SRI LANKA CERT|CC

Public Officials' Information and Cyber Security Readiness Across the Country

2021

Public Officials' Information and Cybersecurity Readiness Across the Country

Multi Tech Solutions (Pvt) Ltd.

CONTENT

List of Tables

List of Figures

Appendixes

ABBREVIATIONS

SLCERT	-	Sri Lanka Computer Emergency Readiness Team
ICTA	-	Information and Communication Technology Agency
KSA	-	Knowledge, Skills, Attitudes
IT	-	Information Technology
ICT	-	Information and Communication Technology
UNODC	-	United Nations Office of Drugs and Crime
BCS	-	British Computer Society
MDIIT	-	Ministry of Digital Infrastructure and Information Technology
SMEs/SMBs	-	Small-to-Medium Sized Enterprises and Businesses
US	-	United States
ICMA	-	International City/ County Management Association
UMBC	-	University of Maryland, Baltimore County
ITU	-	International Telecommunication Union
AI	-	artificial intelligence
IoT	-	Internet of Things
ENISA	-	European Network and Information Security Agency
CIA	-	Confidentiality, Integrity and Availability
GCI	-	Global Cybersecurity Index
FGD	-	Focus Group Discussion
CIO	-	Chief Information Officer
ISO	-	Information Security Officer
PPS	-	Probability Proportional to Size
PC	-	Personal Computer
NVQ	-	National Vocational Qualification
HND	-	Higher National Diploma
GIT	-	General Information Technology
IPS	-	Intrusion Prevention Systems
IDS	-	Intrusion Detection Systems
DS	-	Divisional Secretariat
VPN	-	Virtual Private Network
VLANs	-	Virtual Local Area Network
SSL	-	Secure Sockets Layer
DR	-	Disaster Recovery
ERP	-	Enterprise Resource Planning

ACKNOWLEDGMENT

We wish to acknowledge the cooperation and assistance extended by the following officials of the Sri Lanka Computer Emergency Readiness Team (SLCERT) for the completion of this assignment on Public Official Information and Cybersecurity Readiness across the country. This assignment would not have been possible without their unstinted cooperation.

1) Mr. Jayasiri Amarasena – Chief Executive Officer
2) Dr. Kanishka Karunasena – Head of Research, Policy & Projects
3) Mr. Asanka Suraweera – Programme Manager
4) Ms. Shammi Hewamadduma – Information Security Engineer

We also wish to extend our appreciations to the ICTA office Staff who made a valuable contribution for the completion of this assignment.

Team of Consultants

1) Dr. Lochandaka Ranathunga - Team Leader
2) Mr. Athula Rajapakse - Statistician
3) Mr. Athula R. Samarasinghe - Cyber Security Expert
4) Dr. J. A. D. Janaka Jayalath - Policy Development Specialist
5) Mr. Pranama Munasinghe - Project Manager
6) Mr. Bhadraja Mullegamgoda - Research Analyst

Multi Tech Solutions (Pvt) Ltd.

Executive Summary

Over the past decade, many initiatives have been taken to increase the efficiency of the public sector in Sri Lanka. Many ICT based applications were introduced as an immediate output of these programmes. Similarly, the magnitude of cyber-attacks has increased which is making a significant impact to day-to-day operations of the organizations. Lack of attention is paid to the human aspects which is commonly understood as the weakest aspect of cyber security. Many organizations underestimate the human factor in information and Cybersecurity despite the fact that people's understanding, knowledge, and perceptions on information and Cybersecurity are critical for protecting digital systems in organizations. Under this context, Sri Lanka CERT, in association with MDIIT was keen to assess the public officials' information and Cybersecurity readiness in the country. A comprehensive national survey was conducted to achieve this objective of SLCERT, and outputs of this study will be used to develop a national strategy to uplift public officers' Information and Cybersecurity readiness.

Cybersecurity awareness survey was designed based on a broad conceptual framework Considering information security as a key term. There are three widely accepted elements referred to as the "CIA Triad". The key elements are Confidentiality, Integrity and Availability (Recoverability) of information. It also addresses both Physical Security and Virtual Security. Based on this, two structured questionnaires were designed targeting public officials and ICT officers of public organizations.

The sampling framework consists of four stratums covering all public sector organizations. The study has covered a sample of 3540 officers of agencies and institutions grouped under four strata; a) National Ministries b) Provincial Councils, c) District Secretariats d) Institutions not coming under a specific Ministry. The officials were categorized under Primary, Secondary, Tertiary and Senior level. In these organizations, in these organizations, 178 ICT officers were identified and interviewed. An enumerator training was conducted prior to the data collection and enumerators were trained to reduce the non-sampling errors and to adopt the necessary tools to increase the accuracy of the data. In the process of data validation, 276 points were considered as missing data. Accordingly, the data analysis was conducted in considering 3264 data points.

This island wide survey reveals some generic findings which could be a valuable source to any type of Government organization, policy makers, and individuals in their respective scope of work. According to the survey results, it signifies that the majority of employees have obtained some type of ICT based education and a very limited number of employees have acquired Cybersecurity related education or training. Although, both have not influenced in their Cybersecurity knowledge, skills, attitudes (KSA) competencies. This KSA competency analysis was conducted on considering key variables influencing Cyber security, including internet usage and online activities, device usage, confidentiality awareness (E.g., password practices, information communication and security, social interaction, communication network access, data availability, and storing documents), behaviors (E.g., using devices, engaging online activities, and information sharing), protection, and policy awareness. ICT related policy level awareness was at a very poor level while the majority of organizations has not implemented these types of policies (E.g., Information security, social media, data security etc.). Mainly, primary and secondary category employees were enrolled in using ICT in their organizations (E.g., sending/receiving Emails, documentation, data operations etc.) and they do not have an

assured awareness on Cyber security, specifically primary category employees (E.g., office assistants). The findings from ICT officers' assessment emphasized, very few officials were handling ICT related technical work with properly defined job-scope by the Government. Majority of them were other officers who had somewhat ICT knowledge or skills. Lesser number of CIOs were available, and the majority comprised an average level of KSA compared to other ICT officers. Among ICT officers, very few of them had a basic security knowledge. This is also true for other Cybersecurity related functions including asset classification, ICT policies and procedures, storage and media policy, physical access control, network and application security, disaster recovery, and incident management.

This imposes a higher risk on public organizations. It also discovered that, having this type of freedom and lower KSA competencies, there is a grave danger of going towards E-Government or digitalization. Consequently, these findings show the way towards the requirement on developing a properly planned upliftment of KSA competencies regarding Cybersecurity through various types of initiative considering public officials, technology, process and procedures, and policies.

CHAPTER ONE
INTRODUCTION

1.1. Background

Today's society is driven by data and technology. Public and private sector decision makers in the world mostly rely heavily on data in their decision-making processes. The governments use demographic data, economic statistics in policy making and planning strategies for launching development programmes. Good data is an asset to a country, privacy and security are essential in this context. However major challenges need to be addressed carefully to protect the social equilibrium and one major issue in this respect is the emergence of cybercrime. By sensing the severity of cybercrime, United Nations Office of Drugs and Crime (UNODC) has promoted long-term and sustainable capacity building activities in line with anti-cybercrime by encouraging National structures and operations. In particular, UNODC builds on its expertise in responding to law enforcement systems and provides technical assistance in capacity building, prevention and awareness-raising, international cooperation, and data collection, investigation and analysis of cybercrime (UNODC, 2019). Here, the importance of capacity building is facing the potential challenges of the Cybersecurity has been stressed. These, events and actions imply the gravity of the readiness needed to be done by each nation to face the global Cybersecurity challenges.

When focusing towards the National strategy on uplifting public officers' awareness, there is a need for front-end analysis by considering the desirable state of Cybersecurity awareness among the government officials. Further, the education, official status and duties done by the officers are also diversified into various categories. Therefore, the theoretical framework of the study has been formulated by considering the international programs on Cybersecurity including British Computer Society programs and Cybersecurity Modules developed on Doha Declarations by the UNODC (UNODC-E4J, 2019) (BCS, 2019). In the input category of the employees are categories based on both the National Qualifications and Occupational level. Hence, tools were designed to capture necessary variables with respective to Cybersecurity awareness in line with universally accepted knowledge clusters.

In the year 2015, Sri Lanka CERT has conducted a survey on public awareness of Cybersecurity (CERT, Sri Lanka CERT Cybersecurity Awareness Survey, 2015, 2015). This study was conducted using 347 samples. Among the samples there were several victims of Cybercrime. This indicates the spread of Cybercrime to Sri Lanka. In 2017, there was a survey conducted among youth of the country mainly targeting the awareness of social media security aspects. In 2018, CERT has published a handbook as a guide in view of increasing awareness among the general public. (CERT, Handbook on Information Security, 2018). No comprehensive survey has been conducted so far in Sri Lanka on public officers' awareness on information and Cybersecurity although there is ample evidence to show the lack of knowledge and resources. This study has been initiated by Sri Lanka CERT, in association with MDIIT aiming to assess the awareness of public sector employees on Information and Cybersecurity readiness to work in a digital government environment. The findings of the survey are expected be used to develop a strategy to enhance overall readiness on Information and Cybersecurity of government enterprises.

CHAPTER TWO
LITERATURE REVIEW

The increase in cybercrime has hit all cross-sections of business, but one cohort that is exponentially stressed is Small-to-Medium Sized Enterprises and Businesses (SMEs/SMBs) disregarding its nature whether government or private. Cybercrime is an analogue form of transnational crime taken place with the assistance of computing elements or online media. The complexity of crime in the boundary less cyberspace environment is compounded by the increasing involvement of organized crime groups. Cybercrime offenders and their victims can be located in different regions and their impact can affect societies around the world, highlighting the need to organize an urgent, dynamic, national and international response (Nurse, 2019).

According to the Fraud watch International, 95% of Cybersecurity breaches are due to human faults, further, about 54% of companies claim that they have experienced Cybersecurity breaches within one-year period. Social engineering has been mastered by cyber criminals and as a result the psychological manipulation of victims to convince them to tactfully surrender private data that is then use for attacking purposes (International, 2018). One prominent approach is phishing, where phony emails or links are spread to employees who then have their login credentials mined. It can be seen that, many of cyber-attacks are a result of lack in awareness of Cybersecurity where training is essential.

When considering the global trend in line with the Cybersecurity measures, by the United Nations General assembly, in its resolution 65/230, requested the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and their Development in a Changing World, an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of Cybercrime and responses to it by Member States, the International Community and the private sector, including the exchange of information on National legislation, best practices, technical assistance, and international cooperation, with a view to examining options to strengthen existing and to propose new national and International legal or other responses to cybercrime.

According to the Cybersecurity Assessment Netherlands 2019 Report, nearly one third of the hackers are unaware that these committed acts were criminal offences (Counterterrorism, 2019). Information systems of many government institutions have limited security and might be easily hacked (Bruijn & Janssen, 2017). Therefore, Cybersecurity is vital for officers in public organizations at most as a country as concerns. These targets may be in the top list and the damages could be enormous. Critical processes of national importance are almost entirely dependent on government infrastructure, and therefore failure of these services can potentially have a major impact on society. The interdependencies within critical national infrastructure mean that any disruption to a single critical process can result in chain reactions or cascade effects that impact other critical processes (Counterterrorism, 2019).

In general, cybercrime can be described as cyber-related crime, authorized cybercrime, and, as a certain type of crime, exploitation including child sexual abuse on the Internet (UNODC, 2019).

When preparing for the Cybersecurity program for the United States (US) local government authorities, a survey has conducted to look into insights of the Cybersecurity issues faced by US local governments (ICMA) & University of Maryland, 2016). Through this study, they have understood the ground situation of United State local government Cybersecurity practices, and the study was executed by International City/ County Management Association (ICMA) with the partnership of the University of Maryland, Baltimore County (UMBC). This survey explored the key topic areas include which departments are responsible for cybersecurity; awareness of and support for cybersecurity; what barriers local governments face to achieve higher levels of cybersecurity; and what Cybersecurity practices and tools local governments are using. These survey findings have paved them a path to set up strategies and operational plans for uplifting the Cybersecurity status of the local governments.

