The African Journal of Information Systems

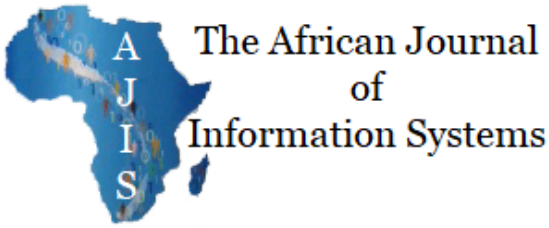
Volume 12 | Issue 2 Article 1

July 2020

A Coordinated Communication & Awareness Approach for Information Security Incident Management: An Empirical Study on Ethiopian Organizations

Keshnee Padayachee
University of South Africa, padayk@unisa.ac.za

Elias Worku
Addis Ababa University, elias.worku@aau.edu.et



A Coordinated Communication & Awareness Approach for Information Security Incident Management: An Empirical Study on Ethiopian Organizations

Research Paper

Volume 12, Issue 2, July 2020, ISSN 1936-0282

Keshnee Padayachee
University of South Africa
padayk@unisa.ac.za

Elias Worku
University of South Africa (PhD Student)
Addis Ababa University
elias.worku@aau.edu.et

(Received May 2019, accepted April 2020)

ABSTRACT

The coordination of communication and awareness efforts in the process of Information Security Incident Management (ISIM) has been identified as a critical means of enhancing information security protection in organizations. This paper aims to explore the nuances of organizational information security with respect to the coordination of communication and awareness efforts among organizational stakeholders towards achieving a shared, interactive, and participatory ISIM. According to the findings of the study in the organizations sampled, it has been identified that reporting, communication, and awareness efforts within ISIM were found to be largely uncoordinated. The exploratory findings provided a rationale for the proposal of a conceptual model. The model would unify and subsume situational awareness and interactive modes of communication toward improving the coordination of awareness and communication efforts among stakeholders in the management of information security incidents.

Keywords

Information Security, Incident Management, Situational Awareness, Incident Reporting, Interactive Model of Communication.

INTRODUCTION

The contemporary large-scale interconnection of computers and cyber-data exchanged globally has created an enormous threat to organizations in safeguarding information security, and the proliferation of cyber security incidents is rife. Threats can come both externally and internally (i.e., from insiders) (Syahrial et al., 2019). A report on 86 global companies commissioned by IBM Security (2019) found that malicious cyber-attacks surged to 51% in 2019, and the longer an organization takes to contain and manage a threat, the more prohibitively expensive it becomes. Moreover, lengthy downtimes can cause reputational risks to an organization (Metzger et al., 2011). The study also found that the time taken to contain incidents has grown by 4.9% and that the cost of breaches that were not contained within 200 days rose to $4.56 million. Therefore, uncoordinated and unsupported management of information security incidents has created significant concern among organizations irrespective of their scope, mission, setting, or type (Ahmad et al., 2012; Johnson, 2006).

Nyman and Große (2019) purport that the high levels of information security incidents demand a formalized incident management process and call for more empirical research to be conducted to guide information security incident management in practice. Ab Rahman and Choo (2015) reason that while incident management is a mature field, there is a lack of consistency with respect to describing incident management and response in the literature. They found that less than 10% of the research conducted involves incident reporting and prioritization (2010-2015). Yohannes et al. (2019) conducted a case study on a financial institution in Ethiopia from an information security incident management perspective in response to the dearth of studies in this context. They found the lack of standardized processes and issues of collaboration, communication, and awareness to be problematic and argued for more studies to be conducted within various organizations in Ethiopia. Consequently, the aim of this study is to explore nuances of organizational information security with respect to the coordination of communication and awareness efforts among organizational stakeholders towards achieving a shared, interactive, and participatory Information Security Incident Management (ISIM) process. This prompted the following research question (RQ): *How do organizations effectively coordinate communication and awareness efforts in ISIM*? The minor research questions that guided the study are: (1) How do organizations integrate communication and awareness efforts into their ISIM policies and practices? (2) To what extent is the integration and stakeholder participation implemented in the process of incident communication and awareness efforts within ISIM processes? and (3) How can organizations enhance the coordination of communication and awareness efforts within the processes of ISIM practice?

ISIM strives to address technical issues such as inquiry, containment, and recovery. It aims at preventing incidents from a management perspective in which planning, detection, reporting, assessment, response, and lessons learned are crucial processes of ISIM (Tøndel et al., 2014). The effective coordination of awareness and communication strategies within ISIM can contribute greatly in mitigating existing and future incidents (ISO/IEC 27035-1:2011, 2011). There have been calls for more studies to explore why ISIM is so challenging (Tøndel et al., 2014). Some of the challenges include lack of documentation, lack of training, lack of planning, misunderstandings between security and control personnel, lack of post-incident evaluations, and the difference of priorities and perspectives between managers and technical personnel (Bartnes et al., 2016b). Some other challenges include gaining senior management commitment, involving all employees, the usability issues of technical tools, incident registration, and collaboration (Line & Albrechtsen, 2016).

The management of information security incidents is indeed challenging, as it involves both technical and social aspects (Ahmad et al., 2012). As a result, an integrated approach encompassing human, organizational, technical, and behavioral factors to information security is crucial to containing

information security threats in a coordinated way. Although some organizations have been utilizing some standards of ISIM, the need to integrate communication and awareness schemes is not well understood and thus inhibits proactive ISIM. Bartnes et al. (2016b) maintain that there is a need for further research that details how communication and collaboration among stakeholders within ISIM occurs in practice. Similarly, Ahmad et al. (2015) argue that there is a paucity of research that considers how the experiences of incident response teams can be used towards improving security processes, and most studies focus on the response part of the process and do not consider the "lessons learned" aspect. Clearly, the lessons learned from previous incidents can be useful only if there is an effective coordination of communication and awareness efforts. This study will explore how communication and awareness efforts are coordinated in practice within several Ethiopian organizations. This will assist in documenting the experiences of ISIM which will be used as a rationale towards developing a conceptual model as an ancillary aim.

The remainder of the paper is organized as follows: the second and third sections explicate the related works and the research methodology, respectively. The fourth and fifth sections provide an analysis of the findings and the discussion of the findings, correspondingly. The sixth section presents the conceptual model. The study limitations, contribution to knowledge, and areas of further research conclude the paper.

LITERATURE REVIEW

An information security incident is defined as "a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (ISO/ IEC 27035:2016, 2016). The goals and activities of ISIM processes are to neutralize the incidents while reducing the damages (Ani & Agbanusi, 2014). Ani and Agbanusi (2014), who conducted a systematic overview of the various frameworks proposed towards ISIM, identified the following similarities among the various approaches:

- Preparation – organizational readiness for incidents which involve training, policies, preventative security mechanisms (e.g. firewalls, backup and recovery software, logs), and a well-defined plan.
- Detection – a system for reporting incidents.
- Formulation of response strategy/planning – identifying the most suitable approach for handling the incident via analysis and collaborating with appropriate stakeholders.
- Containment/preservation – development of a strategy to prevent further damage to the system, such as disabling services.
- Eradication – a long-term solution to eliminating the threat; for example, a policy update.
- Recovery – restoring the system back to normal working order.
- Lesson Learned/Reporting/Follow-Up and Incident Closure – learning from the incident to prevent future similar incidents.

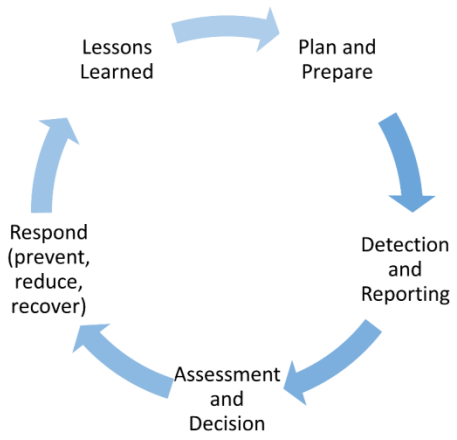


Figure 1. Information Security Incident Management Event Flow Diagram
(adapted from [ISO/IEC 27035-1:2011, 2011])

The ISO/IEC 27035 standard, which is the most recognized organizational security standard (Tøndel et al., 2014), covers the processes for handling information security incidents and vulnerabilities. As depicted in Figure 1, the process of managing an information security incident follows a cyclic process – plan and prepare; detect and report; assess and decide; respond (prevent, reduce, recover); and lessons learned. These steps involve planning by policy and having the right people to manage the incident, identifying and reporting the incident, assessing the incident and making decisions as to how the incident is to be resolved, responding to incidents by containing and resolving them, and learning from the incident in order to be better prepared for future incidents (ISO/ IEC 27035:2016, 2016). Other frameworks include COBIT (Control Objectives for Information and Related Technologies) (ISACA, 2012) and ITIL (Information Technology Infrastructure Library) (Taylor et al., 2007), and NIST (National Institute of Standards and Technology) (Cichonski et al., 2012). The NIST guideline (comparable to the ISO/IEC standard) is also popular – it contains the phases of preparation, detection and analysis, containment, eradication and recovery, and post-incident activity (Tøndel et al., 2014).

Most studies that consider ISIM in practice share several commonalities. Hove et al. (2014) conducted a study on ISIM practices in three large organizations in Norway. From this study, two major issues related to the coordination of awareness and communication efforts were identified. Employees did not know how to report an incident and thus the tacit knowledge of users was being overlooked. Users can be valuable sources of information. Distributed structures hindered the collection and dissemination of incident-related information. The lack of coordination is evidenced by the lack of assigned responsibility. Clearly, one needs to know how to communicate the 'right information" to the "right people" to avoid leaking sensitive information.

