Journal of Information Security, 2018, 9, 191-208
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

# Human Sensor Web Crowd Sourcing Security Incidents Management in Tanzania Context

**Maduhu Mshangi[1*], Edephonce Ngemera Nfuka[2], Camilius Sanga[3]**

[1]NECTA—Tanzania, Dar es Salaam, Tanzania
[2]Open University of Tanzania, Dar es Salaam, Tanzania
[3]Sokoine University of Agriculture, Morogoro, Tanzania
Email: *mshangimaduhu@yahoo.com

**How to cite this paper:** Mshangi, M., Nfuka, E.N. and Sanga, C. (2018) Human Sensor Web Crowd Sourcing Security Incidents Management in Tanzania Context. *Journal of Information Security*, **9**, 191-208.
https://doi.org/10.4236/jis.2018.93014

**Received:** May 24, 2018
**Accepted:** July 7, 2018
**Published:** July 10, 2018



## Abstract

Security incidents affecting information systems in cyberspace keep on rising. Researchers have raised interest in finding out how to manage security incidents. Various solutions proposed do not effectively address the problematic situation of security incidents. The study proposes a human sensor web Crowd sourcing platform for reporting, searching, querying, analyzing, visualizing and responding to security incidents as they arise in real time. Human sensor web Crowd sourcing security incidents is an innovative approach for addressing security incidents affecting information systems in cyberspace. It employs outsourcing collaborative efforts initiatives outside the boundaries of the given organization in solving a problematic situation such as how to improve the security of information systems. It was managed by soft systems methodology. Moreover, security maturity level assessment was carried out to determine security requirements for managing security incidents using ISO/IEC 21827: Systems security engineering capability maturity model with a rating scale of 0 - 5. It employed descriptive statistics and non-parametric statistical method to determine the significance of each variable based on a research problem. It used Chi-Square Goodness of Fit Test ($X^2$) to determine the statistical significance of result findings. The findings revealed that security controls and security measures are implemented in ad-hoc. For managing security incidents, organizations should use human sensor web Crowd sourcing platform. The study contributes to knowledge base management learning integration: practical implementation of Crowd sourcing in information systems security.

## Keywords

Human Sensor Web, Crowd Sourcing, Geographical Information System, Security Incidents, System Architecture

## 1. Introduction

The information systems (IS) in cyberspace experience various security incidents across the globe. An incident reporting, responding and handling is a cornerstone in managing security incidents by minimizing loss and impact through mitigating or reducing risks to an acceptable level, and quick recovery of IS from disruptive events. It is an increasingly problematic situation; researchers are trying to address. Thus, ensuring the security of IS in cyberspace is debatable due to the rapid growth of security incidents affecting IS. The study employs innovative human sensor web Crowd sourcing security incidents approach to improve the security of IS [1]. Human sensor web (HSW) Crowd sourcing security incidents management is an innovative approach for addressing security incidents using collaborative initiatives efforts outside the boundaries of the given organization, sector or country in solving a problematic situation such as how to improve the security of IS [2]. This involves making a public call to the community crowd by inviting people with diverse skills, experiences to respond to the public call to find out the solution to the problem.

The HSW Crowd sourcing uses the community in solving the problem instead of relying on internal efforts (internal resources). This public call to the community normally is accompanied with a prize to contest. This creates a room for people with diverse skills, knowledge, expertise, and experience to contest in finding the best optimal solution. This can result in getting correct solution, solving the complex problematic situation which could be impossible to solve by only depending on internal efforts (internal resources). HSW Crowd sourcing has been applied in various sectors for addressing various problems. For example, it has been applied in addressing real-world problematic situations such as empowering communities in East Africa in water service provision through information from human sensor webs in Zanzibar [3]; rabies surveillance system for humans and animals in Kilosa district, Tanzania [4]. This study seeks to extend the application of HSW Crowd sourcing to security incidents management for IS in cyberspace.

HSW Crowd sourcing security incidents management enables interconnected people in the community to act as a sensor for reporting and responding to security incidents over the web or mobile-based platform. The function of responding to security incidents such as cybercrimes attacks in cyberspace is outsourced to people in the cyberspace [5] [6]. HSW enables people to interact with their devices [1] [3] to forward and respond to security incidents stimuli designated to receiving server [7]. The problem of security incidents can be observed and reported by human sensors in real-time basis [8].

Many uncertainties still exist on reporting, responding and handling of security incidents affecting IS in cyberspace. This has been a long-standing problematic situation which researchers have been trying to address in order to come out with a solution. The approach of Crowd sourcing has been applied in different sectors to address the given problems, but its application to address security

concerns such as security incidents managements in real time has been lagging behind. Practical techniques for implementation of HSW for Crowd sourcing platform in knowledge base management learning have not been undertaken into account [7] [9] [10] [11] in information systems security. HSW Crowd sourcing platform in knowledge base management learning for security incidents management integration is lacking or ineffectively implemented in solving real-world problematic situation such as how to improve the security of IS.

The main objective of this research was to develop human sensor web Crowd sourcing security incidents management platform for addressing the problematic situation on how to improve the security of information in IS (during capturing, processing, storage, and transmission), a case study of the education sector in Tanzania.

This paper presents an innovative human sensor web Crowd sourcing geographical information system platform for instant managing of security incidents, a case study of the education sector in Tanzania. The rest of this paper is organized as follows: Section 2 presents the related work. Section 3 presents the materials and methods employed in this study. Section 4 presents the results findings and discussion. Section 5 describes the developed prototype for human sensor web Crowd sourcing platform for security incidents management. Section 6 presents software development crowd: using the crowd as an innovation partner. Finally, Section 7 presents the conclusion.

## 2. Related Work

Managing security incidents effectively involves detective and corrective controls designed to recognize and respond to events and incidents, minimize adverse impacts, gather forensic evidence [12] [13] [14] and take actions for improvements or other risk treatments [15] [16]. Thus, it involves preparing to deal with incidents; identifying and reporting information security incidents; assessing the incidents and making decisions [7] [15]: patch things and get back to business quickly, or collect forensic evidence; respond to incidents; learning the lessons: making changes that improve the processes [17].