When looking towards developing country aspects, Nepal has conducted a national Cybersecurity awareness assessment to establish a national Cybersecurity awareness program (Kumar & Sharma, 2015). In this scenario also, with the assistance of ITU, they have conducted multiple studies to obtain the facts of Cybersecurity awareness and the status of the country to plan the Cybersecurity awareness program which targeted both businesses and government to understand the current threats and gain tips and best practices in order to identify, manage and mitigate cyber threats from a user and organizational perspective and at the same time to enhance the Cybersecurity sovereignty of the country.

Similar nature of Cybersecurity awareness assessment has been done in Turkey with the participation of 71 government employees, which aimed to measure government employees' awareness of Cybersecurity and cyberspace elements (Kuru & Ocak, 2016). This study emphasizes the importance of constituting collective Cybersecurity plans and clearly defined responsibilities. Based on their country's perspective, the coverage of Cybersecurity aspects in this study has addressed cyberwarfare and cyberterrorism as well. They have also strived to improve the awareness of employees on critical aspects of cybersecurity.

However, the issues are worsened by the changing cyber threat landscape: the faces of cybercrimes are advancing with new technologies such as artificial intelligence (AI), data science, human behavior and are constantly presented with new attack faces, due to the growth and grip of the Internet of Things (IoT). To limit employee threats, organizations need to emphasize employee awareness of Cybersecurity. There is a trend in targeting Cybersecurity attacks on high- profile and/or revenue-earning organizations. This can be seen by analyzing the recent attacks (Nurse, 2019). To achieve successful awareness of Cybersecurity risk, management of organizations must stress the critical nature of Cybersecurity and implement policies to enforce their positions, rather than dismiss its validity as a threat (Grayson Kemper, 2019).

On 27th of June 2019, the European Cybersecurity Act entered into force, setting the new mandate of ENISA (European Network and Information Security Agency), the EU Agency for Cybersecurity, and established the European Cybersecurity certification framework (ENISA, 2019). In this legal enactment, while providing security enforcement directions, it also empowers its European Cybersecurity certification framework for the governance and rules for EU-wide certification of ICT products, processes and services. Certification plays a critical role in increasing trust and security in products and services that are crucial

for the Digital Single Market. At the moment, a number of different security certification schemes for ICT products exist in the EU. But, without a common framework for EU-wide valid Cybersecurity certificates, there is an increasing risk of fragmentation and barriers in the European Single Market. Under the purview of ENISA, there are two key tasks. The first being knowledge and information: to provide analyses and advice and to raise awareness, to become the one-stop shop (InfoHub) for Cybersecurity information from the EU Institutions and bodies; next is on Capacity building: to reinforce support to EU Member States in order to improve capabilities and expertise, for instance on the prevention of and response to incidents (ENISA, 2019).

These activities and the operation within different context and prominent bodies emphasize the relationship among awareness of Knowledge, Skills, Attitudes (KSA) in tandem with vulnerabilities, victimizations and threats of Cybercrimes prevalent in society. Therefore, the enhancement of awareness becomes critical for any Nation vying for Cybersecurity readiness status. A Conceptual Framework has been established to elicit the Cybersecurity awareness among government employees and then to formulate a strategic plan for improvement of sectoral employee readiness to the desired levels. This has been done in line with the logical framework and approach proposed in the inception report.

CHAPTER THREE
CYBERSECURITY AWARENESS SURVEY

3.1. Objectives of the Survey

The objectives of this survey are to (a) conduct a national survey to assess the public officers' readiness on information and cybersecurity, and (b) develop a national strategy to enhance the public officers' overall readiness on information and cybersecurity.

The phases of the survey include;

Phase One: To access the information and Cybersecurity readiness of public officers.
Phase Two: To develop a national strategy to uplift public officers' Information and Cybersecurity readiness.

3.2. Designing Data Collection Tools

According to the glossary of United States National Initiative for Cybersecurity Careers and Studies, Cybersecurity is extensively defined as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation". The definition is further elaborated as "Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (Studies, 2018). These definitions highlight vital aspects that need to be considered in the context of cybersecurity.

Public officer's survey is a foundation metric used to evaluate the awareness of employees, staff and other members of government institutions. To evaluate the current readiness, it is vital to elicit awareness on necessary key elements and their coverage of Cybersecurity in accordance with respective officers' perspectives.

Considering information security as a key term, there are three widely accepted elements referred to as the "CIA Triad". The key elements are Confidentiality, Integrity and Availability (Recoverability) of information. It also addresses both Physical Security and virtual Security. Security awareness surveys have been conducted by many organizations as well as many professional organizations such as ITU, SANS, ISACA, and ISC. Vulnerability of the "human element" is still considered as the weakest link in security (Kamal Dahbur, 2017).

Under the common CIA pillars, in general, officers according to their respective roles and responsibilities must be knowledgeable on the following:

- ***People*:** Public officers must be educated and trained to enhance their knowledge, skills, and attitude with regard to security.
- ***Technology*:** Technology in both software and hardware must be up-to-date, in addition it should be secure and user-friendly. Public officers must be trained on technology based on their respective job roles and responsibilities.

Technology should also be selected and configured properly to facilitate the implementation of functionality without compromising security.

- ***Processes and Procedures*:** Processes must be designed and implemented to regulate the use of technology by public officers based on their respective job roles and responsibilities. Procedures must be defined and implemented as per the guidelines of best-practices to promote effectiveness of processes.
- ***Policies*:** Policies must be clearly defined, using high-level statements that all public officers can understand, to achieve the security objectives of the institution. Management must also be committed to the enforcement of the policies to ensure organizational compliance and their effectiveness.

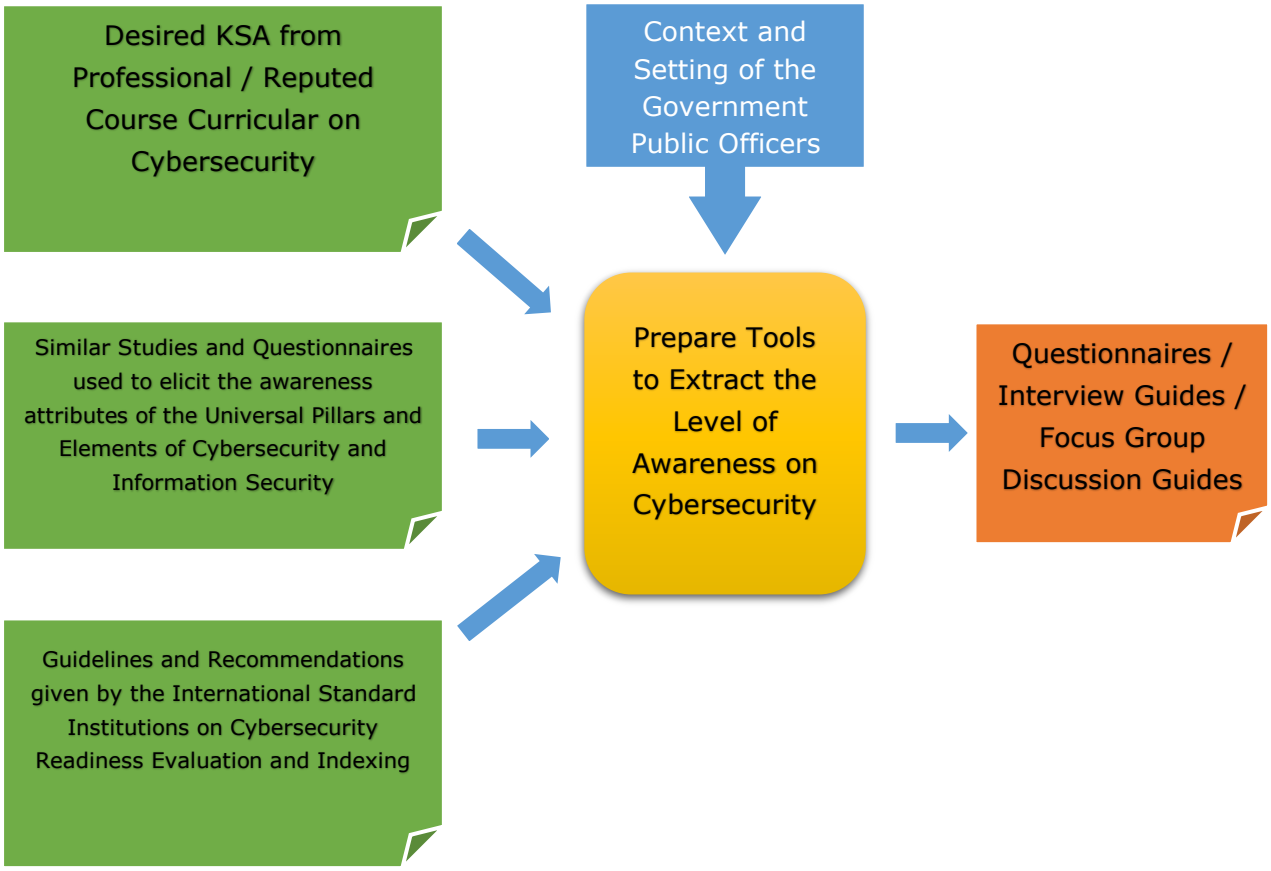
Above four elements are in par with the five indices used by ITU/BDT Cybersecurity Programme for Global Cybersecurity Index (GCI) Reference Model and their Global Cybersecurity Index 2018 Questionnaire Guide (ITU/BDT Cybersecurity Programme, 2018) (Union, 2018). It is vital to consider the relationship of government officers' awareness related to 5 aspects, namely Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation which are used for Global Cybersecurity Indexing purposes; however, all 25 sub-indices are not directly related to individual public officers' awareness levels in executing their respective job roles.

Further to the necessary Cybersecurity elements, in deriving the awareness level under each component, the desired attributes were examined and extracted by investigating several standard professional courses and guides provided by reputed institutes such as BCS, ITU and UNODC (BCS, 2019) (UNODC-E4J, 2019) (Union, 2018).

The conceptual model of deriving the questionnaires for the four public officer groups, interview discussion questions identification, and focus group session guides were derived through the flow of the following conceptual model.

3.3. Conceptual Model for the Preparation of Data Gathering Tools

Figure 3.1: Conceptual Model for the Preparation of Data Gathering Tools



According to the derived conceptual model for the preparation of data gathering tools as in the above figure, there are four main established study areas that have an influential contribution towards the preparation of tools to extract the level of awareness on Cybersecurity from the government employees.

When considering the "Desired KSA from Professional / Reputed Course Curricular on Cybersecurity", there are various standard institutions, professional bodies such as BCS, ITU and UNODC (BCS, 2019) (UNODC-E4J, 2019) (Union, 2018) and Universities have developed various curricular for the Information Security and Cybersecurity. Those materials are reflecting the necessary learning outcomes to derive the expected key Knowledge, Skills as Attitudes to be aware by the different levels of employees in the institutions. Therefore, a careful consideration and extraction of only the necessary learning outcomes which are important for the different levels of roles have been done by studying through the content.

When considering the "Similar Studies and Questionnaires used to elicit the awareness attributes of the Universal Pillars and Elements of Cybersecurity and Information Security", it has been seen that there are various studies conducted by international institutions, academia and organizations to obtain the Information security and Cybersecurity awareness among target groups based on various aims. Out of which, there are studies conducted in line with the core objectives of this study. The tools, approaches and the thoughts elicited from those studies have given foundation for the preparation of questionnaires for our study context. Some of the prominent studies are highlighted in the background.

When looking in to "Guidelines and Recommendations given by the International Standard Institutions on Cybersecurity Readiness Evaluation and Indexing", it has been seen that international standard institutions and governing bodies are highly involved and monitoring the status score of each and every state with respective to the (ITU/BDT Cybersecurity Programme, 2018) (Union, 2018) information and Cybersecurity readiness within states. Therefore, it is highly important to give due respect to the relevant attributes which are focussed by these institutions when considering the scope of the state employees' awareness on Information and Cybersecurity. Therefore, when devising the tools for four categories of target government employees, as key responsible citizens of the country, the key awareness attributes which contribute towards the international indices were also taken into account.

When considering the "Context and Setting of the Government Public Officers", it is highly important to know about interviewees current position, work environment, qualifications with respect to the national and international qualification frameworks. Further, the government employees are holding various responsibilities and information where their gravity could be varying according to the duties they perform. Therefore, there is a need of extracting the interviewees personal status, responsibilities and education level for future analysis when considering the need assessments for placing the necessary strategies to uplift the Cybersecurity awareness level. Further, this study scope felt the necessity of extracting the working environmental factors and behaviors which are reflecting the Cybersecurity awareness of the interviewees and the institution. It was also found that the importance of the technological equipped level of the employees need to be evaluated to derive the correlation among key necessary awareness factors and their nature of duties and behaviors.