Studies show that ISIM is largely uncoordinated. Ahmad et al. (2015) conducted a case study based on the Australian financial sector. They found that there are no formal structures to facilitate the "lessons learned" component. This implies that past incidents do not inform the management of new incidents. Bartnes et al. (2016b) conducted a study on current ISIM practices of Norwegian electric power

organizations. They found that the coordination of ISIM has not improved, as various views persist. In addition, organizations do not accord a high level of priority to ISIM. Line (2013) conducted a preliminary study that overviewed current ISIM practices in power industries. It was found that the process was unsystematic and there was a lack of coordination among the various groups of staff. Yohannes et al. (2019) found that in their case study of an Ethiopian bank that there was no formalized information security incident management, even though the bank was compliant with ITIL and ISO standards. They found that while there was an automated system of detection, issues, such as collaborative work, incident reporting, awareness, manual detection systems, post incident sharing of experiences and rehearsals were not given due consideration. They found that the lack of awareness, lack of skills, the lack of collaboration, and the communication gaps were causative challenges. Jaatun et al. (2009), who conducted interviews (n = 9) regarding information security incident management processes in the Norwegian petroleum industry, also cited challenges with awareness and reporting.

Several suggestions have been proposed to deal with the challenges identified in ISIM. Line et al. (2014) conducted an interview study on ISIM and concluded that there should be a unified approach to ISIM. Similarly, Jaatun et al. (2009) reasoned that there is a need to develop a reporting culture to unify ISIM. They propose enhancing the capability of incident management communication, underscoring organizational learning and individual training to resolve the communication gap among staff in order to unify the risk and situational understanding. They suggest an approach to learning from incidents that is both proactive and reactive, as the organization can learn about real time incidents and previous incidents, emphasizing organizational learning (Jaatun et al., 2009).

Several approaches have been proposed to manage ISIM. Metzger et al. (2011) developed a holistic, process-oriented approach to ISIM where incident response teams can correlate several incidents across multiple channels, which helps in classifying incidents correctly and, depending on the incident, an automated or manual reaction can be triggered. This method combined all reporting channels for consistency. Despite the successful implementation of the model, they found they needed to support the various ways incidents get reported. Furthermore, some incidents are not reported at all, or due to the lack of awareness, users are unable to report incidents correctly. Jeong et al. (2008) proposed an inter-organizational model for organizations that find it difficult to support a security team. Their model involves outsourcing their security information with a coordinator organization that can detect and analyze incidents for the organization. However, this model has not been implemented, as it merely transfers the challenges to another partner organization. Imamverdiyev (2013) considered the problem of prioritizing the volumes of incidents using fuzzy analytics. This can be a technical solution to managing incidents; however, it does not address the socio-technical challenges highlighted by extant studies. Baskerville et al. (2014) developed a framework that strikes a balance between prevention (i.e., managing predicted threats) and information security response (i.e., managing unpredicted threats) which encompasses three elements, namely, situational analysis, planning, and operation in both the prevention paradigm and response paradigm, with a careful balance between the two. An advantage of the model is that it prioritizes incident management, as it places the "lessons learned: as part of the central mode between prevention and response; however, it does not address the awareness and communication efforts required in ISIM.

The coordination of tasks within the security incident response process is highly complex, as it involves assigning responsibilities, duties, and tasks in a well-defined manner so that the correct workflows are triggered to manage incidents (Metzger et al., 2011). This coordination is often marred by poor communication and awareness efforts. Although awareness, training, and updating relevant databases and sharing results with trusted communities are key elements of the ISO/IEC 27035 standard,

unsatisfactory collaboration and poor communication efforts appear to be rife in ISIM (Tøndel et al., 2014). Evidently, organizations should be proactive in building the knowledge base of their stakeholders. Stakeholders (internal or external) may be a potential threat on occasion or the weakest information link (Johnson, 2006). It is evident that the management of incidents requires dynamism and coordination of work, and it requires collaboration from personnel of various perspectives to solve often complex problems (Bartnes et al., 2016b). Consequently, the aim of this study is to understand how organizations coordinate communication and awareness efforts in ISIM as a rationale towards proposing a conceptual model to address these challenges revealed in the study.

RESEARCH METHODOLOGY

The main aim of this study is to understand how organizations coordinate awareness and communication efforts in ISIM. This research study adopted an exploratory approach in order to achieve this aim. This methodology is suitable in studies where the problem is not well-defined. Typically, exploratory research is largely emergent and does not subscribe to a specific paradigm (Munkvold & Bygstad, 2016). Exploratory research can be a pathway into gaining insight into the research methodology to be used in the next phase of the research (Chawla & Sodhi, 2011). As this type of research is characterized by flexibility, pragmatism, and continuous discovery (Jupp, 2006), it is difficult to subscribe to a quantitative or qualitative research design. While the objective to identify patterns suggests a quantitative orientation, the social interactions with the participants suggest a qualitative orientation (Ang, 2014). There has been a recent trend towards "generic qualitative studies" which do not subscribe to the typical prescribed methodologies that guide interpretive research (i.e., narrative, phenomenological, grounded theory, ethnographic, and case study) (Caelli et al., 2003). Reiter (2013) also reflects on this trend relative to exploratory research and argues that exploratory research is entrenched in a socially constructed view of reality, as the aim is to produce new and insightful ways to explain reality and not to develop new facts. Furthermore, Reiter (2013) suggests that a researcher cannot be neutral, as in the positivistic tradition; however, rigor can be achieved by being honest and transparent with respect to the researcher's framing. Therefore, it is important to clarify the epistemological and ontological position of the researcher in an exploratory study.

Oates (2005, p. 292) suggests that an interpretive research paradigm "deals with the social context of an information system; the social processes by which it is developed and constructed by people through which it influences, and is influenced by its social setting." Therefore, an interpretive lens allows for understanding of failures that may be unknown to even those who are immersed in ISIM (Saunders et al., 2019). Consequently, the ontological position is relativist, assuming multiple constructed realities, while the epistemological viewpoint (i.e., the "relationship between the 'knower' [the research participant] and the 'would-be knower' [the researcher]") is within the interpretivist tradition which advocates for a subjectivist stance (Ponterotto, 2005, p. 131). However, given the exploratory nature of this study, a less prescriptive approach was taken, with the aim of obtaining a descriptive picture of the research questions posed as a rationale for the development of an applicable and compatible conceptual model to the problems raised. The authors were oriented towards a positivistic stance in terms of identifying patterns in the data, as this substantiated the development of the conceptual model.

In this study, a semi-structured interview guide (see Appendix A) was selected as an option for data collection. A semi-structured interview is useful in exploratory research, as it can help to clarify and discover concepts (Bless et al., 2006). The interview guide combined quantitative and qualitative questions to allow for interpretive reflections. This research employed a :track bound" approach, as the

interview guide is based on various extant sources as building blocks (Sandberg & Alvesson, 2011), including the ISO/IEC 27035-1:2011 (2011) standard.

The interview guide consisted of two parts. Part I was intended for the information security experts only while Part II (which was self-developed) was intended for end-users. Part I consists of three sections. Section 1 was designed to obtain background information of the organization. Sections 2 and 3 were designed to understand the coordination of awareness and communication efforts among security and end-user personnel respectively. Table 1 shows the derivation of the interview guide per question.

Component	**Question**	**Reference**
Background	1.1-1.1.17	Wooding et al. (2003); Da Veiga and Eloff (2007); Caballero (2013)
Roles and Responsibilities	2.1, 2.2, 2.3 and 2.4	Bernsmed and Tøndel (2013)
Application of Standards	2.5, 2.6 and 2.7	Ab Rahman and Choo (2015); Tøndel et al. (2014)
Formal Agreements	2.8. and 2.9	Johnson (2006)
ISIM Processes	2.10	Ahmed et al. (2012); Bernsmed and Tøndel (2013); Dodson (2001); Kossakowski et al. (1999); and Werlinger et al. (2010)
Awareness Levels	2.11	Bernsmed and Tøndel (2013)
Workflows	2.12 and 2.13	Belsis et al. (2005)
Awareness Efforts	2.14	Johnson (2006)
Communication Efforts	2.15, 2.17, 2.18	Baker (2002); Dodson (2001); and Wood (2012)
Communication Experience	2.16	Werlinger et al. (2010)
Improvement Strategies	2.19 and 2.21	Self-Developed Open-Ended Questions
Challenges	2.20	Self-Developed Open-Ended Question
End-User Involvement	3.1, 3.2, 3.3, 3.4 and 3.5	Johnson (2006)

Table 1. The Questionnaire Items Categorized into Components

A pilot test was conducted among information security experts (n = 6) from each of the organizations involved in the study to assess the content validity of the interview guide. A purposive sampling strategy was designed to meet the following criteria – engagement with large data sets, vulnerability to security incidents, engagement in ISIM processes, and proximity to the researcher.

Validity in qualitative type studies is confirmed by four basic tests – credibility (i.e., did the researcher accurately portray the participants' perceptions), dependability (i.e., coherence of the methods used), transferability (i.e., the extent to which the "working hypothesis" can be transferred to another context, and confirmability (i.e., the extent to which the data can be confirmed by others) (Bradley, 1993). (Note: Lincoln and Guba [1986] provided a baseline of techniques to achieve validity in qualitative studies which correspond to the criteria used by positivists). Credibility was achieved by the following techniques: prolonged engagement, triangulation, peer debriefing, and member checking. The field work was conducted over a period of six months. Peer debriefing was achieved by submitting the data and analysis to the secondary researcher for verification. The triangulation of data collection techniques was used as a mechanism of support and to enhance the validity of the study. The study relied on multiple sources of evidence to increase validity (i.e., document analysis of information security policies, procedures, and standards). A copy of the interview notes was disseminated to the participants for confirmation. Transferability was achieved by means of 'thick description' by attaining a richer understanding of the context via the background information and document analysis of the policies. The applicability of the research instruments was thoroughly linked with existing standards and extant

literature for standardization. Dependability was achieved via maintaining an audit trail. This was achieved by maintaining a list of data records, initially in paper format, and thereafter transferred to a digital format. Confirmability implies maintaining objectivity and neutrality. The neutrality of the study was achieved by assigning research assistants and data collectors in some instances to eliminate biases.

The data for the interview guide was collected both via email and face-to-face. The responses were collected in Amharic and translated into English. The collected data was analyzed quantitatively and qualitatively, case by case, through frequent comparison and inductive analysis based on preformatted themes (Mabuza et al., 2014).