Consequently, information security incidents are bound to occur to some extent, even in organizations that take their information security extremely seriously [5] [6]. The study selected an information security incident management security domain as a case study for developing a prototype for human sensor web for Crowd sourcing platform: central repository information security incidents management. Security incidents such as cybercrimes affecting IS in cyberspace are on the rise [18] [19]. The developed platform serves as a tool for reporting, communicating, sharing, visualizing the reported security incidents and responding to adverse events. This assists the incident response team (IRT) in receiving, analyzing, and responding to information security incidents reported through the human sensor web Crowd sourcing [5] [6] [11] [20] security incidents platform.

## 3. Materials and Methods

The study employed mixed research methods (quantitative and qualitative) for data collection and analysis [21]. The quantitative research method employed [22] was survey questionnaire (**Appendix A**). The qualitative research methods employed were semi-structured interview using electronic assessment tools [23] for focused group/individuals and documentary review [24]. The data collection was conducted in seven organizations under study in the education sector in Tanzania [25] [26]. The seven organizations selected are those which are mainly involved in the educational assessment and management of education in Tanzania, because of their high impact on the whole sector. In this study, the names of the seven selected organizations referred as K, L, M, N, O, P and Q were not disclosed for confidentiality purpose. In this case, the level of analysis is organizational. The research study adopted soft systems methodology (**Figure 1**) to guide the research process. Soft systems methodology (SSM) is an approach to tackling ill-defined complex problematic situation involving human factor [27] [28] [29] such as security incidents affecting IS.

### 3.1. Sampling Techniques

The sample size for this study was 154 respondents from seven organizations in the education sector; the distributions of these respondents are presented in **Table 1**. This sample was selected using purposive and stratified random sampling

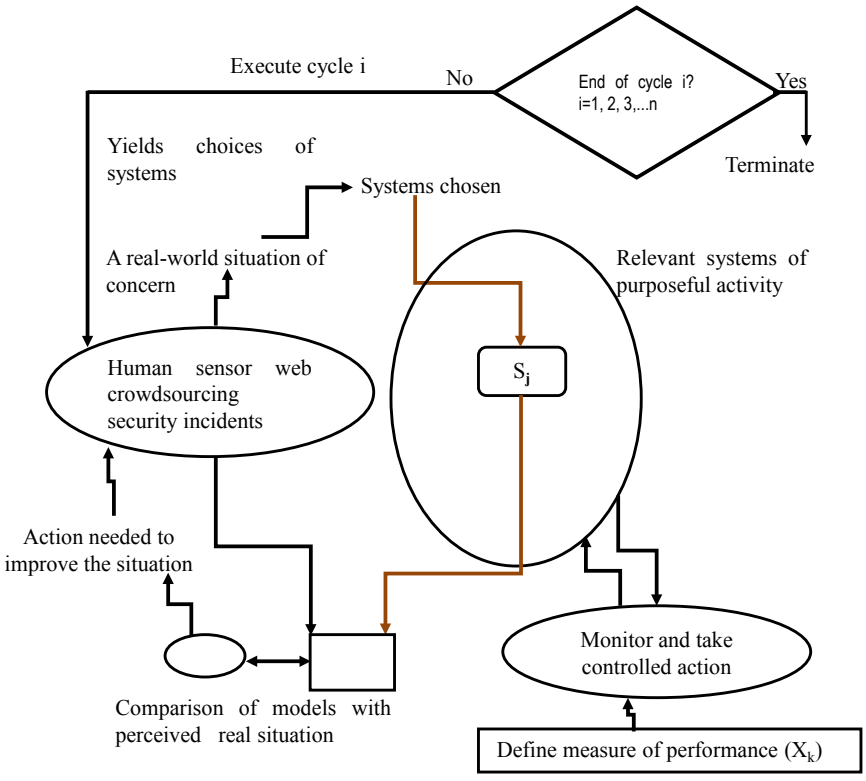


**Figure 1.** How soft systems methodology was used [28] [30]. Key: $S_j$ is the given system under improvement which undergo cycles of iterations (i = 1, 2, 3, ⋯); j = 1, 2, 3, ⋯

**Table 1.** Respondents.

| Respondents | Organization | | | | | | | Total |
|---|---|---|---|---|---|---|---|---|
| | O | P | L | M | Q | K | N | |
| ICT Experts(Expected) | 4 | 4 | 4 | 22 | 4 | 3 | 4 | **45** |
| ICT Experts (Actual response) | 4 | 2 | 3 | 20 | 4 | 3 | 4 | **40** |
| Management (Expected) | 5 | 5 | 6 | 22 | 7 | 5 | 5 | **55** |
| Management (Actual response) | 4 | 5 | 4 | 21 | 6 | 5 | 5 | **50** |
| Users of IS (Expected) | 2 | 3 | 2 | 30 | 7 | 5 | 5 | **54** |
| Users of IS (Actual response) | 2 | 3 | 4 | 19 | 5 | 2 | 3 | **38** |
| **Total Respondents (Sample)** | **11** | **12** | **12** | **74** | **18** | **13** | **14** | **154** |
| **Total Actual Respondents** | **10** | **10** | **11** | **60** | **15** | **10** | **12** | **128** |
| **Survey Response Rate%** | **91%** | **83%** | **92%** | **81%** | **83%** | **77%** | **86%** | **83%** |

Source: [25] [26].

techniques. Purposive sampling relies on the judgment of the researcher when it comes to selecting the units (e.g., people, cases/organizations, events, pieces of data) that are to be studied [24] [31]. The selected respondents in this study were those involved in the managing of ICT and security of IS; procurement decisions of ICT equipment/accessories; ICT use and compliances. The respondents were selected based on the organization structure. Taking into account these aspects, the purposive sampling technique was the optimal choice for sampling design. The respondents (**Table 1**) were comprised of top management (Permanent Secretary, Commissioners, and Chief Executive Officers), senior management (Directors, Chief Financial Officers, Divisions/ Head of Departments), operations management (Head of Units/Sections), ICT experts (Network/Systems Administrators, IT security specialists and other ICT Staff); and normal users (operations staff who interact with IS and know the business processes) from the 7 organizations under study.