Based on the contributions from above influential areas the tools were developed to extract and evaluate the awareness of the Information and Cybersecurity readiness of the government employees. Therefore, Questionnaires (Two main categories), Interview Guides and Focus Group Discussion Guides were developed to elicit information related to the assessment of awareness of information and Cybersecurity.

3.4. Sampling Framework

It is composed of three stages and the final stage derives the number of officials to be surveyed. Multi Stage Stratified Random Sampling technique was used in this assignment to cover all the sectors of public organizations including all categories of public officials as the assignment is based on evaluating Cybersecurity readiness of all the public officials in the country.

3.4.1. Stage 1

In this stage category of employer considered as the stratification factor and therefore, all public sector officials will be categorized into four strata as listed below;

- National Ministries and Institutions grouped under Ministries
- Provincial Councils and Institutions grouped under Provincial Councils
- District Secretariats and Institutions grouped under District Secretariats
- Institutions not grouped under a Ministry

Each stratum designed with a specific theoretical framework and the final strategic plan will also be developed for each of those stratums separately.

Table 3.1: Identified Stratums and Definition

Strata	Definition
Line ministries and Institutions grouped under line Ministries (Strata 1-Line Ministries)	Employees who are currently employed in government and Semi Government agencies coming under the Line Ministries
Provincial Councils and Institutions grouped under Provincial Councils (Strata 2-Provincial councils)	Employees who are coming under Provincial Council, Chief Secretariat which includes all independent institutions functioning under Provincial Councils and 5 Provincial Ministries
District Secretariats and Institutions grouped under District Secretariat (Strata 3- District Secretariets)	Employees who are currently employment in District Secretariats and other institutes grouped under District Secretariats. Each District Secretariat comprises of the staff in the District Secretariat, Divisional Secretariats as well as the Vidatha Centres/Divineguma Praja Moola Banks/ Cultural Centres in Divisional Secretary's Divisions

Institutions not grouped under a Ministry (Strata 4 Institutions not coming under a ministry)	Employees of Government agencies and Semi Government agencies that belong to the Central Government but not coming under a Line Ministry. This includes the Presidential Secretariat, Prime Minister's Office, Parliament and independent officers located in the Parliament Complex, The Supreme Court, Court of Appeal, Election Commission, Judicial Service Commission and its Courts, Audit Service Commission, National Police Commission, Human Rights Commission, Finance Commission, National Procurement Commission, Delimitation Commission etc. and other independent institutions

As per the report generated by Department of Census and Statistics on Census of Public and Semi Government Sector Employment – 2016 following data was extracted for each of the Strums identified above.

Table 3.2: No. of Employees for each Stratum

#	Stratum	No of Employees by Sex - 2016		
		Male	Female	Total
1	National Ministries and Institutions grouped under Ministries	416,036	200,128	616,164 (58.80%)
2	Provincial Councils and Institutions grouped under Provincial Councils	145,968	239,090	385,058 (34.87%)
3	District Secretariats and Institutions grouped under District Secretariats	37,056	52,908	89,964 (8.15%)
4	Institutions not grouped under a Ministry	6,768	6,265	13,033 (1.18%)
Total		**605,828**	**498,391**	**1,104,219**

**Census of Public and Semi Government Sector Employment – 2016 (Department of Census and Statistics)*

The sample selection is based on the Random sampling method. The selection of institutes based on a sensitivity basis considering the usage of IT (Information Technology) at their offices. Further, institutes under each stratum and number of institutes island wide are given in the below tables.

Table 3.3: National Ministries and Institutions grouped under line Ministries

Stratum 1: National Ministries and Institutions grouped under line Ministries	
Name of the Institute	**No. of Institutes Island wide**
Cabinet Ministries	31
Non-Cabinet Ministries	6
State Ministries	19
Departments	121
National Schools	353
National Hospitals	48
MOH	346
Central Dispensaries	475
Police Stations	473
Public Post Offices	4,063
Railway Stations	335
Bus Depots	120
Agrarian Centres	560
Wildlife Offices	170
Technical Colleges	30
Colleges of Technology	9

Source: General Information – 2017, Department of Management Service, Ministry of Finance

Note – The Cabinet Ministries, Non-Cabinet Ministries, State Ministries and Departments were considered for the sample together with a randomly selected sample from other institutes based on the sensitivity.

Table 3.4: Provincial Councils and Institutions grouped under Provincial Councils

Stratum 2: Provincial Councils and Institutions grouped under Provincial Councils	
Name of the Institute	**No. of Institutes Island wide**
Provincial Councils	9
Provincial Schools	9,809
Provincial Hospitals	559
Provincial Ayurvedic Hospitals	92

Source: *General Information – 2017, Department of Management Service, Ministry of Finance*

Note – Provincial Councils were considered for the sample with some other institutions added based on the sensitivity.

Table 3.5: District Secretariats & Divisional Secretariat and Institutions grouped under District Secretariats

Stratum 3: District Secretariats & Divisional Secretariat and Institutions grouped under District Secretariats	
Name of the Institute	**No. of Institutes Island wide**
District Secretariats	25
Divisional Secretariats	332
Municipal Councils	23
Urban Councils	41
Pradeshiya Sabhas	271

Source: *General Information – 2017, Department of Management Service, Ministry of Finance*

Note – All the institutes under the stratum 3 were considered for the sample.

Table 3.6: Institutions not grouped under a Ministry

Stratum4: Institutions not grouped under a Ministry
Administrative Appeal Tribunal
Audit Service Commission
Commission to Investigate Allegations of Bribery or Corruption
Department of Auditor General
Finance Commission
National Salaries and Cadre Commission
National Police Commission
Office of the Cabinet of Ministers
Office of the Chief Government Whip of Parliament
Officer of the Parliamentary commissioner for Admin (Ombudsman)
Parliament of Sri Lanka
Presidential Secretariat
Office of the Leader of the House of Parliament

Prime Minister's Office
Office of the Leader of the Opposition of Parliament
Public Service Commission
Election Commission
National Procurement Commission
Judicial Service Commission
The Delimitation Commission

Source: *General Information – 2017, Department of Management Service, Ministry of Finance*

Note: 10 institutes were selected out of the total institutes in stratum 4.

3.4.2. Stage 2

Total Sample Size:

A total number of 7005 public officials are considered as the total sample size of this study to estimate the public officials' information and Cybersecurity readiness in Sri Lanka.

The government institute is considered as a primary sampling unit and 15 randomly selected employees of each selected institute for the secondary sampling units. Further, it is important to find the gap and formulate the strategy for Readiness on Cybersecurity for each category of employees. Therefore, selection of 15 employees in each institute will be further distributed as follows,

Table 3.7: Sample Allocation by Employee Categories

Minimum Qualification	Government Employee Categories	Sampling units will be covered per institute
G.C.E. O/L	Primary Level	2
G.C.E. A/L	Secondary Level	8
Degree	Tertiary Level	3
Degree / Postgraduate	Senior Level	2
Total		**15**

**Categories were defined based on the Government Public Administrative and Management Circular number 3/2016, issued by the Secretary to the Ministry of Public Administration and Management* (Secretary, 2016) (Treasury, 2006)*. These circulars have indicated the four main employee categories which can be seen in government employee system. Further, under Tertiary level it has taken in to the consideration of special category defined by the CERT and the ICTA Sri Lanka which called as CIO/ISO separately* (CERT, Draft Cybersecurity Act 2019, Sri Lanka, 2019) (ICTA, 2019)*. According to the above Table 7, 3 sample units will be covered from the Tertiary Level and out of those 3 at least one*

of them will be CIO/ISO officer or someone who is performing the same task. Therefore, the Government Employee categorization was carried out on above basis.

Table 3.8: Sample Allocation by Strata

Service Level	Ministries & Institutes	Provincial Councils & Institutes	District Secretariat & Institutes	Not under any Ministry	Total
Primary	516	104	294	20	**934**
Secondary	2064	416	1176	80	**3736**
Tertiary	774	156	441	30	**1401**
Senior	516	104	294	20	**934**
Total	**3870**	**780**	**2205**	**150**	**7005**

At this stage each District is considered as the second stratification factor in order to identify Demographic (Gender) and Geographic spread/ coverage.

Total number of 10 institutes were randomly selected out of 20 institutes under stratum Institutions not grouped under a Ministry. Also, Total number of institutes to be covered under each stratum was calculated by using probability proportional to size (PPS) method.

As per the table 4, based on the probability proportional method, stratum 2 which denotes Provincial councils and Institutes grouped under Provincial Councils get highest proportionate other than stratum 3 which is representing District Secretariats and Institutions grouped under District Secretariats. Stratum 2 includes Provincial Councils, Provincial Schools, Provincial Hospitals and Provincial Ayurvedic Hospitals. Based on our study objectives the importance of the institutes comes under this stratum is considerably lower. Therefore, considering above fact the number of Institutes selected for the sample is reduced and at the same time that number is added to the stratum 3. (Table 9)

Table 3.9: Total Sample allocation

#	Stratum	Proposed Sample Size	
		No. of Institute	No. of Employees
1	Line ministries and Institutions grouped under line Ministries	258	3870
2	Provincial Councils and Institutions grouped under Provincial Councils	52	780
3	District Secretariats and Institutions grouped under District Secretariats	147	2205
4	Institutions not grouped under a Ministry	10	150
Total		**467**	**7005**

Due to the COVID-19 pandemic situation, the study could not be carried out as planned during the planning stage. Due to the lockdowns and poor response from government officials, the survey had to be postponed many times. Most government employees work taking turns due to this situation and it was difficult to conduct survey as expected. Therefore, in accordance with the agreement, we decided to conclude the survey when 50% of the sample was completed. However, we have assessed the impact of the reduction in the sample size in our survey results.

3.4.3. Validation of the new sample size

At the time of proposal development attention was given for accuracy & precision and less consideration was given for cost, time and staff constrains. The behavior /variation of main variables of the study was also not perfectly known at the initial stages of the study. Based on the available information and the stakeholder requirements it was decided to go for a large sample size of 7005 respondents.

According to the situation prevailed due to COVID 19 pandemic it was not possible to carryout field operation as planned. With the great efforts made by all the stakeholders of this project it was possible to complete 3264 sample units of pre decided sampling frame of 7005 sample units.

It was a urgent requirement to study /test whether the available sample size is sufficient to achieve the final objective of the study. The primary analysis it was revealed that 90 percent of government officers did not know or not using Cybersecurity applications in and around their official environments. Whereas main variable of the study is the assessing awareness of Cybersecurity application of the government officials.

Under this situation the following sample size calculation formula was applied to the separate strata to get the total required sample size.

$$\boldsymbol{n = \frac{N z_{\alpha}^{2} PQ}{NE^{2} + Z_{\alpha}^{2} PQ}}$$

The application and its workings are also given below in the Table 3.10.

Table 3.10: The process of sample size calculation by strata

Strata	Notations of the equations	Strata 1-line Ministries	Strata 2 Provincial Councils	Strata 3 District Secretariats	Strata 4 Institutions not grouped under a Ministry
Population Size	N	616164	385058	89964	13033
Expected Knowledge Proportion on Cybersecurity	P	0.1	0.1	0.1	0.1
Unknown Knowledge Proportion on Cybersecurity	Q =(1-P)	0.9	0.9	0.9	0.9
Expected maximum error	E	0.02	0.02	0.02	0.02
Error Squire		0.0004	0.0004	0.0004	0.0004
.05 Sig. level of St. Normal Distribution	Z	1.96	1.96	1.96	1.96
	Z^2	3.8416	3.8416	3.8416	3.8416
N*Z^2*P*Q		213035.006	133131.4932	31104.51322	4506.0816
N*E^2		246.4656	154.0232	35.9856	5.2132
Z^2*P*Q		0.345744	0.345744	0.345744	0.345744
N*E^2+Z^2*P*Q		246.811344	154.368944	36.331344	5.558944
Sample Number	n	863	862	856	811
Total Sample Size		**3392**			

Aa a result of above calculations the total scientific sample size should be the 3392 units whereas the total number completed was 3264. According to the results the sampling error is only 128. (i.e., 3392-3264 = 128)

At the same time, it is to understand that the available stratified sample sizes are large enough to central limit theorem (i.e., n > 30) of the statistics and it is possible to undertake any statistical hypothesis testing if required.