RESEARCH ANALYSIS

Profile of the Sample

A profile of organizations included in the study are summarized in Table 2. The study involved 32 participants' accounts of ISIM practices. The sample consisted of – information security managers (n = 6), information security experts (n = 7), operational managers (n = 5), information security IT auditors (n = 4), information security risk analysis officers (n = 3), and end-users (n = 7). Most of the respondents from the sample have a basic level of education and a first degree commensurate with their positions within the organization. All the organizations indicated that they utilize basic information security mechanisms.

Code	Type	Function	Category	Size	No
ORG A	Government	Aviation	Commercial	>8000	6
ORG B	Government	Financial	Commercial	>10, 000	4
ORG C	Private	Financial	Commercial	>300	5
ORG D	Government	Media	Corporate	>1500	5
ORG E	Private	Financial	Commercial	>1500	5
ORG F	Government	Technology	Agency	>2500	7
TOTAL					32

Table 2. Background and Characteristics of the Organizations

Empirical Results and Analysis

In terms of the coordination of awareness efforts prescribed in the various policy documents, it was found that a large proportion of the awareness efforts are geared toward account usage (i.e., authentication) and antivirus installations. The coordination of awareness efforts of security incident handling and risk awareness were less integrated in policy documents as compared with the other aspects of information security. The responses are summarized in Table 3 (Question Q1.5).

Integrated Aspects	Number	Percentage
Security Incident Handling	10	31.25
Risk Awareness	9	28.13
Account Usage	29	90.63
Internet Application	25	78.13
Software Installation	20	62.50
Antivirus Installation	29	90.63

Table 3. Aspects of Information Security Awareness Issues Addressed in Organizations

Based on the responses, it was surmised that only ORG A and ORG B have a specific ISIM policy document (question Q1.6). ORG C from the private sector has a general information security policy document. The balance of the organizations are either in the process of developing a working policy document or they do not have a policy document in place. Most of the respondents (81%) confirmed that information security policies are drafted by information security experts and are then forwarded to middle management for approval. Notably, government organizations tend to have their own ISIM policy document and private organizations are in the process of developing a policy document.

Based on the responses related to the roles and responsibilities of management in ISIM, it was established that five organizations (ORGs A, B, D, E and F) are guided by the Ethiopian Information Network Security Agency (INSA) regarding information security policies (questions Q2.1 - Q2.3). In all cases, the security personnel develop the security policies, while management ensures its approval. INSA is involved in the process of initiating information security structures and guidelines in all governmental organizations and some private organizations.

Evidently, the communication efforts by managers are largely underwhelming (question Q2.4). The use of standards is sporadic, as it was revealed that only one organization (ORG A) from the government sector is on track to comply with the ISO 27035 standard (questions Q2.5, Q2.6 and Q2.7). Most of the participants (94%) indicated that the application of information security standards in their organizations is at the initial planning stage. The participants indicated that the slow adoption of standards is due to a lack of awareness about the existence of such standards. Furthermore, the participants indicated that the adoption of standards would not have relevance for their organizational information security incident operations. The following reason was offered by participant number three (an information security manager): "However, Lack [sic] of adequate knowledge on the availability of information security standards issues and lack of management commitment to use the existing standards are the factors which have been hindering our organization to adapt the standards." There also was no evidence suggesting the application of specific workflows for ISIM processes (questions Q2.12 and Q2.13).

The application of formal agreements with employees concerning information security policies is marginal (questions Q2.8 and Q2.9). The lack of formal agreements is generally attributed to the lack of awareness of incident management. The responses to question Q2.10, which required the participants to assess their organizations' formal provisions with respect to ISIM processes, are summarized in Figure 2. "Incident response" appears to be the most formalized action while "incident assessment and analysis" is the least formalized action.

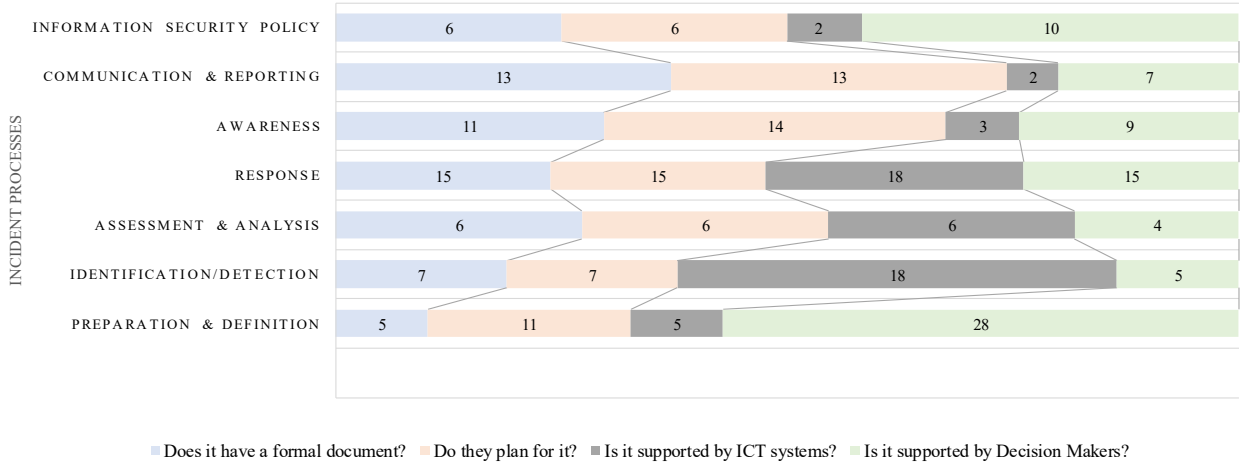


Figure 2. Responses across ISIM Parameters

The responses to question Q2.11, which required the participants to rate the level of information security incident awareness and risk understanding of employees with respect to information security incident awareness indicators, is summarized in Table 4.

Awareness indicators	**Top-Level Management**	**Middle-Level Management**	**Low-Level Management**	**End-Users**	**Information Security Expert (ISIRT)**
Knowledge about ICT systems and components	1.9	3.12	3.1	2.1	5
Information security competence	1.2	2	3.4	1.1	5.8
Reporting security incidents	1.1	2.8	2.3	0.9	5.7
Up-to-date knowledge about relevant threats	0.9	2.7	1.9	1.8	4.1
Learning from previous incidents	3.9	4.2	2.9	3.7	5.8

Table 4. An ISIM Awareness Assessment Indicators Matrix

The ISIM awareness assessment indicators matrix was derived by the respondents scoring each indicator from Poor to Excellent, and these were encoded into Likert scales (1 to 6 respectively) for analysis. Each management category was given a mean score to represent the overall response per category. Although the general awareness quota is low, the rate of awareness is much higher among ICT experts.

Most of the techniques employed by organizations to raise the awareness of information security incidents have been implemented via "promotional," "educational," and "informational methods" (question Q2.14). The information security incident awareness raising methods, as utilized by the organizations, is summarized in Table 5. Punitive measures, such as penalties and accountability, are not given due consideration by the organizations under study.

Awareness raising methods	**ORG A**	**ORG B**	**ORG C**	**ORG D**	**ORG E**	**ORG F**
Promotional methods	√	√	√	√	√	√
Enforcing methods	√	X	X	X	X	√
Educational methods	√	√	√	√	√	√
Informational methods (i.e. updates on information security)	√	√	√	√	√	√
Digital methods	X	X	X	X	X	√
Face-to-face guidance methods	√	√	X	√	X	√

Table 5. ISIM Awareness Raising Methods per Organization

Most of the organizations used manual means of reporting information security incidents (question Q 2.15). The usage per reporting mechanism is as follows – manual reporting (93.75%), face-to-face contact (62.50%), electronic means (46.88%), telephone reporting (43.75%), audio-visual means (21.88%), and customized application software (15.63%).

The level of an employee's communication experience with respect to ISIM was found to be at a very poor or fair level among all managerial levels, except among the experts (question Q2.16). This implies that peer and vertical communication among users and managers was poor compared with peer communication among expert users.

The frequency of communication regarding information security incidents is largely uncoordinated. Most of the respondents (40.6%) indicated that information security incident communication efforts (both peer-to-peer and laterally) are conducted usually when an incident arises (question Q 2.17). Figure 3 shows the percentage of frequency of information security incident communication in the studied organizations. Case in point: "I usually communicate among ourselves and security personnel when incident arises on how to protect and mitigate current security issues without using any formal means of information security communication mechanism [sic]," (Participant No. 11)

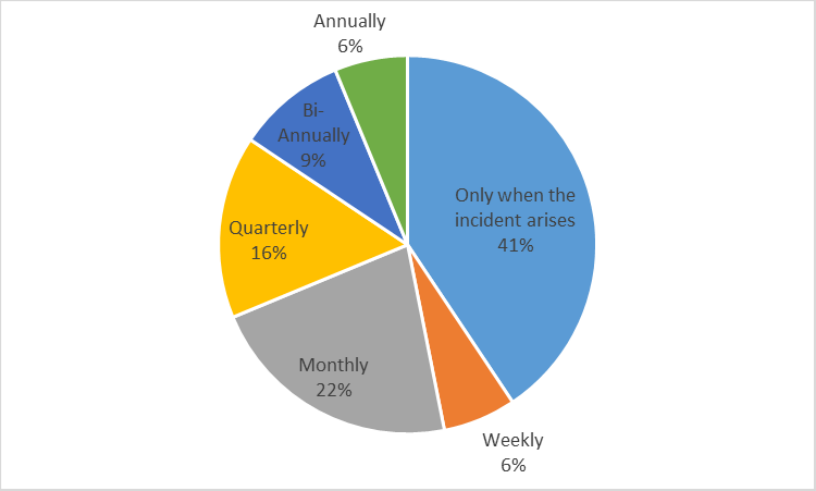


Figure 3. Percentage Frequency of ISIM Communication within the Studied Organizations

The communication and reporting efforts of information security incidents is largely uncoordinated. It was established that most organizations usually communicate via short face-to-face meetings (question Q2.18). Only two organizations (ORGs A and B) coordinated communication efforts through electronic means. A case in point: "The routine information security cases are not communicated to the operational staff, whereas the filtered or analyzed information is not reported to decision makers. We were also rarely communicated about information security incidents that were believed to be critical by the ICT staff and experts*"* [sic] (Participant No. 17).