A stratified random sampling was used for selecting respondents for normal users of IS from sampling frame (list of all normal users of IS for 7 organizations under study) based on research questions. The sampling frame was divided into 7 strata (strata K, L, M, N, O, P, and Q) comprising of normal users of IS from 7 organizations. The respondents from each stratum were selected using random sampling [24] [31].

### 3.2. Data Collection and Analysis

The data collection and analysis were based on systems security engineering-capability maturity model (SSE-CMM) [32] with a rating scale of 0-5: minimum 0 and maximum 5 was used; 0-not performed (non-existent); 1-performed informally (unplanned/ad-hoc); 2-partially implemented (planned); 3-implementation is in progress (planned and tracked); 4-fully implemented (well defined and auditable); 5-fully implemented and regularly up-

dated (monitored and audited for compliance). The research study employed survey questionnaire (**Appendix A**), interview and documentary review techniques for data collection. The designed survey questionnaire was based on SSE-CMM. Due to the nature of the research problem, soft systems methodology [19] [28] [29] [30] was adopted to manage the analysis of collected data in a systematic way and circular fashion [28]. Collected data were first cleaned and coded before being analyzed.

The analysis was carried out using both descriptive statistics and non-parametric statistical method to determine the significance of each variable based on a research problem. The statistical data analysis method employed was the Chi-Square Goodness of Fit Test ($X^2$). This is given by Equation (1).

$$X^2(df) = \sum_i^N \frac{(O_i - E_i)^2}{E_i} \tag{1}$$

In Equation (1), $df$ is the degree of freedom; $O_i$ is the observed frequency for each category $i$; $E_i$ is the expected frequency for each category $i$. In this study, the category I = 0, 1, 2, 3, 4, 5 is based on SSE-CMM. Thus, for $k$ categories, $df = k-1$; $\sum O_i = \sum E_i = N$; $E_i = Np_i$; $p_i = \frac{1}{k}$; $\sum p_i = 1$; where $p_i$ is proportional to expected frequency for category $i$ in $k$ categories. In this study $k$ = 6; hence $p_i = 1/6$ for each category $i$. $N$ is the total number of observation in the sample size of respondents category under study.

In this study, with expected frequency $E_i$ and observed frequency $O_i$, the null and alternative hypothesis can be stated as follows.

$$H_0 : O_i = E_i$$

The variable $x_i$ for security measures or security controls does not contribute to improving the security of information in IS.

$$H_1 : O_i \neq E_i$$

The variable $x_i$ for security measures or security controls does contribute to improving the security of information in IS.

where $H_0$ and $H_1$ denotes the null hypothesis and the alternative hypothesis respectively. The hypothesis was tested at 95% confidence interval, significance level $\alpha = 0.05$. The choice of Chi-Square Goodness of Fit Test ($X^2$) was due to the nature of research problem and nature of research data collected.

## 4. Results and Discussions

This section presents the results findings for addressing the problematic situation on how to improve the security of information in IS (during capturing, processing, storage, and transmission), a case study of the education sector in Tanzania. The data analysis was managed by SSM (**Figure 1**) in a circular fashion by executing every cycle $i$ for a given iteration cycle ($i$ = 1, 2, 3, ⋯ n) for each criterion in security incident management security domain. The data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square

goodness of fit test with 0.05 significance level and df = 5 was carried to assess the effectiveness, efficiency, and efficacy of information security incident management controls implementation in the education sector in Tanzania. It was hypothesized that effective implementation of security incident management controls contributes to improving the security of IS. The results are as follows.

Table 2 presents views when the respondents were asked whether the given organization have incident-handling procedures in place to report and respond to security events throughout the incident lifecycle, including the definition of roles and responsibilities. The majority of respondents (71.8%: IT staff) revealed that organizations have implemented incident-handling procedures in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0 - 5 (Table 2). Likewise, the findings revealed the views when management staff were asked (similar question) whether a given organization has an incident response team in place and is functional. The majority of respondents (62%: management staff) revealed that organizations do not have functional incident response team (scale 0); with a median of 0 in SSE-CMM rating scale of 0 - 5 (Table 2). The findings

**Table 2.** Incident management and response.

| | Observed N | Percent |
|---|---|---|
| IT staff: Incident handling procedures and reporting | | |
| 0-Not performed (non-existent) | 11 | 28.2 |
| 1-Performed informally (unplanned) | 26 | 66.7 |
| 2-Partially implemented (planned) | 2 | 5.1 |
| Total | 39 | 100.0 |
| Median = 1, $E_i$ per category i = 1/6*39 = 6.5, $X^2(df=5)=84.231$, p = 0.000, $\sum E_i = \sum O_i = N = 39$ | | |
| Management staff: Incident response team | | |
| 0-Not performed (non-existent) | 31 | 62.0 |
| 1-Performed informally (unplanned) | 19 | 38.0 |
| Total | 50 | 100.0 |
| Median = 0, $E_i$ per category I = 1/6*50 = 8.3, $X^2(df=5)=108.640$, p = 0.000, $\sum E_i = \sum O_i = N = 50$ | | |
| Users of IS: Incident reporting | | |
| 0-Not performed (non-existent) | 6 | 15.8 |
| 1-Performed informally (unplanned) | 32 | 84.2 |
| Total | 38 | 100.0 |
| Median = 1, $E_i$ per category i = 1/6*38 = 6.3, $X^2(df=5)=129.368$, p = 0.000, $\sum E_i = \sum O_i = N = 38$ | | |

revealed the views when users of IS were asked (similar question) whether they know where to report information security incidents. The majority of respondents (80%: users of IS) revealed that information security incidents are reported in ad-hoc (scale 1: unplanned), with a median of 1 in SSE-CMM rating scale of 0 - 5 (Table 2).

Moreover, the Chi-square goodness of fit test results for all the three categories of respondents (IT staff: ( $X^2(5, N=39)=84.231$, p = .000, p < 0.05), management staff: ( $X^2(5, N=50)=108.640$, p = 0.000, p < 0.05), users of IS: ( $X^2(5, N=38)=129.368$, p = 0.000, p < 0.05)) in Table 2 revealed that organisations should implement security incident management controls such as HSW for Crowd sourcing security incidents management. Thus, in ensuring the security of IS, a given organization should implement incident management controls such as HSW Crowd sourcing security incidents management. Furthermore, it includes incident-handling procedures in place to report and respond to security events throughout the incident lifecycle; security incident response team in place and is functional; awareness to users of IS on how, what and where to report information security incidents.