Therefore, it is derived that that the new sample size is scientifically valid to arrive at statistically accepted conclusions.

3.5. Data Collection

Multiple devices and sources were used for collection of qualitative and quantitative data for this survey. Further, background information, secondary data and field data relevant to the awareness of the Cybersecurity were gathered from various sources. These included a comprehensive literature survey, web surfing and a desk study covering published reports of the ICTA, SLCERT and other agencies, national, provincial and district statistical data on Cybersecurity and Information Technology. The Survey Questionnaire prepared to gather quantitative data targeting specific number of Public Officials as described in the sample design. The questionnaires focused on gathering data on; Demographic data, Employment related information, Cybersecurity literacy, Usage of ICT devices and infrastructure, Daily practices.

Thus, there's a tendency that depending on the type of stakeholder (Designation of Public Official) the questionnaire changed. Especially when it comes to cover areas of assessing Cybersecurity Literacy, Usage of ICT Devices and Infrastructure and Daily practices or job tasks performed since tasks performed differ from one position to another. The questionnaires prepared in English pertaining to the number of stakeholder groups categorized and then translated into Sinhala and Tamil. Of the total sample selected for the study one institute from each stratum selected to carry out the Pilot study (Stratum 1: Ministry of Information Technology, Stratum 2: Sri Lanka Sustainable Energy Authority, Stratum 3: Tertiary and Vocational Education Commission, Stratum 4: Finance Commission).

After conducting the Pilot test, the team of consultants finalized all types of data collection tools prepared including both qualitative and quantitative tools. The team coordinate among enumerators and organized enumerator training in Colombo. It was a comprehensive training to improve participation of all enumerators (26). There the enumerators briefed about this assignment and its importance to the country at first. Next the team comprehend enumerators about organizational structure of a public institute and roughly on job roles performed based on positions in its hierarchical order. Thereafter enumerators were trained to use tools to increase the accuracy of data collection as a part of data validation in this survey, whereas some of key considerations has to be made at ground level to increase the precision of the estimates.

The survey conducted based on the field plan designed. Each enumerator is issued a letter of identification that he/ she is conducting the enumeration under this particular assignment from SLCERT in the given time period as proof to produce at times if requested by organizations. The consultants administer the questionnaire, data process, and analyze them and deliver information to meet the objectives of the client. Various measures were taken to reduce the risk to the accuracy of the survey from these limitations.

- Considerable time taken to finalize the two questionnaires and interview guidelines
- Effect of Covid-19.
- Due to COVID-19 lockdowns, Survey is conducting as Telephone survey. But these questionnaires are not specifically designed for a Telephone Survey.
- Because of time constraints of the public officials, some surveys are conducting for groups rather than individuals.

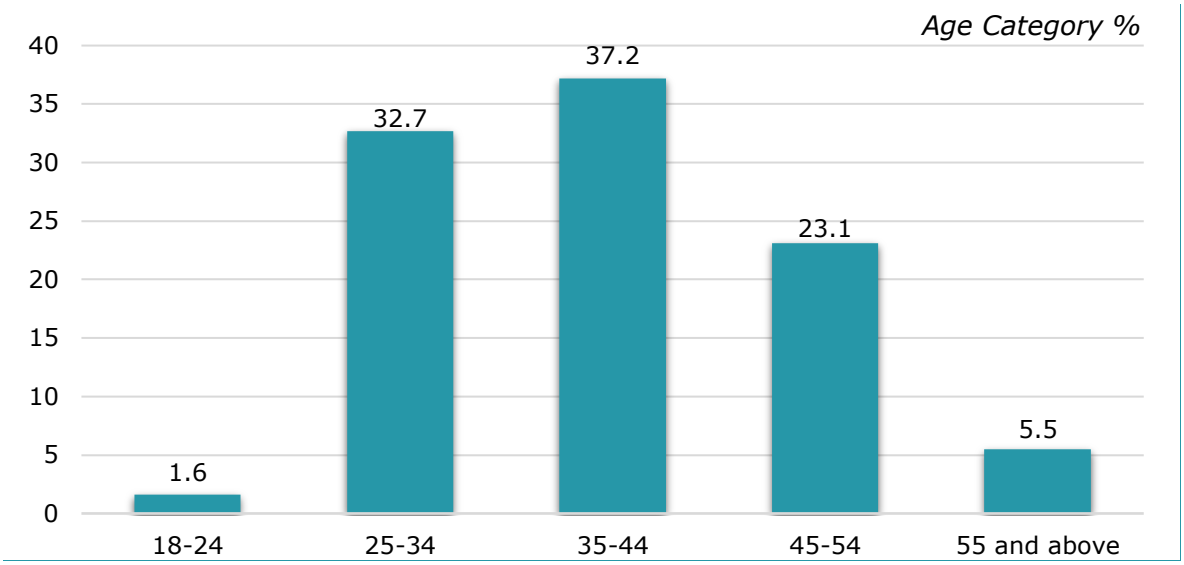
- Some public officials may not be available at time, in turn take more time than expected duration per institute. (E.g., Senior officials may not be available at most of the times)
- Unsatisfactory cooperation from some government officials.
- Lack of responses for some key questions E.g., Type of service
- Since some institutions are working in days basis, employees are not available for scheduled dates.
- The survey has assigned Observations as a validation tool, since the survey is doing over the phone, enumerators can't attend to fill the observation sheet themselves.

CHAPTER FOUR
SURVEY RESULTS

4.1. General Information

The sample distribution based on age category is given in below Figure 4.1.

Figure 4.1: Age Category



According to sample distribution (Figure 4.1), the majority of Government employees (37%) belonged to the 35-44 age category. Smallest proportion was in the 18-24 age category.

Above sample distribution was compared with population distribution (public and semi-Government sector survey, 2016) of Age-category wise, represented in the following table.

Table 4.1: Sample distribution and population distribution

Age	No. of employees in Sample	No. of employees in Population (Total Government employees)
18-24	52 (1.6%)	34,293 (3.1%)
25-34	1,067 (32.7%)	314,034 (28.3%)
35-44	1,214 (37.2%)	337,073 (30.4%)
45-54	753 (23.1%)	309,283 (27.9%)
55 and above	178 (5.5%)	114,792 (10.3%)
Total	**3,264**	**110,9475**

Table 4.1 depicts, there were no significant deviations on all age categories between the sample and population (total employment). Of the employees surveyed, 90% were Sinhalese and 10% were Tamils.

To arrive at better conclusions under number of years of employment, the survey has compared total number of years in the Government service against total number of years under current position in the sample. Based on table 1.2 in Appendix 1, it was revealed that the majority (56%) had a service period of 0-10 years while 26% had a service period of 11-20 years, 15% had a service period of 21-30 years and 2% had a service period exceeding 30 years.

Pearson chi-square tests were conducted for all four category levels, primary, secondary, senior, and tertiary (Appendix 1.1). All the tests conducted indicated high significance. The results showed homogeneity of two variables; Number of years working under current position and the total number of years in Government service.

4.2. Language and Education

In the Government sector, there are 290,378 graduates employed in public and semi government sectors of which 2,014 reported to have more than one basic degree. The majority of graduates (54%) have degrees in Arts discipline, (14.3%) were qualified in Management/ Commerce, and (10.4%) were qualified in science disciplines[1].

Table 4.2: Higher education level

Category	GCE A/L and O/L	Certificate and Diploma	Degree	Degree and above
Primary	271 (67.8%)	60 (15%)	56 (14%)	13 (3.3%)
Senior	16 (3.8%)	21 (5%)	130 (31%)	253 (60.2%)
Tertiary	89 (15%)	39 (6.6%)	260 (43.9%)	204 (34.5%)
Total	**819 (25.1%)**	**405 (12.4%)**	**1,374 (42.0%)**	**666 (20.4%)**

Table 4.2 is an extract from Appendix 2 (Table 2.1). This table shows a majority of (42.0%) is having a degree. Further 20.4 % had a Master's level qualification while 25.1% had only GCE A/L and O/L, and 12.4% had certificate and diploma level qualifications. Consequently, 62% of Government employees are degree holders.

According to English language proficiency and the convenient language in using a PC (Table 2.1 in Appendix 2), 75% of respondents stated that English is the convenient language, while 22% and 2% respectively were in favor of Sinhala and Tamil. Further following findings were made based on the Table 2.1 in Appendix 2.

- In primary category, 5% indicated that their convenient language on using a PC is English. Of that respondent, 4% had a higher level of comfortability on English language, 20% had lower a level comfortability, and 75% had a medium level of comfortability.
- In secondary category, 75% indicated that their convenient language for using a PC is English. Of those respondents, 22% had a higher level of comfortability in English language, 3% had a lower-level comfortability, and 75% had a medium scale comfortability.

[1] Calculations based on the Data of Department of Census and Statistics.

- In senior category, 85% indicated that their convenient language for using a PC is English. Of that respondent, 60% had a higher level of comfortability in English language, 1% had a lower level of comfortability, and 39% had a medium scale comfortability.
- In tertiary category, 82% indicated that their convenient language on using a PC is English. Of those respondents, 43% had a higher level of comfortability in English language, 2% had a lower level of comfortability, and 55% had a medium scale comfortability.

Pearson Chi-square tests were performed for all category levels (Appendix 2.1), while the objectives were to validate the results of convenient language on using a PC and comfortability with the English language. All the tests conducted were highly significant. It showed greater association between convenient language on using a PC and comfortability level of English language (High, Medium, Low). This validates the above results.

Therefore, the tendency of respondents claiming comfortability in use of PCs in English, invariably resulted them having a medium or high standard in English proficiency.

4.3. ICT and Cybersecurity education

In the questionnaire, the ICT knowledge was tested based on ICT related education. Following ICT related programmes were included to observe the ICT knowledge on the respondents.

1) As a Subject in O/L
2) As a subject in A/L
3) GIT in A/L
4) National Vocational Qualification (NVQ)
5) Certificate course in ICT
6) Diploma (Less than one year)
7) Diploma (One year or more)
8) Higher National Diploma
9) ICT professional course (BCS, Java, CCNA, Microsoft. Etc.)
10) As a subject in degree.
11) Degree in ICT
12) Post Graduate Diploma in ICT
13) Master's Degree in ICT
14) Ph.D.

Following represent the stand-alone ICT based qualifications of the respondents. The results are based on Tables from 1-14 in Appendix 3.

1)	As a Subject in O/L	10%
2)	As a subject in A/L	5%
3)	GIT in A/L	12%
4)	National Vocational Qualification (NVQ)	6%
5)	Certificate course in ICT	49%
6)	Diploma (Less than one year)	15%
7)	Diploma (One year or more)	10%

8)	Higher National Diploma	3%
9)	ICT professional course (BCS, Java, CCNA, Microsoft. Etc.)	6%
10)	As a subject in degree.	23%
11)	Degree in ICT	7%
12)	Post Graduate Diploma in ICT	1%
13)	Master's Degree in ICT	2%
14)	Ph.D.	0.001%

Above list of qualifications show that fewer employees have ICT as their core area of expertise. However, 73% of employees have undergone some form of ICT training at O/L, A/L, GIT in A/L, NVQ, Certificate course in ICT, Diploma (less than one year), Diploma (one year or more), HND, ICT professional course, and as a subject in degree level.

Under the National Vocational Qualification segment, 37% had completed NVQ level 1-3, 34% had completed NVQ level 4, 14% had completed NVQ level 5, 6% had completed NVQ level 6, and 7% had completed NVQ level Seven.

In the sample, the following figure represents the Cyber-security knowledge of the employees surveyed.

Figure 4.2: Cybersecurity related knowledge

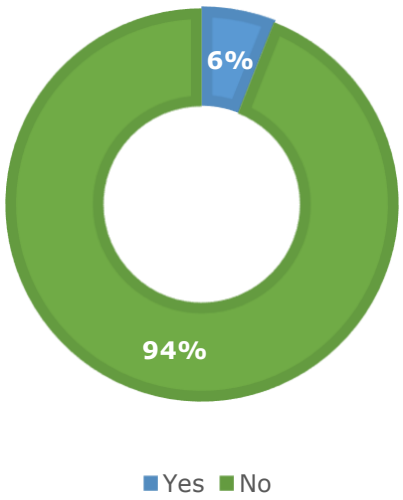


Figure 4.2 indicates that only 6% had Cybersecurity knowledge. They have acquired Cybersecurity knowledge from modules or topics related to Cybersecurity within their programmes of study. Majority of modules/topics studied were as follows:

- Computer network analysis
- Computer security
- Cyber crimes
- Cyber laws
- Cybersecurity in networks
- Ethical hacking
- Information system security

Major themes that were covered on workshops and trainings were indicated as,

- Awareness about modern technology
- Awareness on Cybersecurity
- Cybersecurity and investigations
- Fundamentals in Cybersecurity

4.4. Internet usage and Online activities

Following Table 4.3 represent employees who were having internet access to their computers.