An inspection of the opinions regarding the methods that can be used to improve the awareness and communication efforts among stakeholders revealed that the majority of respondents (91%) opted for policy change, training, and a coordinated incident reporting and awareness effort (question Q2.19).

An examination of the responses concerning the types of challenges involved in the coordination of communication and awareness efforts in ISIM revealed the following challenges – lack of planning, policies, awareness and managerial commitment, and no established center for information security training (question Q2.20).

The respondents offered the following recommendations with respect to the manner ISIM communication efforts can be integrated effectively into an organizational information security policy (question #Q2.21) – integration of reporting policies on ISIM; proactive reporting of information security incidents; enhancing the awareness of ISIM; strong managerial commitment; enforcing automated security incident communication policy and procedure; stronger linkage between an organization's information security team and public relations; benchmarking of information security standards; building an information security knowledge base, and the deployment of a skilled information security incident response team (ISIRT).

Apparently, there is scant involvement of end-users both in the process of information security incident policy formulation, implementation, and communication efforts (questions Q3.1 –Q3.4). The security experts prepare awareness documents for employees, and awareness training is provided by security experts with the support of mid-level management. However, most end-users did not get an invitation to participate in information security policy formulation and incident preparation. The reasons cited for the lack of involvement of end-users include confidentiality, work overload, and the lack of expertise in information security. Only two organizations (ORGs A and B) have initial trials involving end-users in the process of information security incident policy formulation. These organizations provided consultative training for their end-users. Moreover, a fair balance of routine work and the information security awareness scheme was implemented among these organizations.

The accounts of end-user involvement in information security incident cases revealed that most respondents (57.14%) are highly involved in high-level policy issues as opposed to technical and security issues (question Q3.5). The data extracted from Part II of the interview guide confirmed the status of the involvement of end-users in ISIM. The excluded end-users indicated that they would prefer to be consulted in such matters for shared understanding and for upskilling. One end-user indicated that such involvement would not only have been to the benefit of himself but also to the benefit of the organization. Case in point: "It would have been very good if our organization would have provided me the opportunity to participate in information security issues that concern us to the benefit of the organization" (End-User No. 3, ORG A). The following case in point also establishes the need for end-user involvement in ISIM: "I think it will be good if the organization frequently and consistently practice information security training and awareness to all employees irrespective of their position and

role. And we also need a computer based system that alarms us that we are under threat or to aware us [sic]" (End User No. 4, ORG C). Evidently end-users would prefer to be involved in ISIM.

As most of the organizations did not have a standardized information security incident management policy document, the study considered related documents, such as ICT Policy, Information Management Policy, and User Management Policy, to confirm the responses of the participants.

DISCUSSION

Some of the challenges observed in this research are echoed in published academic work. For instance, lack of managerial commitment, lack of collaboration, and lack of documentation are known weaknesses in ISIM (Bartnes et al., 2016a). With respect to the first minor research question (RQ-1), it was found that the coordination of communication and awareness efforts are largely informal and are mired by a lack of planning and managerial commitment; however, there was a drive toward including ISIM in policy documents. The findings of this study are also comparable to Yohannes et al. (2019). In their case study on an Ethiopian bank, they also found that there is a lack of mechanisms to report incidents. They also note that some incidents go unreported due to poor communication efforts.

The importance of coordination between external and internal stakeholders with respect to incident reporting was also highlighted by extant studies (Hove et al., 2014). However, as reflected by Bartnes et al. (2016a) and Tøndel et al. (2014), the collaboration among stakeholders in incident reporting remains a challenge. This finding is also comparable with this study. Furthermore, with respect to the minor question (RQ-2), it was found that while end-users would prefer to be involved in ISIM, the import of their contribution is largely ignored in the process. Consequently, most end-users have a scant awareness of ISIM and the reporting process. This paper proposes that involving end-users in ISIM can reduce the number and severity of information security incidents. First, the involvement of end-users in ISIM may prevent accidental and malicious insider threats, as end-users cannot use the excuse of being ignorant of which actions constitute an information security breach. Second, end-users will be able to identify and report an incident more efficiently, thereby reducing the severity of the incident.

In the organizations studied from Ethiopia, the ISIM issue is a relatively new concept for most organizations. The organizations studied are characterized by the absence of a strong ISIM policy document and low levels of stakeholder participation, with an emphasis on responding to incidents (i.e., reactive) rather than an effective proactive strategy. This implies that Ethiopian organizations are highly susceptible to information security incidents. Most of the organizations studied emphasized general information security threats and technical security equipment installations. It has been recognized that there is a need for a fair balance between prevention and response for an organization to proactively and retroactively respond to incidents (Baskerville et al., 2014). The lack of plans and formal employee collaboration in the process of information security incidents could pose a severe risk to organizations (Tøndel et al., 2014; Werlinger et al., 2010). As a result, it cannot be overstated that organizations must include proactive planning, resource allocation, and formal employee involvement in all phases of ISIM (Ab Rahman & Choo, 2015).

The findings of this study imply that the coordination of awareness and communication efforts are executed in a fragmented and disjointed manner. Werlinger et al. (2010) observed that most organizations do not have the culture of working collaboratively with stakeholders and end-users, especially in terms of setting and communicating information security incident policies. The findings of this study also established that the culture of information security incident awareness and

communication is largely absent. It can be reasoned that ISIM requires a reframing of awareness and communication efforts into an inclusive process, which is the subject of the next section.

A CONCEPTUAL FRAMEWORK

This study identified two key problems in ISIM – poor coordination of communication and awareness efforts. These key problems negatively influence the reporting of incidents and the collaborative power of groups acting in coordination, and this presents a major risk to organizations. These issues led the study to unpack the final minor research question (i.e., how can organizations enhance the coordination of communication and awareness efforts within the processes of ISIM practice?).

Most studies recommended training programs for awareness creation (Hove et al., 2014; Tøndel et al., 2014; Yohannes et al., 2019). Based on the challenges identified in the exploratory study, a socio-technical solution may be required to coordinate awareness efforts. ISIM will benefit from a socio-technical solution to combat incident challenges proactively in organizations (Werlinger et al., 2010). An alternative way of increasing awareness may be achieved through policy. Wiant (2005) suggested that information policy may increase the awareness of incidents; however, this empirical study found that policy does not influence the number and severity of incidents reported. Tøndel et al. (2014) formulated a model of incident management based on a systematic review of the literature. In the model, the "plan and prepare" phase catered for incident management awareness (via training) while the "response" phase catered for communication efforts. They argued that an incident tracking system will facilitate communication among technical staff. However, they contend that there is a lack of policies on formal channels for communication. They suggested that incident ticketing systems require a shared mental model to improve coordination of communication efforts. However, they could not verify the process of a shared mental model; they felt that this may be the missing element in the information required by technicians in incident ticketing systems. Entin and Entin (2000) surmised that mental models create awareness and the accuracy and congruence of these models impact a team's level of Situational Awareness. Scarfone et al. (2008) argue that maintaining Situational Awareness in incident management involves planning, documenting, and assigning roles and responsibilities. Therefore, the process must be managed carefully, which may be the reason why this process is deficient in ISIM.

Webb et al. (2014) highlighted the relevance of Situational Awareness to information security in general and specifically to information security risk management which share many of the problems with ISIM – (1) information risk identification is perfunctory; (2) security risks are estimated without due attention to situation awareness; and (3) risk assessments are done intermittently without attention to historical data. In a previous study conducted by the current authors (Padayachee & Worku, 2017), the application of Situational Awareness to ISIM was considered. As there are few descriptions of a Shared Situational Awareness model for organizations, this model considered representations from other contexts, such as supply chain management (Kurapati et al., 2013a; Kurapati et al., 2013b). The model developed by the authors demonstrated that the process of incident management could iterate from individual Situational Awareness to Shared Situational Awareness, thereby increasing the responsiveness and collaborative power in the process. However, the model did not address the pathways of communication channels. Linderoth et al. (2015, p. 321), who conducted a study within emergency situations which share a similarity with ISIM, found that Situational Awareness, communication, and attitude were challenges and they stated that effective communication pathways "are essential to obtain sufficient and identical situation awareness." The processes of incident preparation, detection, and reporting are crucial steps in ISIM, which are followed by assessment, decision, response, and lessons learned (Humphreys, 2008). Consequently, communication flow is a vital component of every step in cyber security incident

response. The next elaboration aims to show a formalized approach to coordinating Situational Awareness with communication pathways.

Situational Awareness

Situational Awareness is more than just being aware of "numerous pieces of data," as it requires an advanced level of situational understanding and a projection of future system states (Endsley, 1995). Situational Awareness is the perception and comprehension of the elements in the current state and a projection of their status into the near future state (Endsley, 1988), which requires a user's ability to understand, infer and make decisions proactively based on empirical information about a situation. Figure 4 demonstrates an application of Situational Awareness to ISIM. (The application of Situational Awareness to ISIM was developed by the authors, however, the basic elements of Situational Awareness were adapted from Endsley (1995). Webb et al. (2014) argued that Situational Awareness is highly suitable to organizational process design.