Moreover, interview and documentary review results revealed that IS in cyberspace are affected by security incidents such as the hacking of IS; computer viruses; theft of computers; laptops in the office and theft of laptops during travels; information resources capacity limit such as web server capacity limit, LAN, WAN or Internet bandwidth limit capacity; hardware or software failures; fire; floods; developing applications using code generators frameworks, open sources software or content management systems (CMS) such Joomla without shutdown open holes (vulnerabilities).

## 5. Human Sensor Crowd Sourcing Platform for Security Incidents Management

The study proposes human sensor web crowd sourcing platform for managing security incidents. It comprises of system architecture, interfaces architecture for HSW crowd sourcing security incidents, mobile-based sub-system, interactive reports and database repository.

### 5.1. System Architecture for Human Sensor Web Crowd Sourcing

The proposed system architecture for HSW crowd sourcing security incidents comprises of web-based geographic information system (GIS), GIS server, interactive geo-maps, database repository, SMS alert, report security incidents, web server and interactive reports (Figure 2).

### 5.2. Interface Architecture for HSW Crowd Sourcing Security Incidents

The interface architecture for HSW crowd sourcing comprises of security incidents reporting, mobile base sub-system: SMS Alert, visualize security incidents in the GIS and interactive reports (Figure 3). The descriptions are as follows:

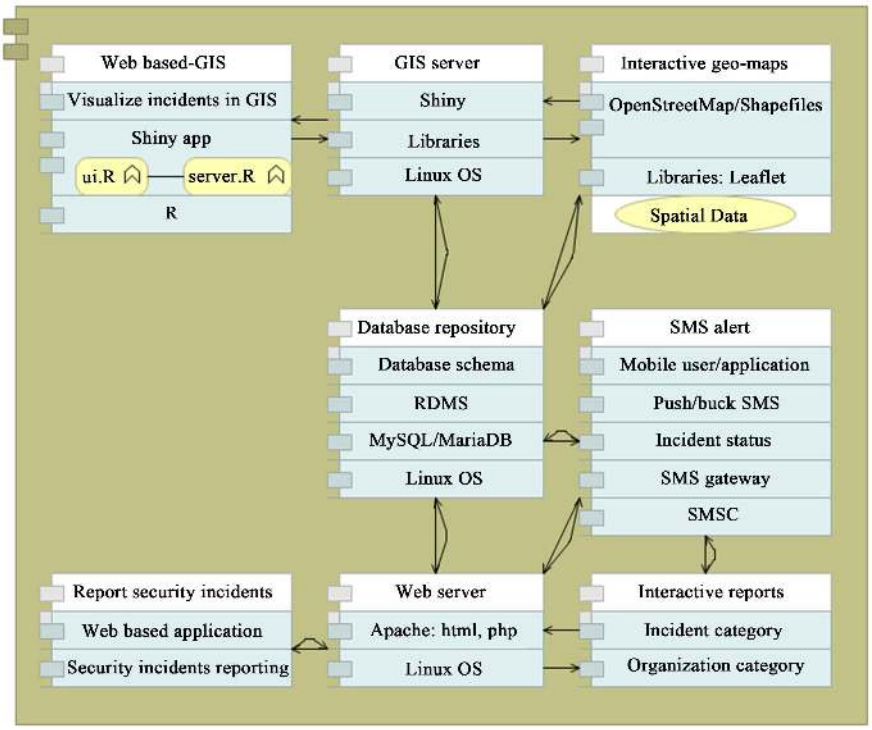


**Figure 2.** System architecture for human sensor web Crowd sourcing.

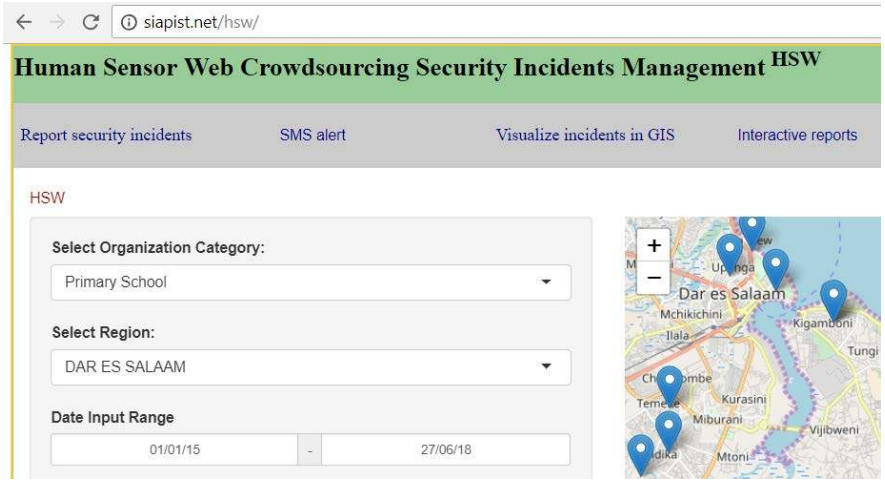


**Figure 3.** The user interface for human sensor web [33].

### 5.2.1. Security Incidents Reporting

Figure 4 presents a web-based user interface for reporting security incidents; with filled in sample data. The reporter of security incident fills in information about the incident. The reporter is required to select the category of organization, organization name in which security incident(s) has occurred; the incident category and enter other details about the incident(s) before submitting the data to the database-repository.

