016. https://www.fsisac.com/article/european-banking-federation-and-fs-isac-press-release (9 August 2017, date last accessed).
77. FS-ISAC. *Mission statement*. https://www.fsisac.com/about/mission (9 August 2017, date last accessed).
78. FS-ISAC. *FS-ISAC monthly newsletter February 2017*. https://www.fsisac.com/article/fs-isac-member-newsletter-february-2017 (9 August 2017, date last accessed).
79. SWIFT. *SWIFT launches the SWIFT Information Sharing and Analysis Centre*. https://www.swift.com/news-events/news/swift-launches-the-swift-information-sharing-and-analysis-centre (9 August 2017, date last accessed).
80. Spamhaus. *Frequently asked questions*. https://www.spamhaus.org/faq/section/Spamhaus DBL (9 August 2017, date last accessed).
81. Shadowserver. *Welcome to Shadowserver*. https://www.shadowserver.org/wiki/ (9 August 2017, date last accessed).
82. Metcalf L, Spring JM. Blacklist ecosystem analysis - spanning Jan 2012 to Jun 2014. In: *2nd ACM Workshop on Information Sharing and Collaborative Security*, 2015. pp. 13–22. ACM.
83. Catota FE. Cybersecurity capabilities in a critical infrastructure sector of a developing nation. PhD. Thesis. Engineering and Public Policy Department, Carnegie Mellon University, 2016.
84. FS-ISAC. FS-ISAC Expands Global Operations, 2015.
85. Schneier B. Attack trees - modeling security threats. *Dr. Dobb's J* 1999.
86. Kordy B, Piètre-Cambacédès L, Schweitzer P. DAG-based attack and defense modeling: don't miss the forest for the attack trees. *Comput Sci Rev* 2014; **13–14**:1–38.
87. Sindre G, Opdahl AL. Eliciting security requirements with misuse cases. *Requir Eng* 2005; **10**:34–44.
88. Hansman S, Hunt R. A taxonomy of network and computer attacks. *Comput Secur* 2005; **24**:31–43.
89. Cebula JJ, Popeck ME, Young LR. *A taxonomy of operational cyber security risks version 2*. Carnegie Mellon University, Software Engineering Institute, 2014.
90. Howard JD. An analysis of security incidents on the internet. PhD. Thesis. Engineering and Public Policy Department, Carnegie Mellon University, 1997.
91. Howard JD, Longstaff TA. *A common language for computer security incidents*. Sandia National Laboratories, 1998.
92. Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *6th Annu Int Conf Inf Warf Secur* 2011; **1**:80.
93. Caltagirone S, Pendergast A, Betz C. The diamond model of intrusion analysis. center for cyber intelligence analysis and threat research, 2013.
94. Activeresponse. Diamond model or kill? http://www.activeresponse.org/diamond-model-kill-chain/ (11 August 2017, date last accessed).
95. Laszka A, Felegyhazi M, Buttyan L. A survey of interdependent information security games. *ACM Comput Surv (CSUR)* 2015; **47**:1–38.
96. Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: an economic analysis. *J Account Public Policy* 2003; **22**:461–85.
97. Nolan A. *Cybersecurity and information sharing: legal challenges and solutions*. Congressional Research Service, 2015.
98. Bhatia J, Breaux TD, Friedberg L, *et al*. Privacy risk in cybersecurity data sharing. In: *ACM on Workshop on Information Sharing and Collaborative Security, Vienna, Austria*, 2016. pp. 57–64.
99. Gal-Or E, Ghose A. The economic incentives for sharing security information. *Inf Syst Res* 2005; **16**:186–208.
100. Powell B. Is cybersecurity a public good? Evidence from the financial services industry. *J Econ Pol* 2005; **1**:497.
101. Tullock G. Adam Smith and the prisoners' dilema. *Q J Econ* 1985; **100**:1073–81.
102. Robinson N, Disley E. Incentives and challenges for information sharing in the context of network and information security. European Network and Information Security Agency (ENISA), 2010.
103. Lampson BW. Computer security in the real world, Microsoft Research, 2004.
104. Mulligan K, Schneider B. Doctrine for cybersecurity. *Daedalus* 2011; **140**:70–92.
105. Hutchings A, Holt TJ. The online stolen data market: disruption and intervention approaches. *Glob Crime* 2016; **18**:11–30.

Downloaded from https://academic.oup.com/cybersecurity/advance-article-abstract/doi/10.1093/cybsec/tyy002/4990518
by guest
on 02 July 2018