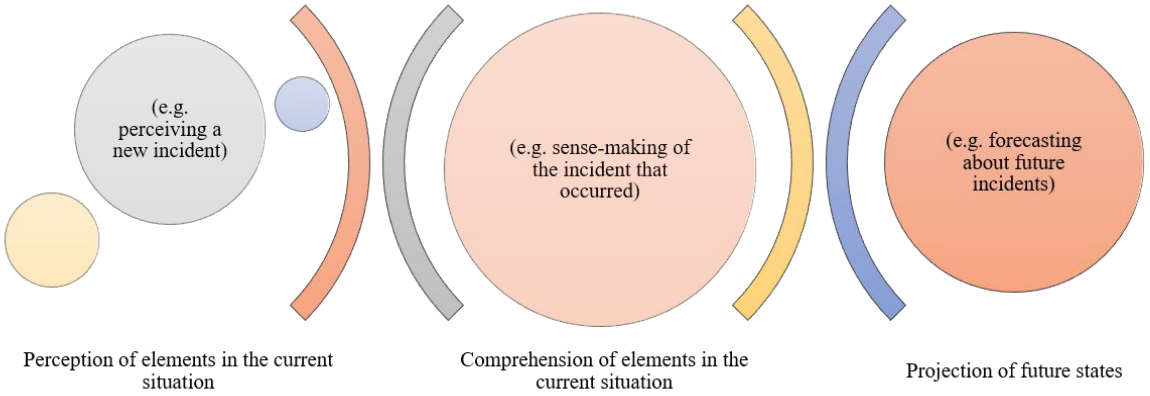


Figure 4. Levels of Situational Awareness for Information Security Incident Management

Situational Awareness could have a potential role in understanding, perceiving, and anticipating future incidents so that active incidents are addressed proactively. According to Barford et al. (2010), there are seven aspects of Situational Awareness which can be applied to incident management, which were also explored in a previous work by the authors of the current paper (Padayachee and Worku, 2017): (1) awareness of the current situation which includes situation recognition (knowing that an attack is occurring) and identification (i.e., type of attack), the source (who, what) and target; (2) awareness of the impact of the attack (impact assessment, vulnerability analysis), which includes current impact and future assessment; (3) situation tracking; (4) awareness of the adversary's behavior, trends, and intent analysis; (5) awareness of why and how the current situation was caused; (6) awareness of the trustworthiness of the collected situation awareness data; (7) projecting and constraining future actions from the adversary, whereby, the constraint involves understanding intent, opportunity, and capability.

Moreover, a multi-actor activity like ISIM should be subsumed in a Shared Situational Awareness framework. According to Endsley and Jones (2001, p. 48), Shared Situational Awareness is defined as "the degree to which team members possess the same SA (Situational Awareness) on shared SA (Situational Awareness) requirements." Shared Situational Awareness, which is more appropriate to organizational settings, involves "a number of persons trying to form a common picture" (Nofi, 2000, p. 28).

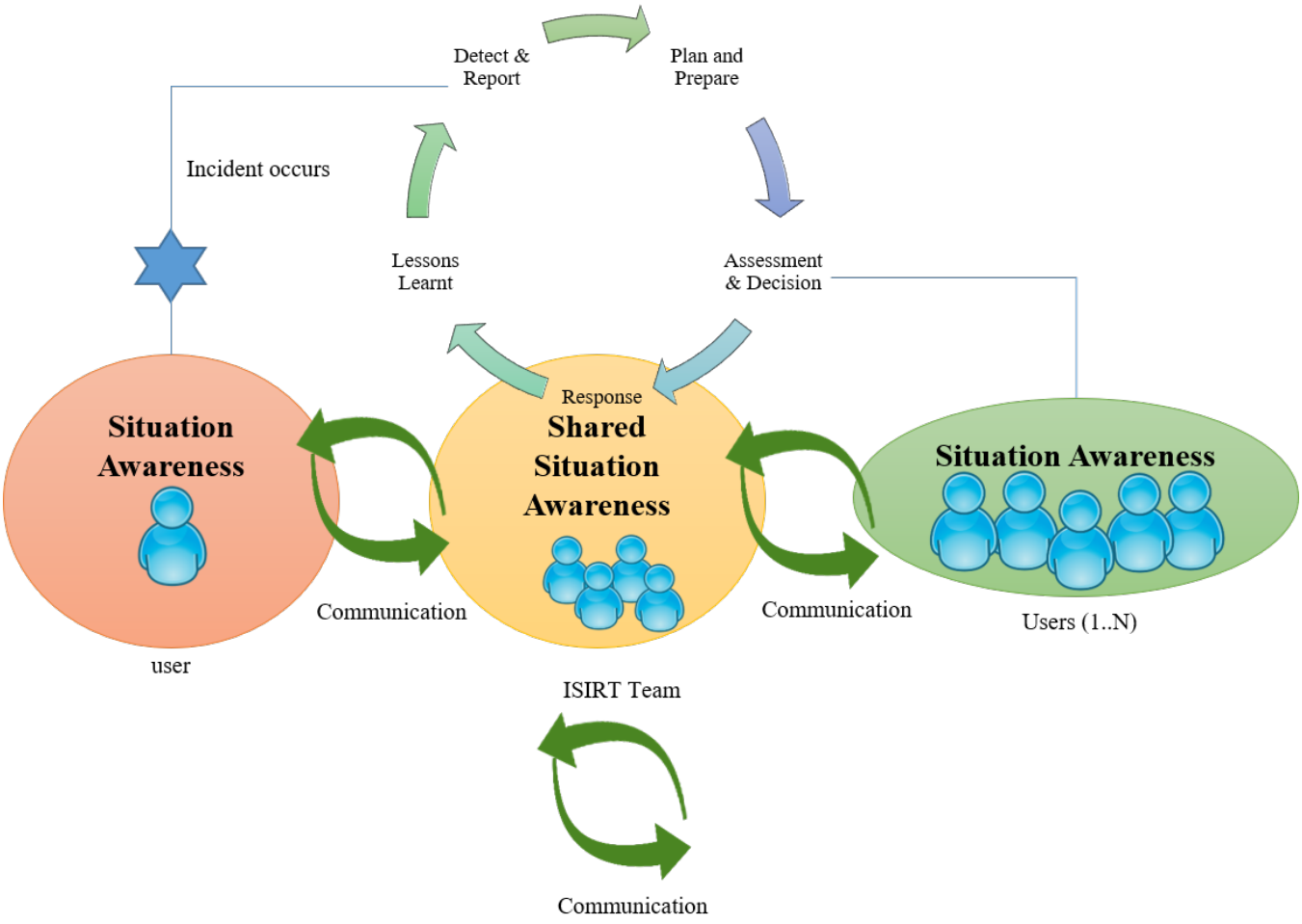


Figure 5. Communication Pathways to Achieve Shared Situational Awareness for ISIM

The relationship between Shared Situational Awareness and socio-technical systems has not been thoroughly explored (Kurapati et al., 2012). Nofi (2000) suggests that building Shared Situational Awareness within organizations involves the following criteria: first, consider the individual Situational Awareness within the framework of what needs to be accomplished. Second, establish roles of other members of the organization to share their awareness appropriately (mental models) by using a communication protocol. Third, integrate various individual mental models of the situation to develop a common understanding. In this modification of the "Conceptual Model for Shared Situational Awareness for Information Security Incident Management," the authors leverage communication pathways to address this deficiency in the original conceptualization (see Figure 5). The notion of a communication protocol within Situational Awareness was adapted from Linderoth et al. (2015); however, the application to ISIM was developed by the authors.

In Figure 5, the user detects an incident and will need to report the incident. The user will report it according to his/her perception of the elements involved in the incident detected; for example, the type of attack, and the source and target of the attack. Based on his/her perceptions and comprehension of the current situation, the user also will create a projection of future incidents. The user will then *communicate* his/her report to the ISIRT team who will interpret and analyze the report. Using this

information and additional tools (e.g., impact assessment and vulnerability analysis) and their perceptions and comprehension of the current situation, the ISIRT team will also conduct a projection of future incidents in order to plan and prepare for managing future incidents and lessons learned. This will be an internal *communication* between the ISIRT team members. The ISIRT team will *communicate* assessments and decisions to the wider stakeholders. In the next sub-section, the communication protocol for the conceptual model is explored in further detail.

An Interactive Model of Communication for ISIM

In general terms, "[c]ommunication implies a sender, a channel, a message, a receiver, a relationship between sender and receiver, an effect, a context in which communication occurs and a range of things to which 'messages' refer" (McQuail & Windahl, 2015, p. 5). According to Sellnow (2005), there are three basic communication models – the linear model, the interactive model, and the transactional model. The linear model views communication as one-directional, while the interactive model is bidirectional. The transactional model is more advanced than the interactive model, as it also considers the context of the communication which may influence the interaction, such as culture. However, the transactional model encourages non-verbal cues and "noise" as communication between senders and receivers occurs simultaneously (Businesstopia, 2018). The interactive model, more specifically, the Interactive Model of Communication (IMC) was chosen for this study, as it is often used for the Internet where people can respond to mass communication (Businesstopia, 2018). Additionally, it is beyond the scope of this research to consider the cultural and societal issues that may affect communication. Communication models have been applied within ICT settings (Madida, 2018; Moise, 2008; Velten & Arif, 2016). However, there appears to be few instances of its application to incident management, with the exception of Valecha et al. (2012).

Valecha et al. (2012) used IMC in order to standardize emergency communication reports. They developed a messaging model which determines the structure of a message and standardizes the format so that it could be shared with several departments. They used the model to identify key elements and state transitions in emergency communications. They indicate that their work could be extended to information management, coordination, and accountability. However, this study will propose using the communication model within the context of Situational Awareness.

The underlying rationale in applying a communication model, such as the IMC (see Figure 6), is to enhance the communication of information security incidents, policies, and procedures in a coordinated manner. The model deals with the exchange of information and messages taking place bi-directionally from sender to receiver and vice-versa (Schramm, 1954). The IMC takes into account the communicators' fields of experience – the greater that their field of experience overlaps, the greater the understanding between the communicators (Wood, 2014). The concept of a shared understanding appears to be congruent with Shared Situational Awareness. Successful application of the IMC model in incident management is also shaped by the technical abilities and communication skills of both the sender and the receiver, and this is known as the field of experience. There also may be interferences to communication such as process, physical, semantic, and psychosocial barriers (Lunenburg, 2010). It is beyond the scope of this research to consider these interferences. The model will facilitate the management and exchange of information among stakeholders regarding encountered incidents, which can potentially answer the "What," "When," and "Who" aspect of the incident. In the next elaboration, an application of the concept is unpacked.