Table 4.3: Internet access to computers

Employee Category	Not having internet access	Having internet access
Primary	172 (43%)	228 (57%)
Secondary	138 (3%)	1714 (97%)
Senior	17 (4%)	403 (96%)
Tertiary	37 (6%)	555 (94%)
Total	364 (11.1%)	2,900 (88.8%)

Table 4.4: Per-day usage of the internet at the office by the Government employees

Category	0-3 Hrs.	4-6 Hrs.	7 and above
Primary	211 (85.7%)	21 (8.5%%)	14 (5.8%)
Secondary	1164 (67.5%)	380 (22.2%)	179 (10.3%)
Senior	252 (62.6%)	109 (27.1%)	41 (10.3%)
Tertiary	355 (63.5%)	151 (27%)	53 (9.5%)
Total	1982 (67.64%)	661 (22.55%)	287 (9.79%)

Of the sample, 88.8% had internet access to their computers. Table 4.4 depicts, 67.6 % of employees were using 0-3 Hrs. of internet at the office, while 22.6% were using 4-6 Hrs., and 9.8% indicated that their usage was above 7Hrs. Although, 10.2% were not having any usage of the internet at their offices.

Table 4.5: Per-day usage of the internet at the home by the Government employees

Category	0-3 Hrs.	4-6 Hrs.	7 and above
Primary	291 (87.6%)	35 (10.5%)	6 (1.9%)
Secondary	1453 (84.0%)	237 (13.7%)	39 (2.3%)
Senior	359 (89.5%)	34 (8.4%)	8 (2.1%)
Tertiary	474 (86.0%)	68 (12.3%)	9 (1.7%)
Total	2,577 (85.5%)	374 (12.41%)	62 (2.05%)

Table 4.5 reveals, 85.5% of employees were using 0-3 Hrs. of internet at the home, while 12.4% were using 4-6 Hrs., and 2.1 % indicated that their usage were above 7Hrs.

Both work and office, total usage per week indicated as,

- In office; 0-15 Hrs. (60.7%), 16-30 Hrs. (20.3%), 31 and above (8.8%),
- At home; 0-15 Hrs. (79%), 16-30 Hrs. (11.5%), and 31 and above (1.9%).

When considering the difference between age categories on total hours of internet usage, it was observed that the null hypothesis was not rejected (Appendix 4.1, 4.2 test statistics), showing there is no significant difference between age groups. For instance, internet usage in between age group 25-34 and age group 55 and above was likely to be

same. This was true for both office usage and home usage. Therefore, internet usage is likely to be same between young, aged group and older aged group.

Following section described the online activities that the employees were engaged. The online activities are divided in to three scales in terms of exposure, namely.

1) Higher scale activities (Critical activities), which exposed to the higher degree of risk.
2) Medium scale activities, which comprised medium scale of risk. This has divided in to two components, I) Generic activities (E.g., online social networks) II). Office-based activities (E.g., uploading documents).
3) Lower scale activities, which comprised least degree of risk.

Table 4.6: Higher scale activities

Category	Online Banking	Buying goods and services	Selling goods and services	Online Banking and Buying goods and services	Online Banking and selling goods and services	Buying and selling goods and services	Engaged in all of activities	Engaged in none of activities
Primary	60 (15%)	34 (8.5%)	1 (0.3%)	56 (14%)	1 (0.3%)	4 (1%)	14 (3.5%)	230 (57.5%)
Secondary	399 (21.5%)	150 (8.1%)	10 (0.5%)	524 (28.3%)	14 (0.8%)	17 (0.9%)	110 (5.9%)	628 (33.9%)
Senior	112 (26.7%)	26 (6.2%)	-	137 (32.6%)	4 (1%)	1 (0.2%)	18 (4.3%)	122 (29%)
Tertiary	159 (26.9%)	44 (7.4%)	6 (1%)	185 (31.3%)	1 (0.2%)	2 (0.3%)	22 (3.7%)	173 (29.2%)
Total	**730 (22.36%)**	**254 (7.78%)**	**17 (0.52%)**	**902 (27.63%)**	**20 (0.61%)**	**24 (0.73%)**	**164 (5.02%)**	**1153 (35.32%)**

Table 4.6, total indicates 35% were not engaged in any higher scale activity showing that 65% were engaged with one or more critical activities, in category wise, 43% primary, 66% secondary, 70% senior, 70% tertiary were engaged in one or more activities. Online Banking and buying goods and services were the most famous activities among Government employees.

Table 4.6.1: Medium scale generic activities

Category	Using Online social networks	Playing games online	Using Online social networks and playing games	No activity
Primary	230 (58.3%)	20 (5%)	50 (12.5%)	97 (24.3%)
Secondary	1164 (62.9%)	41 (2.2%)	254 (13.7%)	393 (21.2%)
Senior	291 (69.3%)	3 (0.7%)	36 (8.6%)	90 (21.4%)
Tertiary	372 (62.8%)	13 (2.2%)	58 (9.8%)	149 (25.2%)
Total	2057 (63.07%)	77 (2.36%)	398 (12.2%)	729 (22.35%)

Table 4.6.1 reveals, generic activities which would have medium scale vulnerability. Of the respondents,78% were engaged (22% not engaged in any activity) in one or more generic activity in terms of online social networks and playing games online.

Table 4.6.2: Medium scale activities – Office based work

Category	Upload and download official documents	Data Entry work	Upload/ Download and Data Entry work	No activity
Primary	142 (35.5%)	10 (2.5%)	24 (6%)	224 (56%)
Secondary	1094 (59.1%)	34 (1.8%)	278 (15%)	446(24.1%)
Senior	277 (66%)	4(1%)	66 (15.7%)	73 (17.4%)
Tertiary	337 (56.9%)	12 (2%)	93 (15.7%)	150 (25.3%)
Total	1850 (56.67%)	60 (1.83%)	461(14.12%)	893 (27.35%)

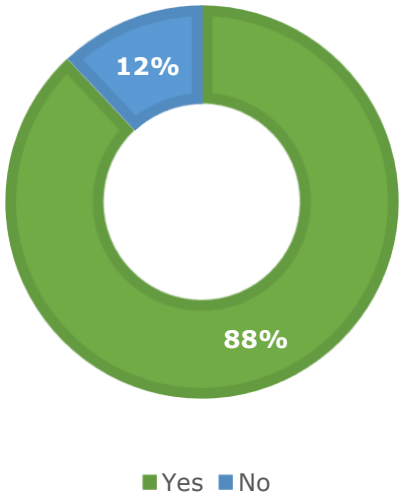
According to table 4.6.2, 73% were engaged in one or more of office based medium scale activities (27% not engaged in any activity) including upload download official documents and data entry work.

Table 4.7: Lower scale activities

Category	Watching TV	Reading News online	Watching TV and reading news	No activity
Primary	34 (8.5%)	102 (25.5%)	61 (15.3%)	203 (50.7%)
Secondary	95 (5.1%)	641 (34.6%)	345 (18.6%)	771 (41.6%)
Senior	12 (2.9%)	154 (36.7%)	86 (20.5%)	168 (40%)
Tertiary	21 (3.5%)	212 (35.8%)	121 (20.4%)	238 (40.2%)
Total	162 (4.96%)	1109 (33.97%)	613 (18.78%)	1380 (42.27%)

Following figure 4.1. represent the people who were using Emails as an online activity.

Figure 4.3: Using Emails

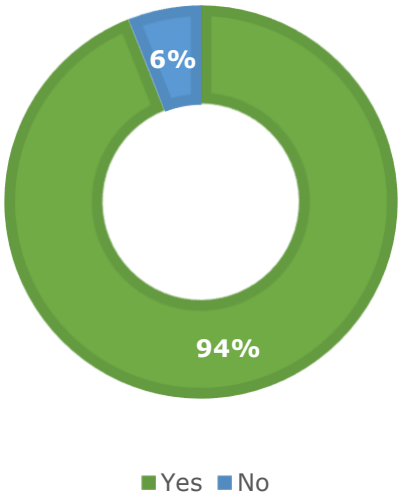


Further, Pearson Chi-square tests was performed to identify the relationship between 1) ICT education and engaged in higher scale online activities and 2) Cybersecurity education and engaged in higher scale online activities (online banking, buying goods and services, selling goods and services). The results (Appendix 4.3) signify, there is a significant relationship between ICT education and conducting critical activities. This suggest that People who have any kind of educational qualification on ICT were conducting critical activities. Also, there is significant relationship between Cybersecurity education and conducting critical activities. People who had any education/training on Cybersecurity also conducting critical activities. In addition, there is no significant difference between age-groups and conducting critical activities. All age groups are engaged in critical activities in the same manner.

4.5. Device Usage

According to computing device usage including mobile phones, tablets, PCs, laptops etc., 94% of respondents were using at least one device in their workplace (Figure 4.4), maybe personal or office property. Category wise, 76% of primary, 96% of secondary, 97% of senior and 95% of tertiary employees were using at least one ICT device.

Figure 4.4: Usage of ICT Devices



The device usage was also tested within Age categories (Appendix 5.1) based on hypothesis test on population proportion. The test statistics shows that there is no significant difference between age groups on device usage. Accordingly, device usage of young employees (18-34) and older category (44 and above) were likely to be the same.

Following tables represent device usage at home and workplace.

Table 4.8: Per day usage at office

Category	0-3 Hrs.	4-6 Hrs.	7 and above
Primary	199 (49.8%)	55 (13.8%)	35 (8.8%)
Secondary	693 (37.4%)	619 (33.4%)	392 (21.2%)
Senior	182 (43.3%)	131 (31.2%)	87 (20.7%)
Tertiary	234 (39.5%)	180 (30.4%)	131 (22.1%)
Total	1308(44.52%)	985 (33.52%)	645 (21.95%)

According to table 4.8, majority (44.5%) were using devices 0 to 3 Hrs. at their work and 33.5% using 4 to 5Hrs and 21.9% using above 7 Hrs.

Table 4.9: Using a Computer at Office

Category	Not having a computer at office	Using a separate Computer	Using a shared Computer	Using a personal Computer
Primary	179 (44.8%)	66 (16.5%)	139 (34.8%)	16 (4%)
Secondary	32 (1.7%)	1357 (73.3%)	394 (21.3%)	69 (3.7%)
Senior	10 (2.4%)	375(89.3%)	18(4.3%)	17(4%)
Tertiary	24(4.1%)	479(80.9%)	62(10.5%)	27(4.6%)
Total	245 (7.5%)	2277 (69.76%)	613 (18.78%)	129 (3.95%)

Table 4.9 depicts, 7.5 % were not using a computer, 69.8 % were using a separate computer, 18.8 % were using a shared computer, and 3.9 % were using their personal computers at their workplaces.

Table 4.10: Comparison of using a computer by officials having some type of ICT Education/training.

Category	Persons who have undergone some type of ICT training			
	Not having a computer at office	Using a separate Computer	Using a shared Computer	Using a personal Computer
Primary	51 (28.5%)	46 (69.7%)	92(66.2%)	9(56.3%)
Secondary	16(50%)	1068(78.7%)	290(73.6%)	52(75.4%)
Senior	4(40%)	262(69.9%)	14(77.8%)	13 (76.5%)
Tertiary	7(29.2%)	384(80.2%)	42(67.7%)	20(74.1%)
Total	78 (3.29%)	1760 (74.26%)	438 (18.48%)	94 (3.96%)

The Table 4.10 reveals among the people who have undergone some type of ICT training 3.3% are not having a computer in the office, 74.3% are using a separate computer, 18.5% using shared computers and 3.96% are using personal computers. This highlight the fact that the majority 74.3% are using separate computers.