### 5.2.2. Mobile-Based Sub-System: SMS Alert

The HSW for Crowd sourcing security incidents management system has

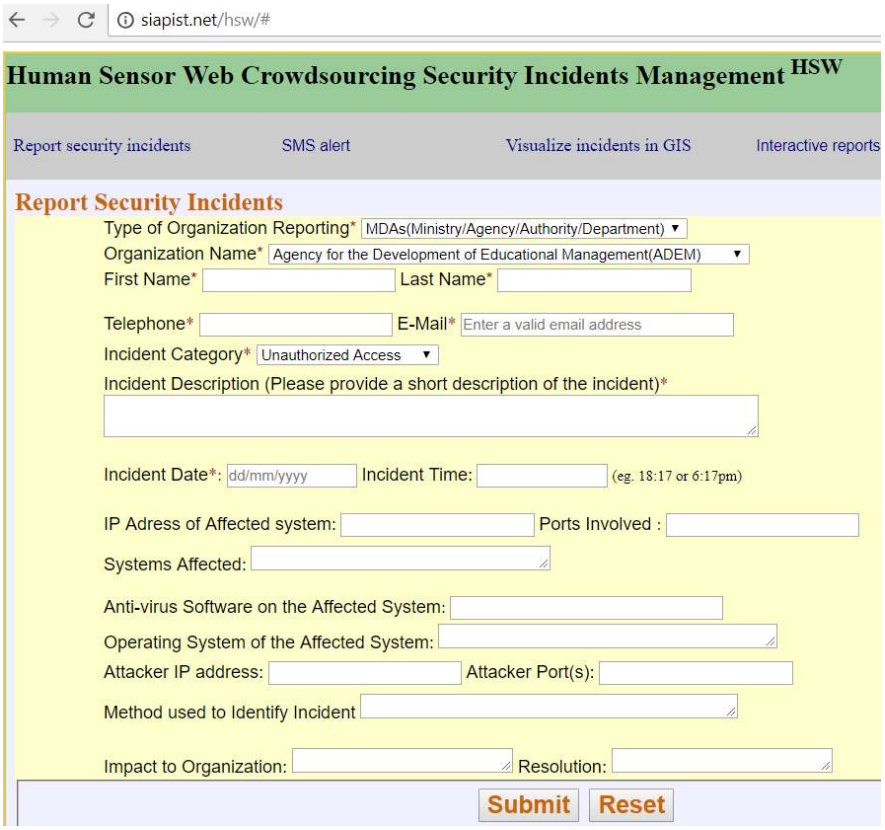


**Figure 4.** The user interface for reporting security incidents.

mobile-based sub-system for pushing and pulling SMS (**Figure 3**). Push messages are those SMS that the organization chooses to send out to a mobile subscriber (customers, reporters), without the mobile subscriber initiates a request for the information. Pull messages are those SMS that are initiated by a subscriber (customer, reporter), using a mobile phone to obtain information or perform other operations. The pull SMS will involve SMS interactions by requesting incidents status from the database repository. The system has two sub-menus under SMS interactions menu: Push SMS and Pull SMS.

**1) Push SMS**

This menu gives a functionality of pushing SMS to many recipients at once (**Figure 3**). The central incidents response team can create SMS and broadcast to all relevant parties about critical information for security incident such as dangerous viruses; hackers. Furthermore, the "Push SMS" menu has functionalities for sending SMS to users/entities subscribed to that SMS; fired based on condition met or triggered. For example, a dangerous virus which erases all data in hard disks; the system can be configured to send SMS to all organizations/security incidents response teams for information, sharing solution; and any remedial action.

**2) Pull SMS**

The user of the HSW for crowding security incidents system can send SMS in a pre-defined format to request information about information security inci-

dents in real time (Figure 3). These can include requesting statistics of information security incidents by incident category, by organization category.

### 5.2.3. Visualize Security Incidents in GIS

Web-based GIS is a geographical web-based application for visualizing reported security incidents in interactive geographical maps. The web-based GIS has been developed using R programming and shiny. The R language is widely used for data mining, developing statistical software and data analysis. Shiny is a web framework for R which uses a reactive programming model to simplify the development of R-powered web applications. Shiny apps have two components: a user-interface script (ui.R) and a server script (server.R). The user-interface (ui.R) script controls the layout and appearance of the application. The server.R script contains the instructions that computer needs to build the given application on execution.

The web-based GIS is hosted and executed by the GIS server (shiny server). The GIS server hosts shiny web applications and interactive documents online. The GIS server process and manipulates data such as reported security incidents, spatial data from the database repository. The GIS server calls various libraries such as leaflet for integrating interactive geo-maps; MySQL: interface to MySQL/MariaDB database repository. The web-based GIS allows the users to visualize the reported security incidents by selecting organization category; region and date range (Figure 3). The visualization of reported security incidents includes a histogram, 3D pie chart and interactive maps visualization using markers.

**1) Visualization in GIS using Histogram**

The HSW Crowd sourcing platform can visualize the reported security incidents through histogram (Figure 5). The histogram portrays the reported security incidents in a given category over a date range.

**2) Visualization in GIS Using a 3D Pie Chart**

HSW Crowd sourcing platform can visualize the reported security incidents

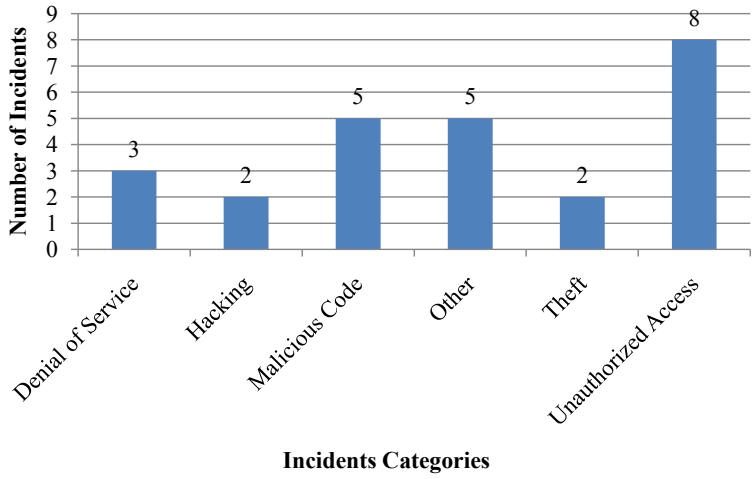


Figure 5. Visualize security incidents through histogram in GIS.

through 3D Pie chart (Figure 6). The 3D Pie chart portrays the reported security incidents in a given category over a date range. The area of each portion represents the relative proportion of data points falling into a given incident category (Figure 6).

**3) Interactive maps visualization using markers**

The security incidents are presented in interactive maps using markers (Figure 7) on GIS map. The user should select organization category, region, and incident date range to visualize the security incidents.