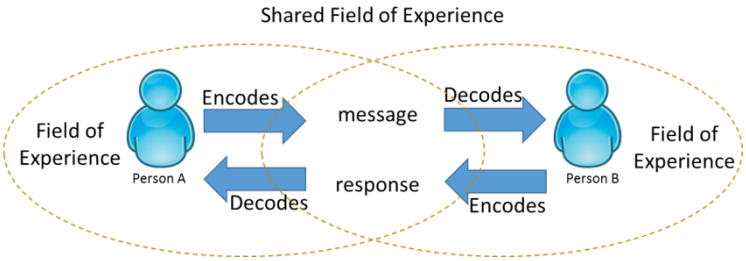


Figure 6. Interactive Model of Communication
(adapted from Schramm, 1954).

Application of the Conceptual Model

Figure 7 shows the application of using IMC and Situational Awareness in ISIM within a role-based system.

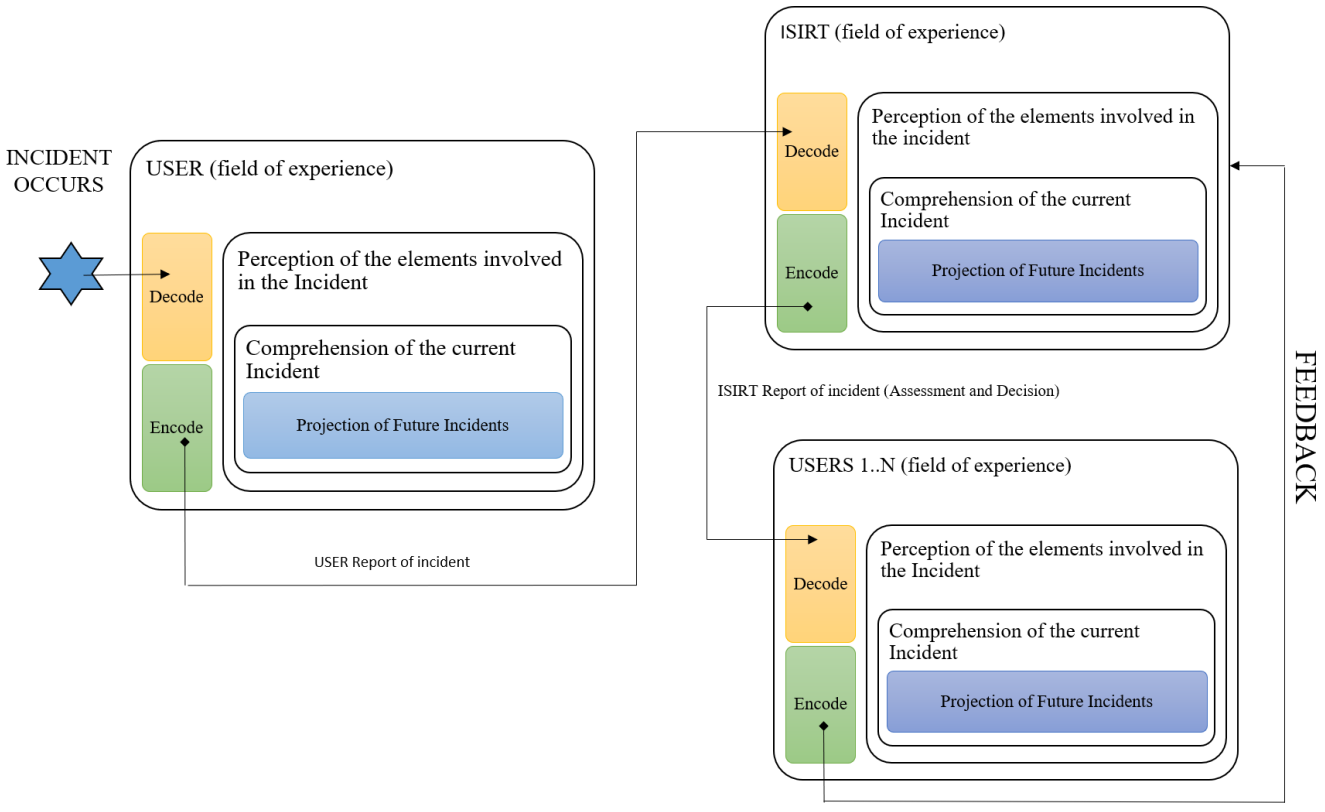


Figure 7. An Application of the Conceptual Model

This application of the conceptual framework focuses on the phases of "Detection and Reporting" and "Response," as there is poor communication between reporting the incident and the notification back to the users regarding the response. The user detects an incident within the field of experience (based on prior planning and preparation and lessons learned from previous incidents) and needs to decode the

incident. The user needs to formally document (encode) the incident. The user will encode the incident according to his/her perception of the elements involved in the incident detected; for example, the type of attack, and the source and the target of the attack. Based on his/her perceptions and comprehension of the current situation, the user also will create a projection of future incidents using specific codes and data elements. The user then will upload his/her report to the ISIRT team, which will interpret and analyze the information (i.e., decode) based on past incidents and lessons learned (i.e., their field of experience). Using this information and additional tools (e.g., impact assessment and vulnerability analysis) and perceptions and comprehension of the current situation, the ISIRT team will also encode a projection of future incidents, which includes planning and preparation for managing future incidents and lessons learned. They also will encode their assessment, response, and decisions regarding the incident. They then will direct their assessment and decisions, which will be forwarded to all users based on their roles. Each user then decodes the assessments and decision report and they will encode their feedback (including a projection of future incidents) to the ISIRT team for verification. Table 6 shows how the incident is managed within the conceptual framework. The model is intended to work in a role-based system in order to manage multiple stakeholders.

ROLE	**Perception of the elements in the incident**	**Comprehension of the current situation**	**Projection of future incidents**	**Output**
USER (the reporter of the incident)	Decode the new Incident Identify new Incident	Encode the Incident -Incident Source -Incident Category -Incident Risk -Incident Target	Encode the Projection of future incidents with the support of additional enablers such as situational, structural and automated tools.	USER Report of Incident
ISIRT	Decode report from ISIRT	Encode the Incident -Register Incident -Review Incident -Verify Incident -Analyze Incident -Scale Incident -Classify Incident -Impact Assessment -Vulnerability Assessment -Backtracking -Filter Incident according to roles	Encode the Projection of future incidents. Plan and Prepare for future incidents. Lessons Learnt in preparation for future incidents.	ISIRT Report of the Incident
USER 1…N	Decode the ISIRT Report according to roles	Encode the ISIRT Report according to roles	Encode the Projection of future incidents based on the collective information.	Submit Verification of Action to ISIRT

Table 6. An Application of the Conceptual Model

CONCLUSION

This paper proposed a novel conceptual model to address the challenges identified by an empirical study. The model potentially will leverage the collaborative power of bringing diverse stakeholders together, including end-users via Shared Situational Awareness. The communication channels are clearly outlined and provide a mechanism to develop a unified understanding of ISIM. Although this study was exploratory with a limited sample size, it provides new empirical data on ISIM practices (with respect to awareness and communication efforts) which appears to be congruent to other global research studies. As the study was limited to organizations in Ethiopia, the findings may not be generalizable to all contexts. The research approach for this study should be viewed within a framework of a design science approach. The preliminary phases of a design science approach requires the identification and description of a relevant problem (March & Storey, 2008) which was presented here. Future research will involve prototyping and evaluating the conceptual model.

REFERENCES

Ab Rahman, N. H., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 45-69. https://doi.org/10.1016/j.cose.2014.11.006

Ahmad, A., et al. (2012). Incident response teams–challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643-652. https://doi.org/10.1016/j.cose.2012.04.001

Ahmad, A., et al. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6), 717-723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Ahmed, M., et al. (2012). Human errors in information security. *International Journal of Advanced Trends in Computer Science and Engineering*. *1*(3),, 82-87.

Ang, S. H. (2014). *Research design for business & management*. Sage. https://doi.org/10.4135/9781473909694

Ani, U. P. D., & Agbanusi, N. C. (2014). A comparative assessment of computer security incidence handling. *Journal of Advances in Mathematics and Computer Science*. *4*(22), 3120-3134. https://doi.org/10.9734/BJMCS/2014/11874

Baker, K. A. (2002). Organizational communication. Retrieved from https://web.archive.org/web/20190326144116/http://www.au.af.mil/AU/AWC/AWCGATE/doe/benchmark/ch13.pdf

Barford, P., et al. (2010). Cyber SA: Situational awareness for cyber defense. In S. Jajodia, P. Liu, V. Swarup & C. Wang (Eds.), *Advances in information security* (pp.3-13). Springer. https://doi.org/10.1007/978-1-4419-0140-8_1

Bartnes, M., et al. (2016a). Current practices and challenges in industrial control organizations regarding information security incident management – does size matter? Information security incident management in large and small industrial control organizations, *International Journal of Critical Infrastructure Protection*, *12*, 12-26. https://doi.org/10.1016/j.ijcip.2015.12.003

Bartnes, M., et al. (2016b). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, *61*, 32-45. https://doi.org/10.1016/j.cose.2016.05.004

Baskerville, R., et al. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management*, *51*(1), 138-151. https://doi.org/10.1016/j.im.2013.11.004

Belsis, M. A., et al. (2005). Workflow based security incident management. In *Proceedings of the Panhellenic Conference on Informatics* (pp. 684-694). https://doi.org/10.1007/11573036_65

Bernsmed, K., & Tøndel, I. A. (2013). Forewarned is forearmed: Indicators for evaluating information security incident management, In H. Morgenstern, R. Ehlert, F. Freiling, S. Frings, O. Goebel, D. Guenther, S. Kiltz, J. Nedon, & D. Schadt (Eds.), *Seventh International Conference on IT Security Incident Management and IT Forensics* (pp. 3-14). https://doi.org/10.1109/IMF.2013.14

Bless, C., et al. (2006). *Fundamentals of social research methods: An African perspective*, Juta and Company, Ltd.