4.6. Confidentiality Awareness

4.6.1. Shared Computer practices

Following table represent awareness on separate (private) user logins for people who were using a shared computer. Of the respondents, 23% were using a shared computer. (Appendix 6)

Table 4.11: Sperate (Private) User logins

Category	Not having separate logins	Having separate logins	"Do not know"
Primary	127 (66%)	40 (20%)	25 (13%)
Secondary	521 (61%)	242 (28%)	87 (10%)
Senior	84 (65%)	32 (25%)	14 (10%)
Tertiary	122 (57%)	61 (29%)	30 (14%)
Total	854 (61.6%)	375 (27.07%)	156 (11.26%)

Table 4.11 shows, majority 61.6% were not having a separate (private) user login and 27% were having separate user logins and 11.3% do not know whether they were having separate logins or not. Following Table 4.12 represents the comparison of usage of user logins of officers who are having some type of ICT education & training.

Table 4.12: Comparison of ICT education and separate (private) user logins

Category	Persons who have some type of ICT education /training		
	Not having separate logins	Having separate logins	"Do not know"
Primary	83 (67%)	31(25%)	09 (7%)
Secondary	397 (60%)	199 (30%)	68 (10%)
Senior	59 (61%)	26 (27%)	11 (11%)
Tertiary	23 (14%)	89 (54%)	52 (32%)
Total	562 (53.67%)	345 (32.95%)	140 (13.37%)

Table 4.12 compared employees who had ICT education with the use of separate (private) user logins, 54% respondents were not having separate logins, while 33% are having separate logins, 33% comes under "do not know" category. Following table 4.13 represents practices followed by the employees who had shared computer and users of separate (private) user logins.

Table 4.13: Practices followed by shared computer users and having separate (private) user logins

Category	Persons who have some type of ICT education /training		
	Having a common user for all accounts	Never shared the password	Shared password with Co-workers
Primary	80 (56.7%)	29 (20.5%)	32 (22.8%)
Secondary	241 (41.2%)	209 (35.7%)	135 (23.1%)
Senior	16 (28.5%)	29 (51.8%)	11 (19.7)
Tertiary	44 (33.3%)	58 (44.3%)	30 (22.7%)
Total	381 (41.68%)	325 (35.55%)	208 (22.75%)

Table 4.13 indicates, of the persons who were using shared computers and using separate user logins, 42% were having common users for all accounts, 36% had never shared the password and 23% had shared the password with their Co-workers.

Table 4.14:ICT education and Practices followed by separate (private) login users

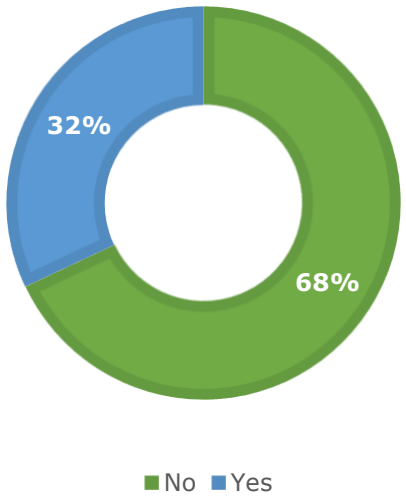
Category	Having a common user account for all users	Never shared my password	Shared password with co-workers
Primary	51 (53%)	23 (34%)	22 (23%)
Secondary	172 (38%)	167(37%)	111 (25%)
Senior	13 (31%)	22 (52%)	7 (17%)
Tertiary	30 (29%)	51 (50%)	22 (21%)
Total	266 (38.49%)	263 (38.06%)	162 (23.4%)

Table 4.14 represents, relationship between ICT education and practices followed by participants. Respondents who were having a common user account was 38% and who have never shared was also 38% and who have shared the password with Co-workers, 23%.

4.6.2. Password practices

Following Figure 4.5 represent usage of passwords across all accounts.

Figure 4.5: Using same Password across user accounts



Along with above figure, 32% were using same password across all accounts. In category wise distribution, 39% primary, 31% secondary, 30% of senior, and 30% of tertiary employees were using password across all accounts. (Appendix 6)

Table 4.15: Frequency of password changes

Category	Annually	Monthly	Never	Quarterly	Randomly
Primary	16(4%)	12(3%)	214(53%)	13(3%)	145(36%)
Secondary	128(7%)	50(3%)	551(30%)	169(9%)	954(52%)
Senior	28(7%)	16(4%)	106(25%)	52(12%)	218(52%)
Tertiary	39(7%)	14(2%)	173(29%)	50(8%)	316(53%)
Total	211 (6.46%)	92 (2.81%)	1044 (31.98%)	284 (8.7%)	1633 (50%)

Table 4.15 shows, 6.5% of respondents were changing annually, 2.8% were changing monthly, 8.7% were changing quarterly, and 50% were changing randomly. Although, 32% were not changing their passwords.

Further few tests based on Pearson Chi-square, Contingency Coefficient, and Phi-coefficient were conducted (Appendix 6.1.) to check the nature of password practices and ICT knowledge. The results are indicated in below.

1. All the tests are highly significant. This implies there is a relationship between ICT knowledge and using password across all accounts.
2. The Phi coefficient is negative. This shows, employees who were having ICT education would use same password across all accounts, signifying that the having ICT education would not necessarily reduce the critical practices of employees.
3. According to contingency coefficient There is no necessary association between column and raw variables, which implies the relationship between ICT knowledge and critical practice (using same password) likely to be random. This reflect the fact that people who were having some knowledge in ICT would not necessarily choosing the non-critical practices.

Practices on keeping/remembering the password is ranked according to 1. Decent, 2. Medium, and 3. Critical kind of practices.

1) Decent practices.
Remembering or keeping password in memorize, considered as a decent practice.

Table 4.16: Good practices in usage of passwords

Category	In Memorize	Not using this practice
Primary	296 (74%)	104 (26%)
Secondary	1562 (84.3%)	290(15.7%)
Senior	346 (82.4%)	74 (17.6%)
Tertiary	495 (83.6%)	97 (16.4%)
Total	2699 (82.68%)	565 (17.31%)

Table 4.16 reveals the fact that, 83% sharing this decent practice. In category wise distribution, 74% of primary, 84% of secondary, 82% of senior, and 84% of tertiary were sharing this practice. (Appendix 6)

2) Medium level practices
Remembering or keeping password, which is written in a secure place is considered as a medium scale practice.

Table 4.17: Medium scale practices in usage of passwords

Category	Written in a secure place	Not using this practice
Primary	83 (20.8%)	317 (79.3%)
Secondary	615 (33.2%)	1237 (66.8%)
Senior	164 (39%)	256 (61%)
Tertiary	190 (32.1%)	402 (67.9%)
Total	1052 (32.23%)	2212 (67.76%)

Table 4.17 shows, only 32% were following the practice of writing the password in a secure place. The category wise distribution is 21% of primary, 33% of secondary, 39% of senior and 32% tertiary and among them the highest is senior level.

3) Critical practices
Under critical practices, written in a common place, telling someone, and autosaved passwords are considered as critical practices of employees.

Table 4.18: Critical practices in usage of passwords

Category	Written in common place	Tell someone	Autosave password	Written in common place and Autosaved	Tell someone and autosaved	Not using these practices
Primary	4 (1%)	3 (0.8%)	21 (5.3%)	-	-	372 (93%)
Secondary	18 (1%)	7 (0.4%)	133 (7.2%)	2 (0.1%)	-	1692 (91.4%)
Senior	-	2 (0.6%)	34 (8.1%)	-	1 (0.2%)	383 (91.2%)
Tertiary	5 (0.8%)	3 (0.5%)	47 (7.9%)	-	-	537 (90.7%)
Total	27 (0.82%)	15 (0.45%)	235 (7.19%)	2 (0.06%)	1 (0.03%)	2984 (91.42%)

Above Table 4.18 shows, that 91% of respondents were not following any of these critical activities indicating that only 9% are having critical practices. Although, one of common use of practices were autosave passwords in today, only 7% were following this practice. Of that respondent, 9% who were having any kind of Cybersecurity education/training were using this practice of auto saving passwords. (Appendix 6)

Following Table 4.19 showcase the practices that the employees were following when creating a password. These practices also scaled as Decent, Medium, and Critical practices.

a) Critical Practices

Creating passwords by using only numbers OR letters, using personal details as passwords, and using common words or patterns are considered as critical activities.

Table 4.19: Critical practices on creating a password

Category	Methods used in creating the password							
	Only numbers or letters	Personal Details	Common words or patterns	Numbers or letters and Personal Details	Numbers or letters and common words or patterns	Personal Details and common words	All practices	Not using any kind of practices
Primary	92 (23%)	137 (34%)	8 (2%)	4 (1%)	3 (1%)	22 (5%)	1 (1%)	133 (33%)
Secondary	245 (13%)	544 (29%)	94 (5%)	25 (1.8%)	4 (0.1%)	86 (5%)	2 (0.1%)	852 (46%)
Senior	33 (8%)	126 (30%)	17 (4%)	5 (1%)	2 (0.5%)	13 (3%)	1 (0.2%)	223 (53%)
Tertiary	81 (14%)	154 (26%)	34 (6%)	10 (2%)	2 (0.3%)	24 (4%)	0 (0%)	287 (48%)
Total	451 (13.81%)	961 (29.44%)	153 (4.68%)	44 (1.34%)	11 (0.33%)	145 (4.44%)	4 (0.12%)	1495 (45.8%)

Table 4.19 reveals, that around 54% were using some type of critical practices mentioned above (46% not using any kind of practices). Further, usage of these practices and its nature of the relationship between ICT education and Cybersecurity education/training was tested separately.

b) Medium scale practices

Creating password by using only numbers AND letters are considered as a medium scale practice.

Table 4.20: Medium scale practices on creating a password

Category	Using Numbers and Letters	Not using this practice
Primary	117 (29.3%)	283 (70.8%)
Secondary	575 (31%)	1277 (69%)
Senior	138 (32.9%)	282 (67.1%)
Tertiary	148 (25%)	444 (75%)
Total	978 (29.96%)	2286 (70.03%)

Table 4.20 shows, that of the medium scale 30% are creating passwords by using numbers and letters and 70% of are not following this practice.

c) Good practices

Creating passwords by using combination of numbers, Uppercase/ Lowercase letters and special characters and creating passwords by using passphrases are considered as good practices.

Table 4.21: Good practices on creating a password

Category	using combination of numbers, uppercase/ lowercase letters and special characters	using passphrases to create password	Using both	Not using both
Primary	117 (29.3%)	9 (2.3%)	2 (0.5%)	272 (68%)
Secondary	952(51.4%)	21(1.1%)	37 (2%)	842 (45.5%)
Senior	256(61%)	4(1%)	10(2.4%)	150(35.7%)
Tertiary	340(57.4%)	2(0.3%)	9(1.5%)	241(40.7%)
Total	1665 (51.01%)	36 (1.1%)	58 (1.77%)	1505 (46.1%)

In Table 4.21, Of the respondents, 46% were not engaged in any kind of good practices on creating passwords. Category wise, 68% of primary, 45% of secondary, 35% of senior, and 40% of tertiary employees were not engaged in any kind of good practices. Further, the tests were performed based on Pearson chi-square, contingency coefficient, and Phi-coefficient (Appendix 6.2). Following observations are made based on these tests.

I. ICT education and engaged in at least one critical activity.

- There is an association between ICT education and engaged in one critical activity.
- There is a negative relationship but closer to zero. This shows higher the ICT knowledge likely to reduce the critical activities marginally.

- However, there is a lower association between row and column variables, means higher ICT knowledge not necessarily involve in not using a critical practice. Therefore, choosing a critical practice is not necessarily associate with the ICT education, people who may have higher ICT education would likely to be engaged in critical activities.

II. Cybersecurity knowledge and engaged in at least one critical activity.

- There is an association between Cybersecurity knowledge and engaged at least one critical activity.
- There is a negative relationship and closer to zero, means higher Cybersecurity knowledge is likely to reduce engaging in critical activities marginally.
- However, there is a lower association between row and column variables, means higher Cybersecurity knowledge not necessarily involve in not using a critical practice. Therefore, choosing a critical practice is not necessarily associate with the Cybersecurity education/training, people who may have higher Cybersecurity training/education would likely to be engaged in critical activities.

Following section represent folder and document password practices of the Government employees. Table 4.22 indicated in below shows the usage of folder passwords.