#### 5.2.4. Interactive Reports

This interface is comprised of interactive reports for security incidents management. The web-based "interactive reports" interface includes viewing the report by incidents category and by organization category (Figure 3).

**1) View by Incidents Category**

View by incidents category menu gives statics by category over a date range for information security incidents reported (Figure 3).

**2) View by Organizations Category**

View by organizations category menu gives statics by category over a date range for information security incidents reported (Figure 3).

### 5.3. Database Repository

Figure 8 presents the logical view of the database for HSW crowd sourcing security incidents management platform. It defines how the data is organized and how the relations among them are associated.

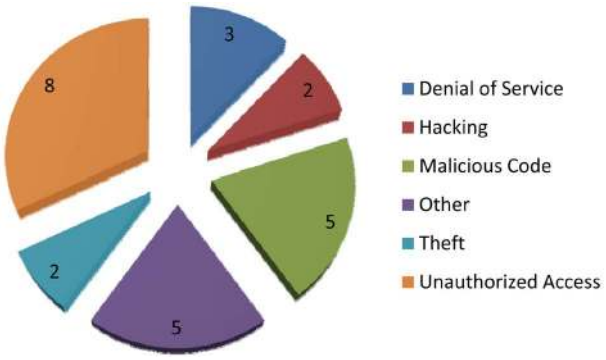


Figure 6. Visualize security incidents through 3D-pie chart in GIS.


Figure 7. Visualization in the geographical map.

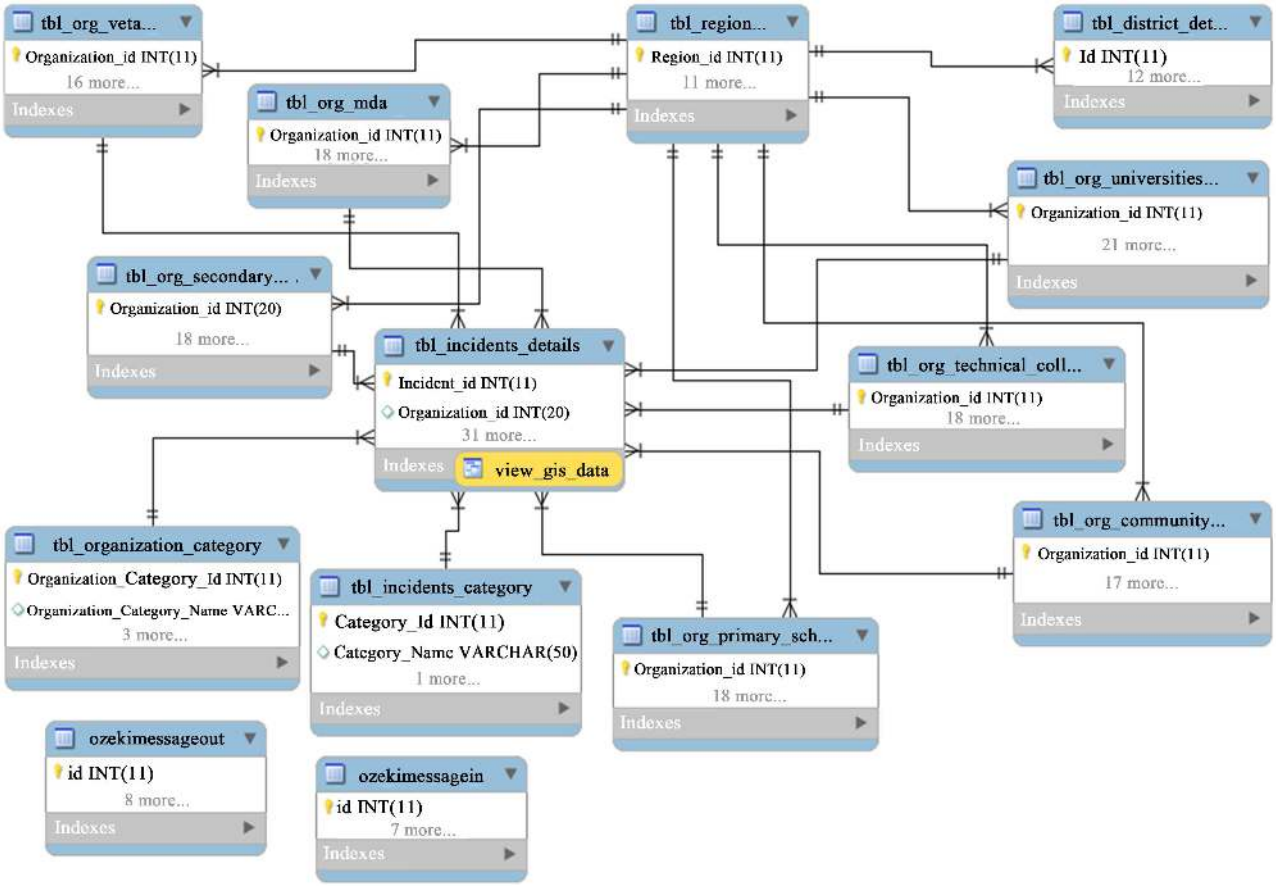


**Figure 8.** The logical view of the database repository.

## 6. Software Development Crowd: Using the Crowd as an Innovation Partner

The development of HSW Crowd sourcing security incidents management platform was achieved using crowd and it was guided by SSM in a cyclic fashion [34] [35]. Software development crowd is an emerging area of software engineering as opposed to traditional software engineering methodologies such as waterfall model, agile software development [11] [36]. It is an open call for participation [7] [20] in any task of software development, including documentation, design, coding, and testing [9]. These tasks are normally conducted by either member of a software enterprise or people contracted by the enterprise [11] [36]. But in software Crowd sourcing, all the tasks can be assigned [7] to anyone in the general public [5] [9]. The Crowd sourcing platform was developed participatory with crowds and thereafter, crowds used it for reporting security incidents such as cyber-attacks, hacking, cracking, viruses in real time [33]. The human sensor web Crowd sourcing security incidents management platform was used for searching, querying and sharing solutions for security incidents challenges based on dynamic knowledge base management learning. Thus, human sensor web for Crowd sourcing platform creates a dynamic knowledge base management learning for improving information systems security.