Bradley, J. (1993). Methodological issues and practices in qualitative research. *The Library Quarterly*, *63*(4), 431-449. https://doi.org/10.1086/602620

Businesstopia. (2018). Models of communication. Retrieved from https://www.businesstopia.net/communication

Caballero, A. (2013). Information security essentials for IT managers: Protecting mission-critical systems. In J. R. Vacca (Ed.), *Computer and information security handbook* (pp. 379-407). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-394397-2.00021-0

Caelli, K., et al. (2003). 'Clear as mud': Toward greater clarity in generic qualitative research. *International Journal of Qualitative methods*, *2*(2), 1-13. https://doi.org/10.1177/160940690300200201

Chawla, D., & Sodhi, N. (2011). *Research methodology: Concepts and cases*. Vikas Publishing House.

Cichonski, P., et al. (2012). *Computer security incident handling guide* (SP 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361-372. https://doi.org/10.1080/10580530701586136

Dodson, R. (2001). Information incident management. *Information Security Technical Report*, *3*(6), 45-53. https://doi.org/10.1016/S1363-4127(01)00307-7

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 97-101). https://doi.org/10.1177/154193128803200221

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Journal of the Human Factors and Ergonomics Society*, *37*(1), 32-64. https://doi.org/10.1518/001872095779049543

Endsley, M. R., & Jones, V. M. (2001). A model of inter-and intrateam situation awareness: Implications for design, training, and measurement. In M. McNeese, E. Salas, & M. R. Endsley (Eds.), *New trends in cooperative activities: Understanding system dynamics in complex environments* (pp. 46-47). Human Factors and Ergonomics Society.

Entin, E. B., & Entin, E. E. (2000). Assessing team situation awareness in simulated military missions. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 73-76). SAGE Publications. https://doi.org/10.1177/154193120004400120

Hove, C., et al. (2014). Information security incident management: Identified practice in large organizations. In F. Freiling, H. Morgenstern, S. Frings, O. Goebel, D. Guenther, J. Nedon, & D. Schadt (Eds.), *Eighth International Conference on IT Security Incident Management & IT Forensics* (pp. 27-46). https://doi.org/10.1109/IMF.2014.9

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247-255. https://doi.org/10.1016/j.istr.2008.10.010

IBM Security. (2019). Cost of a data breach report 2019. Retrieved from https://databreachcalculator.mybluemix.net/executive-summary https://doi.org/10.1016/S1361-3723(19)30081-8

Imamverdiyev, Y. (2013). An information security incident prioritization method. In *7th International Conference on Application of Information and Communication Technologies* (pp. 1-5). https://doi.org/10.1109/ICAICT.2013.6722750

ISACA. (2012). Cobit 5: Enabling procceses. Author.

ISO/IEC 27035:2016. (2016). Information technology — security techniques — information security incident management: Part 1: Principles of incident management. International Organization for Standardization.

ISO/IEC 27035-1:2011. (2011). Information technology – security techniques – information security incident management: Part 1: Principles of incident management . International Organization for Standardization.

Jaatun, M. G., et al. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, *2*(1-2), 26-37. https://doi.org/10.1016/j.ijcip.2009.02.004

Jeong, K., et al. (2008). A security coordination model for an inter-organizational information incidents response supporting forensic process. In J-H. Kim, D. Delen, P. Jinsoo, F. Ko, & Y.J. Na (Eds.), *Fourth International Conference on Networked Computing and Advanced Information Management* (pp. 143-148). https://doi.org/10.1109/NCM.2008.126

Johnson, E. C. (2006). Security awareness: Switch to a better programme. *Network Security*, *2*, 15-18. https://doi.org/10.1016/S1353-4858(06)70337-3

Jupp, V. (2006). The Sage dictionary of social research methods. Sage. https://doi.org/10.4135/9780857020116

Kossakowski, K.-P., et al. (1999). *Responding to intrusions, CMU/SEI-SIM-006*. Carnegie Mellon Software Engineering Institute. https://doi.org/10.21236/ADA360500

Kurapati, S., et al. (2012). A theoretical framework for shared situational awareness in sociotechnical systems. In A. Moore, V. Pammer, L. Pannese, M. Prilla, K. Rajagopal, W. Reinhardt, T.D. Ullmann, & C. Voigt (Eds.), *Proceedings of the 2nd Workshop on Awareness and Reflection in Technology-Enhanced Learning.* (pp.47-53.

Kurapati, S., et al. (2013a). Exploring shared situational awareness in supply chain disruptions. In T. Comes, F. Fiedrich, S. Fortier, J. Geldermann, & T. Müller (Eds.), *ISCRAM 2013: Proceedings of the 10th International Conference on Information Systems for Crisis Response and Management* (pp. 151-155).

Kurapati, S., et al. (2013b). Exploring shared situational awareness using serious gaming in supply chain disruptions [slideshare presentation]. Retrieved from https://www.slideshare.net/streamspotter/exploring-shared-situational-awareness-using-serious-gaming-in-supply-chain-disruptions

Lincoln, Y. S., & Guba, E. G. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. In D. D. Williams (Ed.), *New directions for program evaluation* (pp. 73-84). Jossey-Bass. https://doi.org/10.1002/ev.1427

Linderoth, G., et al. (2015). Challenges in out-of-hospital cardiac arrest – a study combining closed-circuit television (cctv) and medical emergency calls. *Resuscitation*, *96*, 317-322. https://doi.org/10.1016/j.resuscitation.2015.06.003

Line, M. B. (2013). A case study: Preparing for the smart grids - identifying current practice for information security incident management in the power industry. In H. Morgenstern, R. Ehlert, F. Freiling, S. Frings, O. Goebel, D. Guenther, S. Kiltz, J. Nedon, & D. Schadt (Eds.), *Seventh International Conference on IT Security Incident Management and IT Forensics* (pp.26-32). https://doi.org/10.1109/IMF.2013.15

Line, M. B., & Albrechtsen, E. (2016). Examining the suitability of industrial safety management approaches for information security incident management. *Information & Computer Security*, *24*(1), 20-37. https://doi.org/10.1108/ICS-01-2015-0003

Line, M. B., et al. (2014). Information security incident management: Planning for failure. in F Freiling, H. Morgenstern, S. Frings, O. Goebel, D. Guenther, J. Nedon, & D. Schadt (Eds.), *Eighth International Conference on IT Security Incident Management & IT Forensics* (pp. 47-61). https://doi.org/10.1109/IMF.2014.10

Lunenburg, F. C. (2010). Communication: The process, barriers, and improving effectiveness. *Schooling*, *1*, 1-61.

Madida, M. S. (2018). *Innovative communication protocols for teaching in rural secondary schools* [Unpublished master's thesis]. University of Zululand.

March, S. T., & Storey, V. C. (2008). Design science in the information systems discipline: An introduction to the special issue on design science research. *MIS quarterly*, *32*(4), 725-730. https://doi.org/10.2307/25148869

McQuail, D., & Windahl, S. (2015). *Communication models for the study of mass communications* (2nd ed.). Routledge. https://doi.org/10.4324/9781315846378

Metzger, S., et al. (2011). Integrated security incident management--concepts and real-world experiences. In H. Morgenstern, R. Ehlert, S. Frings, O. Goebel, D. Guenther, S. Kiltz, J. Nedon, & D. Schadt (Eds.), *Sixth International Conference on IT Security Incident Management and IT Forensics* (pp.107-121). https://doi.org/10.1109/IMF.2011.15

Moise, G. (2008). Communication models used in the online learning environment. In M. Vlada, G. Albeanu, & D. Popovici (Eds.), *Proceedings of The 3rd International Conference on Virtual Learning* (pp. 247-254).

Munkvold, B. E., & Bygstad, B. (2016). The land of confusion – clearing up some common misunderstandings of interpretive research. In *NOKOBIT-Norsk Konferanse for Organisasjoners Bruk av Informasjonsteknologi, 24*(1), 1-12.

Nofi, A. A. (2000). *Defining and measuring shared situational awareness, CRM D0002895.A1*. Center for Naval Analyses.

Nyman, M., & Große, C. (2019). Are you ready when it counts?: IT consulting firm's information security incident management. In P. Mori, S. Furnell, & O. Camp (Eds.), *Proceedings of the 5th International Conference on Information Systems Security and Privacy* (pp. 26-37). https://doi.org/10.5220/0007247500260037

Oates, B. J. (2005). *Researching information systems and computing*, Sage.

Padayachee, K., & Worku, E. (2017). Shared situational awareness in information security incident management. In *12th International Conference for Internet Technology and Secured Transactions* (pp. 479-483). https://doi.org/10.23919/ICITST.2017.8356454

Ponterotto, J. G. (2005). Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. *Journal of Counseling Psychology*, *52*(2), 126. https://doi.org/10.1037/0022-0167.52.2.126

Reiter, B. (2013). *The epistemology and methodology of exploratory social science research: Crossing Popper with Marcuse* (Paper 99, pp. 1-22). University of South Florida Government and International Affairs Faculty Publications.

Sandberg, J., & Alvesson, M. (2011). Ways of constructing research questions: Gap-spotting or problematization?. *Organization*, *18*(1), 23-44. https://doi.org/10.1177/1350508410372151

Saunders, M. N., et al. (2019). Understanding research philosophy and approaches to theory development. In M N. K. Saunders, P. Lewis, & A. Thornhill (Eds.), *Research methods for business students* (pp. 128-170. Harlow, Pearson Education.

Scarfone, K., et al. (2008). *Computer security incident handling guide, SP 800-61 Rev. 1*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r1

Schramm, W. (1954). How communication works In W. Schramm (Ed.), *The process and effects of mass communication* (pp. 3-26). University of Illinois Press.

Sellnow, D. (2005). *Confident public speaking* (2nd ed.). Thomson/Wadsworth.