Table 4.22: Folder passwords usage

Category	Using Folder Passwords	Not using Folder Passwords	Not having a knowledge of how to use a Folder Password
Primary	43(10.8%)	165(41.3%)	192(48.0%)
Secondary	356(19.2%)	1074(58.0%)	422(22.8%)
Senior	75(17.9%)	231(55.0%)	114(27.1%)
Tertiary	106(17.9%)	371(62.7%)	115(19.4%)
Total	580 (17.76%)	1841 (56.4%)	843 (25.82%)

This indicate the fact that 18% of total employees were using folder passwords and 56% were not using folder password while 26% did not have any kind of knowledge on how to input a folder password. In addition, it was tested against the ICT education of the people, and following observations were made.

- In primary category, employees who did not have some knowledge to input a folder password, 30% were having an any ICT-related qualification.
- In secondary category, employees did not have had some knowledge to input a folder password, 58% were having an any ICT-related qualification.
- In senior category, employees who did not have some knowledge to input a folder password, 57% were having an any ICT-related qualification.
- In tertiary category, employees who did not have some knowledge to input a folder password, 57% were having an any ICT-related qualification.

Table 4.23: Document passwords usage

Category	Using Document Passwords	Not using Document Passwords	Not having a knowledge of how to use a Document Password
Primary	36(9.0%)	161(40.3%)	203(50.7%)
Secondary	341(18.4%)	1055(57.0%)	456(24.6%)
Senior	85(20.2%)	219(52.1%)	116(27.6%)
Tertiary	97(21.4%)	287(63.4%)	69(15.2%)
Total	559 (17.88%)	1722 (55.1%)	844 (27%)

This indicate the fact that only 17% employees were using document password and 55% were not using document passwords while 27% did not have some kind of knowledge on how to input a document password. In addition, it was tested against the ICT education of the people, and following observations were made.

- In primary category, employees who did not have some knowledge to input a document password, 32% were having an ICT-related qualification.
- In secondary category, employees who did not have some knowledge to input a document password, 59% were having an ICT-related qualification.
- In senior category, employees who did not have some knowledge to input a document password, 61% were having an ICT-related qualification.
- In tertiary category, employees who did not have some knowledge to input a document password, 57% were having an ICT-related qualification.

Table 4.24: Encrypting Documents

Category	Encrypting documents	Not encrypting documents	Not having a knowledge of how to encrypt a document
Primary	19(4.8%)	142(35.5%)	239(59.8%)
Secondary	150(8.1%)	972(52.5%)	730(39.4%)
Senior	45(10.7%)	215(51.2%)	160(38.1%)
Tertiary	45(7.6%)	333(56.3%)	214(36.1%)
Total	259 (7.93%)	1662 (50.91%)	1343 (41.14%)

Table 4.24 shows, that only 8% of the total were encrypting documents, 51% were not encrypting documents while 41% did not have any kind of knowledge on how to encrypt a document. In addition, it was tested against the ICT education of the people, and following observations were made.

- In primary category, employees who did not have some knowledge to encrypt a document, 37% were having an ICT-related qualification.
- In secondary category, employees who did not have some knowledge to encrypt a document, 66% were having an ICT-related qualification.
- In senior category, employees who did not have some knowledge to encrypt a document, 61% were having an ICT-related qualification.

- In tertiary category, employees who did not have some knowledge to encrypt a document, 63% were having an ICT-related qualification.

Table 4.25: Hiding Documents/Folders.

Category	Hiding documents/ folders	Not Hiding documents/ folders	Not having a knowledge of how to hide a document/ Folder
Primary	49 (12.3%)	151 (37.8%)	200 (50.0%)
Secondary	314 (17.0%)	1096 (59.2%)	442 (23.9%)
Senior	68 (16.2%)	239 (56.9%)	113 (26.9%)
Tertiary	81 (13.7%)	387(65.4%)	124 (20.9%)
Total	512 (15.68%)	1873 (57.38%)	879 (26.93%)

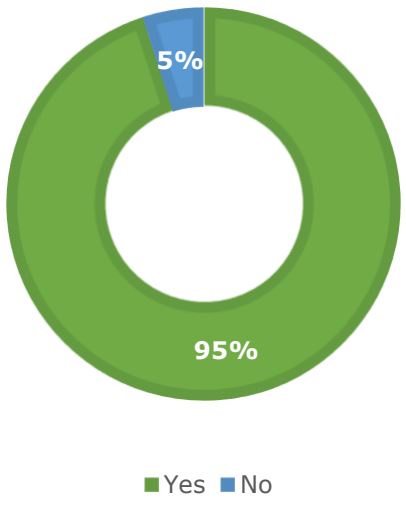
Table 4.25 shows, only 16% of the total were hiding document folders, 57% of total employees were not hiding documents/folders while 27% did not have any kind of knowledge on how to hide a document/folder. In addition, it was tested against the ICT education of the people, and following observations were made.

- In primary category, employees did not have some knowledge to hide a document/folder 31% were having an ICT-related qualification.
- In secondary category, employees who did not have some knowledge to hide a document/folder 57% were having an ICT-related qualification.
- In senior category, employees who did not have some knowledge to hide a document/folder 58% were having an ICT-related qualification.
- In tertiary category, employees who did not have some knowledge to hide a document/folder 55% were having an ICT-related qualification.

4.7. Emails

Figure 6.3.1. indicated in below shows the usage of email addresses.

Figure 4.6: Using Emails

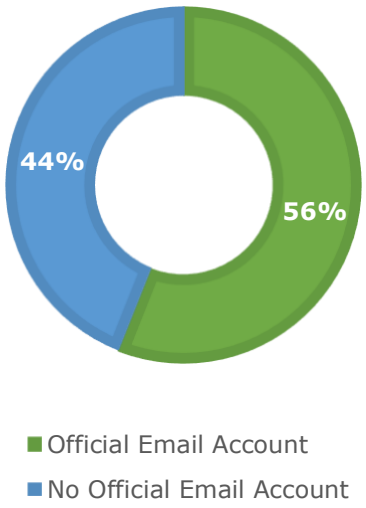


Of the employees, 85% of primary, 97% of secondary, 99% of senior, and 95% of tertiary employees were having an Email address. According to the relationship between ICT education and usage of emails following observations are made based on the findings.

- In primary category, employees having an Email address, 55% consist of least one ICT qualification.
- In secondary category, employees having an Email address, 78% consist of least one ICT qualification.

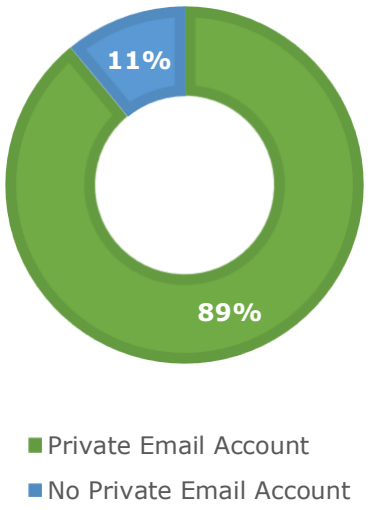
- In senior category, employees having an Email address, 70% consist of least one ICT qualification.
- In tertiary category, employees having an Email address, 80% consist of least one ICT qualification.
  (Refer Appendix 6)

Figure 4.7: Usage of official Emails



Above figure shows, of the respondents, 56% were having an official Email account. In category wise, 17% of primary, 58% of secondary, 79% of senior, and 64% of tertiary employees were having an official Email address. (Appendix 6)

Figure 4.8: Usage of private Emails



Above figure shows, 89% were having a private Email account, in category wise, 74% of primary, 91% of secondary, 95% of senior, and 90% of tertiary employees were having a private Email Account (based on the decomposition of figure 6.3.3)

Table 4.26: Use of Emails for official communication

Category	Using Emails for official communication	Not using Emails for official communication
Primary	105 (26.3%)	295(73.8%)
Secondary	1432(77.3%)	420(22.7%)
Senior	368(87.6%)	52(12.4%)
Tertiary	456(77%)	136(23%)
Total	2361 (72.33%)	903 (27.66%)

Table 4.27: Using private Email for official work

Category	Using private Email for office work	Not using private Email for office work
Primary	100 (25%)	300(75%)
Secondary	888(47.9%)	964(52.1%)
Senior	238(56.7%)	182(43.3%)
Tertiary	327(55.2%)	265(44.8%)
Total	1553 (47.57%)	1711 (52.42%)

Table 4.28: Using a shared email at office

Category	Using a Shared Email at office	Not using a Shared Email at office
Primary	67(16.8%)	333(83.3%)
Secondary	755(40.8%)	1097(59.2%)
Senior	104(24.8%)	316(75.2%)
Tertiary	190(32.1%)	402(67.9%)
Total	1116 (34.19%)	2148 (65.8%)

Table 4.26 shows, 72% were using Emails for official communications. Table 4.27 implicit the characteristics of emails usage within the employees who do not have an official Email account, 48% were using private email for official work and Table 4.28 shows 34% were using shared Email.

Figure 4.9: Merging private and Official Email

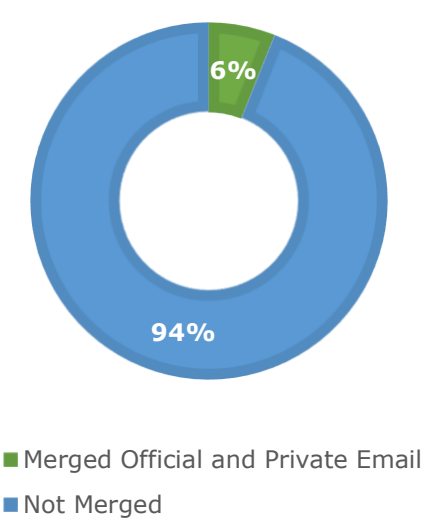


Figure 4.9 implicit, only 6% had merged their emails. In category wise distribution, 2% of primary, 5% of secondary, 8% of senior, and 6% of tertiary employees had merged their Email accounts (based on the decomposition of figure 4.9)

Table 4.29: Using official Email for personal communication

Category	Using official Email for personal communication	Not using official Email for personal communication
Primary	31(7.8%)	369(92.3%)
Secondary	191(10.3%)	1661 (89.7%)
Senior	58(13.8%)	362(86.2%)
Tertiary	69(11.7%)	523(88.3%)
Total	349 (10.69%)	2915 (89.3%)

Above table shows, 10% of respondents using official email for personal communication. Of the employees, 14% stated that their superior/line manager had requested them access his or her Email account. Following table shows the status of sharing Office-Email password with someone else in the office or outside the premises.

Table 4.30: Sharing office Email password

Category	Sharing the password	Not sharing the password
Primary	20(5%)	380(95%)
Secondary	259(14%)	1593(86%)
Senior	39(9.3%)	381(90.7%)
Tertiary	55(9.3%)	537(90.7%)
Total	373 (11.42%)	2891 (88.57%)

Table 4.30 depicts, only 11% had shared official Email password with someone else. Following observations also made on this target group.

- In primary category, people who shared the Email password, 80% of them had any kind of ICT based education.

- In secondary category, people who shared the Email password, 82% of them had any kind of ICT based education.
- In senior category, people who shared the Email password, 64% of them had any kind of ICT based education.
- In tertiary category, people who shared the Email password, 78% of them had any kind of ICT based education.
- Based on calculation from Appendix 6

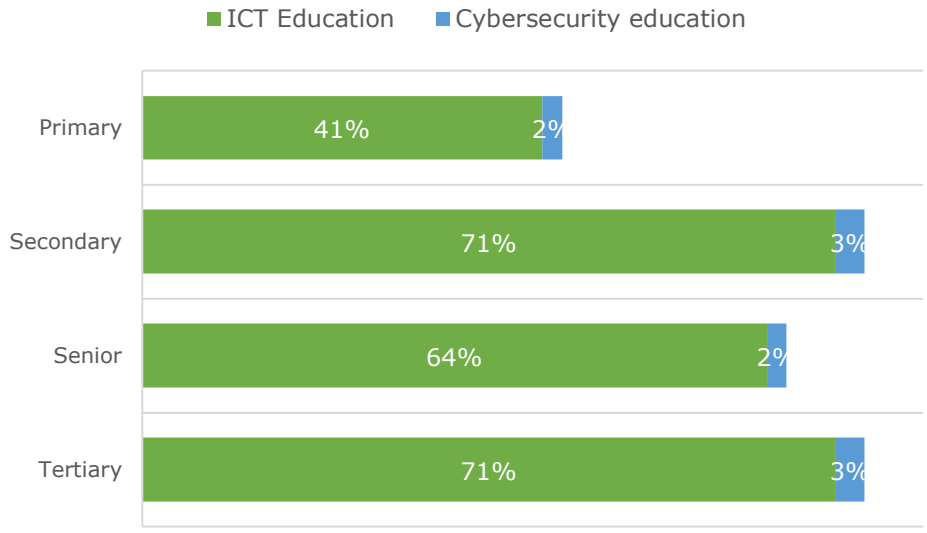
The questionnaire also tested the critical incidents based on hacking of government employees' emails. Following table represents the hacking incidents of their emails.