## 7. Conclusion

The paper proposes human sensor web Crowd sourcing platform for security incidents management. It is an innovative approach for addressing security incidents affecting information systems in cyberspace. It uses outsourcing collaborative initiatives efforts outside the boundaries of the given organization. The human sensor web incidents management platform comprises of system architecture, interface architecture, mobile-based sub-system, interactive reports and database repository. Open source software tools were used in creating the platform and the resulting data contained in the Crowd sourcing platform is open data. The proposed HSW Crowd sourcing platform creates a knowledge base management learning database repository for security incidents management. It employed descriptive statistics and non-parametric statistical method to determine the significance level contribution for improving the security of information systems. It used Chi-Square Goodness of Fit Test ($X^2$) to determine the statistical significance of result findings. The results revealed that implementation of security controls and security measures for managing security incidents are done in an ad-hoc manner. Thus, for improving the security of information systems, organizations should use human sensor web Crowd sourcing platform for security incidents management. The future research work is to extend human sense web Crowd sourcing to cybersecurity whistleblowers using homomorphic cryptography techniques.

## References

[1] Tsega, H., Lemmens, R., Kraak, M.J. and Lung, J. (2015) Towards a Smarter System for Human Sensor Web. *IEEE International Conference on Pervasive Computing and Communication Workshops* (*PerCom Workshops*), St. Louis, MO, 14-19. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7133986&isnumber=7133953

[2] Verma, R. and Ruj, S. (2014) Security Services Using Crowd Sourcing. *Procedia Computer Scienc*e, **32**, 505-512.

[3] Verplanke, J., Becht, R., Miscione, G., Kimara, H., Benz, H., Jürrens, E., Yen, C. and Sung, S.Y. (2010) Empowering Communities in East Africa in Water Service Provision through Information from Human Sensor Webs. ftp://ftp.itc.nl/pub/pgis/HSW/HSW%20final%20report.pdf

[4] Kipanyula, M.J., Geofrey, A.M., Fue, K.G., Mlozi, M.R.S., Tumbo, S.D., Haug, R. and Sanga, C.A. (2016) Web and Mobile Phone Based Rabies Surveillance System for Humans and Animals in Kilosa District, Tanzania. *International Journal of Information Communication Technologies and Human Development*, **8**, 47-59.

[5] Lasnia, D., Broering, A., Jirka, S. and Remke, A. (2010) Crowd Sourcing Sensor Tasks to a Socio-Geographic Network. In: 13*th AGILE International Conference on Geographic Information Science* 2010, Guimarães, Portugal, 1-8. http://plone.itc.nl/agile_old/Conference/2010-guimaraes/ShortPapers_PDF/98_DOC.pdf

[6] Kamel, B.M.N., Resch, B., Crowley, D.N., Breslin, J.G., Sohn, G., Burtner, R., *et al.* (2011) Crowd Sourcing, Citizen Sensing and Sensor Web Technologies for Public and Environmental Health Surveillance and Crisis Management: Trends, OGC

Standards and Application Examples. *International Journal of Health Geographics*, **10**, 38-67.

[7] Fue, K., Geoffrey, A., Mlozi, M.R., Tumbo, S.D., Haug, R. and Sanga, C.A. (2016) Analyzing Usage of Crowd Sourcing Platform Ushaurikilimo' by Pastoral and Agro-Pastoral Communities in Tanzania. *International Journal of Institutional Technology and Distance Learning*, **13**, 3-19. http://www.itdl.org/Journal/Dec_16/Dec16.pdf

[8] Havlik, D., Schade, S., Sabeur, Z.A., Mazzetti, P., Watson, K., Berre, A.J. and Mon, J.L. (2011) From Sensor to Observation Web with Environmental Enablers in the Future Internet. *Sensors*, **11**, 3874-3907.

[9] Karim, R. (2013) Using the Crowd as an Innovation Partner. Retrieved April 1, 2018. https://hbr.org/2013/04/using-the-crowd-as-an-innovation-partner

[10] Kasita, C. and Laizer, L.S. (2013) Information and Knowledge Management Security Architecture for Tanzania Higher Learning Institutions' Data Warehouse. *Information and Knowledge Management*, **3**, 25-32. http://www.iiste.org/Journals/index.php/IKM/article/view/7996/8329

[11] Sanga, C., Phillipo, J., Mlozi, M.R.S., Haug, R. and Tumbo, S.D. (2016) Crowd Sourcing Platform "Ushaurikilimo" Enabling Questions Answering between Farmers, Extension Agents and Researchers. *International Journal of Instructional Technology and Distance Learning*, **13**, 19-28. http://www.itdl.org/Journal/Oct_16/Oct16.pdf

[12] Microsoft (2002) The STRIDE Threat Model. https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx

[13] Microsoft (2015) Microsoft Advanced Threat Analytics. https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

[14] Mbowe, J.E., Msanjila, S.S., Oreku, G.S. and Kalegele, K. (2016) On Development of Platform for Organization Security Threat Analytics and Management (POSTAM) Using Rule-Based Approach. *Journal of Software Engineering and Applications*, **9**, 601-623. https://doi.org/10.4236/jsea.2016.912041

[15] Cichonski, P. and Scarfone, K. (2012) Computer Security Incident Handling Guide (Draft) Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology (NIST), Revision 2, 1-57. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[16] ISO/IEC (2016) ISO/IEC 27035:2011 Information Technology—Security Techniques—Information Security Incident Management. http://www.iso27001security.com/html/27035.html

[17] Coole, M., Corkill, J. and Woodward, A. (2012) Defence in Depth, Protection in Depth and Security in Depth: A Comparative Analysis towards a Common Usage Language DEPTH: A Comparative Analysis towards a Common. *Proceedings of the 5th Australian Security and Intelligence Conference*, Perth, 3-5 December 2012, 27-35. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1023&context=asi

[18] Nfuka, E.N., Sanga, C. and Mshangi, M. (2014) The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: Is This a Myth or Reality in Tanzania? *International Journal of Information Security Science*, **3**, 182-199. http://www.ijiss.org/ijiss/index.php/ijiss/article/view/72

[19] Mshangi, M., Nfuka, E.N. and Sanga, C. (2015) Using Soft Systems Methodology and Activity Theory to Exploit Security of Web Applications against Heartbleed Vulnerability. *International Journal of Computing and ICT Research*, **8**, 32-52. http://ijcir.mak.ac.ug/volume8-number2/article4.pdf