Syahrial, H., et al. (2019). Information security policy compliance model at Indonesian government institutions: A conceptual framework. In J. Abawajy, M. Othman, R. Ghazali, M. Deris, H. Mahdin, & T. Herawan (Eds.), *Proceedings of the International Conference on Data Engineering* (pp. 393-401). Springer. https://doi.org/10.1007/978-981-13-1799-6_41

Taylor, S., et al. (2007). ITIL service design (3rd ed.). TSO publications.

Tøndel, I. A., et al. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42-57. https://doi.org/10.1016/j.cose.2014.05.003

Valecha, R., et al. (2012). Messaging model for emergency communication. In *Proceedings of the Mid-West Association of Information Systems.*

Velten, J. C., & Arif, R. (2016). The influence of snapchat on interpersonal relationship development and human communication. *The Journal of Social Media in Society*, *5*(2), 5-43.

Webb, J., et al. (2014). A situation awareness model for information security risk management. *Computers & security*, *44*, 1-15. https://doi.org/10.1016/j.cose.2014.04.005

Werlinger, R., et al. (2010). Preparation, detection, and analysis: The diagnostic work of it security incident response. *Information Management & Computer Security*, *18*(1), 26-42. https://doi.org/10.1108/09685221011035241

Wiant, T. L. (2005) Information security policy's impact on reporting security incidents. *Computers & Security*, *24*(6), 448-459. https://doi.org/10.1016/j.cose.2005.03.008

Wood, J. T. (2012). *Communication in our lives* (6th ed.). Wadsworth Publishing, Cengage Learning.

Wood, J. T. (2014). Communication mosaics: An introduction to the field of communication (7th ed.). Wadsworth Publishing, Cengage Learning.

Wooding, S., et al. (2003). *Rising citizen awareness of information security: A practical guide*. eAware Consortium.

Yohannes, T., et al. (2019). Information security incident response management in an Ethiopian bank: A gap analysis. In *Twenty-fifth Americas Conference on Information Systems* (pp. 1-13).

APPENDIX A: INTERVIEW GUIDE

Note: The interview guide was designed to be conversational.

PART I: INTERVIEW QUESTIONS (EXPERTS ONLY)

Background

1.1. How many employees currently work in your organization?

1.2. To which of the following organizational categories does your organization belong?

Organizational category	Specialization
Government organization	□Education □Service □Health □Military □Technology □Energy
Non-governmental organization	□Local NGO □International NGO
Private Sector	□Commercial □Non-commercial
Corporate organization	□
Security organization	□
Public relations & Marketing	□
Other	□

1.3. Which of the following Information systems does your organization deploy and utilize?

□ Business and Commercial Information Systems

□ Customer Information Systems

□ Employee Management

□ Data and Information Security

□ National Security Systems

□ Telecom & Network systems

□ Other_____

1.4. Which of the following information security mechanisms does your organization utilize?

Information security mechanism	Specific methods
Technical Information Security	□Antivirus and Anti-spyware □Firewall □Virtual private network □Encryption & Decryption □Intrusion and Detection System (IDS) □Endpoint □Backup and restore □Wireless security
Physical Information security	□Room □Human security □Hardware
System and Data Security	□Systems and network security □Business communications security □Web and application security
Non-Technical Information security	□Security employee training and awareness □Security policies and procedures □Policy: Corporate security policy, password policy, hiring and disciplinary policy
Other	□

1.5. Which of the following aspects of information security awareness issues are addressed in your organizational information security policy document?

□ Security incident handling

□ Risk awareness

□ Account usage (Username and Password)

□ Internet application (Email, Downloading, and social media utilization)

□ Software installation

□ Antivirus installation and usage

□ Other_____

1.6. Does your organization have a specific policy document on information security incident management issues?

1.7. If your answer to the above question is 'NO', provide possible reasons for the lack of information security and incident management policies?

2. Information security incident management

2.1. Which of the following role-players in your organization is assigned the responsibility of developing incident management processes?

□ ICT office

□ Management or Executive body

□ National regulatory body

□ Organizational stakeholders

□ Other _____

2.2. Which of the following management levels plays an active role in awareness and communication regarding information security incident management?

□ Top-Level Management

□ Middle-Level Management

□ Low-Level Management

□ Not Applicable

2.3. Describe the role that management currently plays/should play in information security incident awareness?

2.4. Describe the role that management currently plays/should play in information security incident communication?

2.5. Which of the following standards does your organization, currently comply?

□ ISO/IEC 27001

□ ISO/IEC 27002 Standard

□ ISO/IEC 27035 Standard

□ The ITIL Framework

□ NIST Special Publication 800-61

□ ENISA - Good Practice Guide for Incident Management

□ Nor SIS - Guideline for Incident Management

□ SANS: Incident Handler's Handbook

□ COBIT 5

□ ISMM

□ IEEE 802.11

□ Other _____

2.6. If your organization uses any of the above information security management standards, how does it implement this with respect to information security incident management processes?

2.7. If your organization does not apply any of the above information security incident management standards, provide possible reasons for the lack of standard usage.

2.8. Does your organization have any formal agreement with employees regarding information security incident management process issues?

□ Yes

□ No

2.9. If your answer to the above question is 'no', provide possible reasons for the lack of such agreement between the organization and the employees.

2.10 Assess your organizations information security incident management processes

No	How does the organization manage the following incident management processes?	Does it have a formal document?	Do they plan for it?	Is it supported by ICT systems?	Is it supported by Decision Makers?
1	Incident preparation and definition				
2	Incident identification/detection				
3	Incident assessment and analysis				
4	Incident response				
5	Incident awareness, understanding, anticipation and knowledge of employees				
6	Incident communication and reporting				
7	Information security policy efficiency				

Risk understanding and identification

2.11. Rate the level of information security incident awareness and risk understanding of employees with respect to the following indicators? **(***Excellent, Very good, Good, Satisfactory, Fair, Poor)*

No	Information security incident awareness indicators	Top-Level Mgt	Middle-Level Mgt	Low-Level Mgt	End-Users	ICT Experts
1	Knowledge about ICT system and					

	components					
2	Information security competence					
3	Reporting security incidents					
4	Up-to-date knowledge about relevant threats					
5	Learning from previous incidents					

2.12. Does your organization have a specific workflow for information security incident management processes?

□ Yes

□ No

2.13. If you have answered 'YES' to the previous question, comment on the following aspects:

2.13.1. How is it prepared and maintained?

2.13.2. How is it communicated to the members of the incident management team?

2.14. Which of the following methods support managers in increasing awareness of information security incident management policies in your organization?

No	Awareness raising methods	Description and specific tools
1	□Promotional methods	Screen savers, Banners on the intranet, Hyperlinks from the intranet homepage to the security page, Articles in the internal publication, Posters, Puzzles and games, Pre-printed note pads or sticky notes, T-shirts, Mugs and cups, Mouse pads, Stickers
2	□Enforcing methods	Underwriting security principles, Confidentiality agreements, Required awareness exam or test, Disciplinary actions for non-compliance, Inclusion in annual evaluations or, promotion criteria, Rewarding mechanisms
3	□Educational methods	Slide presentation, training, brief targeted session, Online learning module, Demonstration, Video, Workshops
4	□Informational methods	Leaflets, Short articles or news stories, Intranet security web site postings, E-mail warnings, Information security guides, Tips-of-the-month, Flash cards, Newsletters
5	□Digital methods	CD-ROM or DVD materials, simulated production, Audio-visual tools, Online methods, Closed Circuit TV
6	□Face-to-face guidance method	

Adapted from (Johnson, 2006)

2.15. Which of the following reporting mechanisms does your organization use to communicate with staff about information security incidents?

□ Telephone reporting

□ Manual/paper-based reporting

□ Face-to-face contact or meeting

□ Electronic means (E-mail, Social media, Mobile phone)

□ Audio-visual/Multimedia format

□ Special software application for incident reporting

□ Other_____

2.16. How would you assess the level of an employee's communication experience with respect to information security incident management among different clusters of employees in your organization?

No	Employee Cluster	Excellent	Very Good	Good	Satisfactory	Fair	Poor
1	Top-Level management						
2	Middle-Level management						
3	Low-Level management						
4	End-users						
5	ICT Experts						

2.17. How frequently does your organization communicate regarding information security incidents?

□ When an incident happens

□ Quarterly

□ Bi-annually

□ Weekly

□ Annually

□ Monthly

□ Other_____

2.18. How does your organization communicate and report information security incidents to employees?

2.19. In your opinion, what should be done to improve the awareness and communication strategies among employees and stakeholders in order to enhance information security incident management in your organization?

2.20. What kind of challenges does your organization face regarding information security incident communication and awareness cases?

2.21. In your opinion, how can communication with regard to information security incident management be effectively integrated into your organizational information security policy?

3. Information Security Incident Management and End-users' involvement

3.1. Identify the role and relation of the various stakeholders with regard to Information security incident management issues in your organization.

Stakeholder	Role
All staff members	
Line management	
Executive management and boards of directors	
Field staff	
Laptop users	
IT department	
IT help desk	
System and/or data owners	
E-mail users	

Vendors and suppliers	
Other_____	

3.2. Does your organization involve end-users in the process of information security incident awareness and communication matters?

□ Yes

□ No

3.3. If your answer is 'YES' to the above question, describe how your organization involves end-users in the process of information security and incident management policy issues?

3.4. If your answer is 'NO' to question No 3.2, describe the reason why your organization does not involve end-users in the process of information security policy awareness and communication matters.

3.5. Which information security incident cases, regarding end-users, are taken into account by the organization?

□ All security cases

□ Only non-technical cases

□ Only technical cases

□ Some higher level policy issues

□ Other_____

PART II: INTERVIEW QUESTIONS (END-USERS ONLY)

Have you ever been involved in the setting of information incident security management guidelines in your organization?

If your answer to the above question is 'YES', describe your level of participation.

Have you ever participated in an information security incident awareness program?

If your answer to the above question is 'YES', describe your role with regard to communication and awareness aspects to improve information security incident management in your organization?

If your answer to the question 3 is 'NO', what should your organization put into practice in order to involve end-users and stakeholders to improve awareness and communication?

In your opinion, how can your organization plan and prepare better information security management through awareness and communication mechanisms?