[20] Goodchild, M.F. and Glennon, J.A. (2010) Crowd Sourcing Geographic Information for Disaster Response: A Research Frontier. *International Journal of Digital Earth*, **3**, 231-241. https://doi.org/10.1080/17538941003759255

[21] Jick, T.D. (1979) Mixing Qualitative and Quantitative Methods: Triangulation in Action Mixing Qualitative and Quantitative Methods: Triangulation in Action. *Administrative Science Quarterly*, **24**, 602-611. https://doi.org/10.2307/2392366

[22] Davey, J.W., Gugiu, P.C. and Coryn, C.L.S. (2010) Quantitative Methods for Estimating the Reliability of Qualitative Data. *Journal of Multi-Disciplinary Evaluation*, **6**, 140-162. http://journals.sfu.ca/jmde/index.php/jmde_1/article/download/266/254/0

[23] EDUCASE (2015) Assessment Tool—Educause. https://library.educause.edu/~/media/files/library/2015/11/heisctool-xlsm.xlsm

[24] Cohen, L., Manion, L. and Morrison, K. (2007) Research Methods in Education. Professional Development in Education. 6th Edition, Vol. 38, Routledge, New York.

[25] PMO-RALG (2016) The Prime Minister's Office, Regional Administration and Local Government (PMO-RALG). http://www.tamisemi.go.tz/

[26] MEST (2016) Ministry of Education, Science and Technology (MEST). http://moe.go.tz/en/

[27] Checkland, P.B. (1998) Systems Thinking, Systems Practice. John Wiley & Sons Ltd., Hoboken.

[28] Sanga, C. (2010) A Technique for the Evaluation of Free and Open Sources E-Learning Systems. PhD Thesis, The University of the Western Cape, Cape Town. http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/2564/Sanga_PHD_2010.pdf?sequence=1

[29] Mshangi, M., Nfuka, E.N. and Sanga, C. (2017) An Innovative Soft Design Science Methodology for Improving Development of a Secure Information System in Tanzania Using Multi-Layered Approach. *Journal of Information Security*, **8**, 141-165. https://doi.org/10.4236/jis.2017.83010

[30] Checkland, P.B. and Scholes, J. (1990) Soft Systems Methodology in Action. John Wiley & Sons, Inc., New York. http://dl.acm.org/citation.cfm?id=130360

[31] Saunders, M.N.K., Lewis, P., Thornbill, A. and Jenkins, M. (2009) Research Methods for Business Students. 5th Edition, Pearson Education Limited, London.

[32] ISO/IEC 21827 (2008) ISO/IEC 21827:2008 Information Technology Security Techniques Systems Security Engineering Capability Maturity Model. https://www.iso.org/standard/44716.html

[33] Mshangi, M., Nfuka, E.N. and Sanga, C. (2018) Human Sensor Web Crowd Sourcing Security Incidents Management Platform. http://siapist.net/hsw/

[34] Li, W., Huhns, M.N., Tsai, W.-T. and Wu, W. (2015) Crowd Sourcing Cloud-Based Software Development. Springer, Heidelberg, New York, Dordrecht, London.

[35] Devi, V. (2013) Traditional and Agile Methods: An Interpretation. https://www.scrumalliance.org/community/articles/2013/january/traditional-and-agile-methods-an-interpretation

[36] Misra, A., Gooze, A., Watikins, K., Asad, M. and Le Dantec, C.A. (2014) Crowd Sourcing and Its Application to Transportation Data Collection and Management. *Transportation Research Record: Journal of the Transportation Research Board*, **2**, 1-16. https://doi.org/10.3141/2414-01

## Appendix A

**Survey Questionnaire for Security Incidents Management**

The open university of Tanzania

Faculty of science, technology and environmental studies

The aim of this questionnaire is to find out your feelings, perception and options on the security incidents.

*Note*: *All information, including answers to various questions in this questionnaire, shall be treated as confidential and solely for academic purposes only. Respondents should feel free to express themselves openly. Please do not reveal your name in this questionnaire*.

**Part One: Personal Information**

For the following statements please tick (✓) the box that matches your view most closely.

(For Organization Name, Other and occupation fill in accordingly).

| | | | |
|---|---|---|---|
| 1 | Organization Name | | |
| 2 | Gender | Male ☐ | Female ☐ |
| 3 | Age | Below 25 Years ☐ | 25 - 35 Years ☐ 36 - 45 Years ☐ 46 - 55 Years ☐ Above 55 Years ☐ |
| 4 | Level of Education | Postgraduate ☐ | First Degree ☐ Advanced Diploma ☐ Ordinary Diploma ☐ Other |
| 5 | Occupation/Profession | | |

**Part Two: Security incidents management**

For the following statements, please indicate your response by ticking (✓) one checkbox per question: rating scale of 0 - 5: minimum 0 and maximum 5.

0-Not performed (non-existent);

1-Performed informally (unplanned);

2-Partially implemented (planned);

3-Implementation is in progress (planned and tracked);

4-Fully implemented (well defined and auditable);

5-Fully implemented and regularly updated (monitored and audited for compliance).

| S/N | Questions | SSE-CMM rating scale | | | | | |
|---|---|---|---|---|---|---|---|
| i | Are incident-handling procedures in place to report and respond to security events throughout the incident lifecycle, including the definition of roles and responsibilities? | 0 ☐ | 1 ☐ | 2 ☐ | 3 ☐ | 4 ☐ | 5 ☐ |
| ii | Does your organization has an incident response team in place and is functional? | 0 ☐ | 1 ☐ | 2 ☐ | 3 ☐ | 4 ☐ | 5 ☐ |
| iii | Does the organization incident response team aware of legal or compliance requirements surrounding evidence collection? | 0 ☐ | 1 ☐ | 2 ☐ | 3 ☐ | 4 ☐ | 5 ☐ |
| iv | I know where to report information security incidents (e.g. viruses, fire, flood, etc.) | 0 ☐ | 1 ☐ | 2 ☐ | 3 ☐ | 4 ☐ | 5 ☐ |

Comments and Suggestions (if any)

Thank you very much for your responses