Table 4.31: Email Hacking incidents

Category	Email account has been hacked	Email account not has been hacked	Do not know whether the email account has been hacked or not
Primary	15(3.8%)	139(34.8%)	246(61.5%)
Secondary	58(3.1%)	1116(60.3%)	678(36.6%)
Senior	26(6.2%)	222(52.9%)	172(41.0%)
Tertiary	24(4.1%)	355(60.0%)	213(36.0%)
Total	123 (3.76%)	1832 (56.12%)	1309 (40.1%)

Table 4.31 reveals, that in 4% email has been hacked and 56% not hacked while 40% of total employees surveyed had no idea on whether their Email account has been hacked or not. In addition, employees who were not aware on their own account hacking incidents, were examined along with their ICT education and Cybersecurity education/training, and following observations were made.

Figure 4.10: Distribution of ICT and Cybersecurity knowledge on people who do not know whether their accounts have been hacked or not



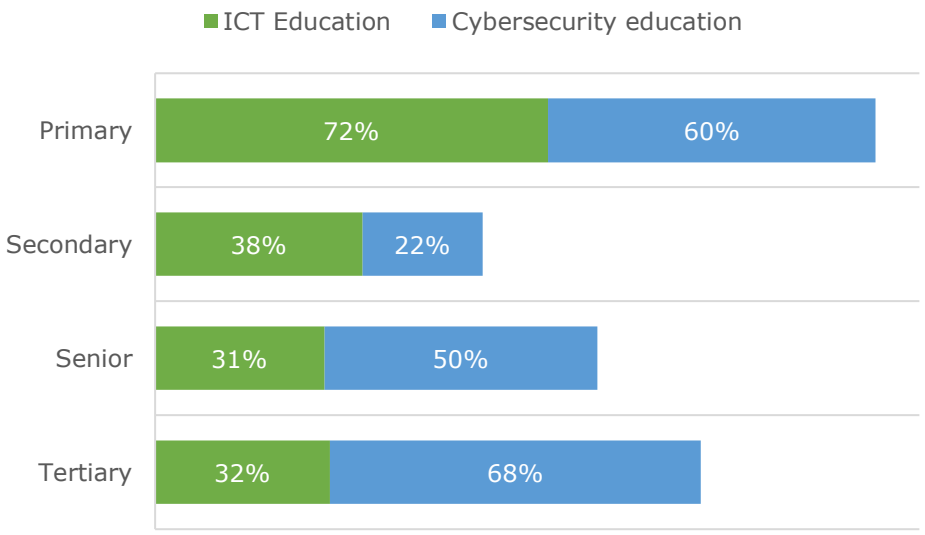
As indicated in the Figure 4.10 in tertiary category, of the employees who do not know their accounts has been hacked or not, 71% were having ICT education and 3% were having Cybersecurity education/training. In senior category, 64% were having ICT education and 2% were having Cybersecurity education/training. In secondary category, 71% were having ICT education and 3% were having Cybersecurity education/training. In primary category, 41% were having ICT education and 2% were having Cybersecurity education/training.

Table 4.32: Spam filtering option in the Email

Category	Having a spam filtering option	Not having a spam filtering option	Do not know
Primary	65(16.3%)	82(20.5%)	253(63.2%)
Secondary	831(44.9%)	351(19.0%)	670(36.2%)
Senior	201(47.9%)	60(14.3%)	159(37.9%)
Tertiary	306(51.7%)	108(18.2%)	178(30.1%)
Total	1403 (42.98%)	601 (18.41%)	1260 (38.6%)

Of the employees, 43% had a spam filtering option, 18% did not have and 39% had a no knowledge regarding spam filtering in the Email. It is vital to form a distribution on the employees who do not have some knowledge on spam filtering option given ICT education and Cybersecurity education/training.

Figure 4.11: Distribution of ICT and Cybersecurity knowledge on employees who do not have a knowledge on spam filtering of their Emails.



Above figure reflects that 72% of the primary employees has ICT education and the second highest category having ICT education with 38% is the secondary level. The IT education in senior and tertiary level is comparatively low. The Cybersecurity education in tertiary level is high with 68% and the second highest is the primary level with 60%. The secondary level is low in both ICT and Cybersecurity education.

4.8. Social Media

This section signifies the social media experience of the surveyed employees.

Following social media platform were considered in this survey.

1) Facebook
2) Instagram
3) WhatsApp
4) Viber
5) You Tube
6) Twitter

Table 4.33: Social Media platforms

Category	Facebook	WhatsApp	Viber	You Tube	Two or More	None
Primary	7 (1.8%)	7(1.8%)	3(0.8%)	5(1.3%)	345(86.3%)	33(8.3%)
Secondary	21 (1.1%)	33(1.8%)	12(0.6%)	11(0.6%)	1728(93.3%)	47(2.5%)
Senior	6(1.4%)	11(2.6%)	-	1(0.2%)	400(95.2%)	2(0.5%)
Tertiary	5(0.8%)	9(1.5%)	1(0.2%)	1(0.2%)	554(93.6%)	22(3.7%)
Total	39 (1.19%)	60 (1.83%)	16 (0.49%)	18 (0.5%)	3027 (92.7%)	104 (3.18%)

Table 4.33 reveals, very few people were using only one platform. E.g., In tertiary category only 0.8% were using Facebook, 1.5% were using WhatsApp only etc. Majority were using two or more platforms. Of the total surveyed employees, 93% were using two or more social media platforms. Also, only 3% were not using any of the social media mentioned in above. Both Twitter and Instagram were not using as a stand-alone platform by the users.

Table 4.34: Social Media usage

Category	Several times a day	Once a day	Once a week
Primary	190 (65.5%)	86 (29.6%)	14 (4.9%)
Secondary	1103 (70.7%)	396 (25.3%)	61 (3.91%)
Senior	238 (67.8%)	97 (27.6%)	16 (4.6%)
Tertiary	326 (68.2%)	131 (27.4%)	21 (43.9%)
Total	1857 (69.31%)	710 (26.5%)	112 (4.18%)

Table 4.34 depicts, majority (69%) were using social media for several times of the day, implying a higher usage of social media.

Table 4.35: Default security settings of social networks

Category	changing default security settings	Not changing default security settings
Primary	129 (32.2%)	271(67.8%)
Secondary	1019 (55.0%)	833(45.0%)
Senior	208(49.5%)	212(50.5%)
Tertiary	313(52.9%)	279(47.1%)
Total	1669 (51.13%)	1595 (48.86%)

Table 4.35 shows in secondary, senior, and Tertiary categories there were no significant deviations between changing security settings and not changing the settings. Also, for the total sample, 49% stated that they were changing the default security settings to increase the security of their social network sites. To validate the supposition of, this behavior was due to ICT education and Cybersecurity education/knowledge or not, two separate tests (Appendix 6.3) were conducted based on Pearson Chi-square and contingency coefficient.

1) ICT education and security measures on social networking sites.

   Category wise Pearson Chi-square tests and Contingency coefficient tests were suggested that there is a somewhat relationship between ICT education and security measures. However, the relationship is likely to be random (based on the contingency coefficient), implying having ICT education is not necessarily allow them to follow security measures in using social networking sites.

2) Cybersecurity education/training and security measures on social networking sites.

   Category wise Pearson Chi-square tests and Contingency coefficient tests were suggested that there is a somewhat relationship between Cybersecurity education/training and security measures. However, the relationship is likely to be random (based on the contingency coefficient) and surprisingly more degree of random behavior than having ICT education. This implies that having Cybersecurity education/training is not necessarily allow them to follow security measures in using social networking sites.

In addition, the employees who allowed security setting to be changed were tested based on the methods of use of the settings.

- Enabling two factor authentications (A code is sent to the mobile or the Email when someone is trying to login) and Enabling security questions considered as a less vulnerability practice.
- Making posts/Information etc. visible to a limited audience, enabling tagging notifications, and Activating recovery Email addresses/Phone numbers considered as a more vulnerability practice.

Table 4.36: Lower vulnerability practices for risks on using social media

Category	Enabling two factor authentications	Enabling Security Questions	Enabling two factor authentications and-Security Questions	None
Primary	40(31.0%)	08(6.2%)	13(10.1%)	68(52.7%)
Secondary	306(30.0%)	98(9.6%)	239(23.5%)	376(36.9%)
Senior	43(20.7%)	25(12%)	43(20.7%)	97(46.6%)
Tertiary	79(25.7%)	37(11.8%)	66(21.1%)	131(41.9%)
Total	468 (28.04%)	168 (10.06%)	361 (21.62%)	672 (40.26%)

Table 4.36 depicts, 38% were following one of the practices in their daily/weekly usage of social networks. 22% were following both practices and 40% of employees were not following any of these practices on using social media.

Table 4.37: Higher vulnerability practices on using social media

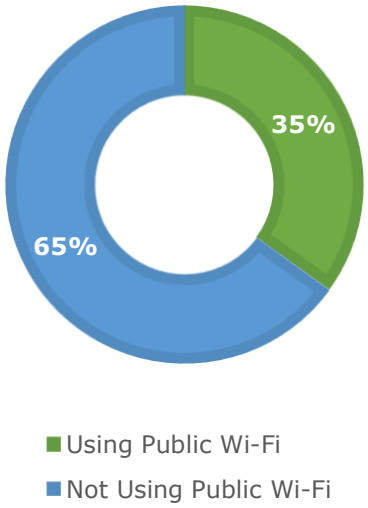
Category	Sharing posts/information etc. visible to a Limited Audience	Enabling tagging notifications	Activating recovery email	Sharing posts/information etc. visible to a Limited Audience and Enabling tagging notifications	Sharing posts/information etc. visible to a Limited Audience And Activating recovery email	Enabling tagging notifications And Activating recovery email	Following All Practices
Primary	11 (18.0%)	4 (6.5%)	28 (45.9%)	3 (4.9%)	2 (3.3%)	5(8.2%)	8 (13.2)
Secondary	58 (9.5%)	45 (7.4%)	202 (33.3%)	21 (3.4%)	87 (14.3%)	56 (9.2%)	136 (22.9%)
Senior	12 (9.9%)	07 (5.7%)	62 (52.2%)	03 (2.4%)	15 (12.3%)	06 (4.9%)	16 (13.2%)
Tertiary	12 (6.5%)	10 (5.4%)	75 (41.2%)	04 (2.7%)	30 (16.4%)	10 (5.4%)	41 (22.4%)
Total	93 (9.59%)	66 (6.81%)	367 (37.87%)	31 (3.19%)	134 (13.82%)	77 (7.94%)	201 (20.74%)

Table 4.37 shows, 25% of respondents were using more than one practices mentioned in above while 20% were following all three practices. Many of them were had activated a recovery email as a single practice.

4.9. Public Wi-Fi

This section explains the public Wi-Fi usage.

Figure 4.12: Usage of public Wi-Fi



Category-wise, 28% of primary, 35% of secondary, 45% of senior, and 35% of tertiary employees were using public Wi-Fi (based on the decomposition of figure 6.5.1)

The activities performing by using public Wi-Fi is clustered under three scales of the criticality, Lower, Medium, and Higher scale activities.

1. Lower scale; Downloading (films, documents etc.)
2. Medium scale; Sending and receiving emails, using social media platforms
3. Higher scale; online payments, accessing bank accounts.

Table 4.38: Lower scale activities

Category	Downloading (films, documents etc.)	Not engaged
Primary	47(40.9%)	68(59.1%)
Secondary	361(55.8%)	286(44.2%)
Senior	90(47.9%)	98(52.1%)
Tertiary	104(50.2%)	103(49.8%)
Total	602 (52%)	555 (47.96%)

Table 4.38 reveals 52% of the respondents were engaged in a lower scale activity.

Table 4.39: Medium scale activities

Category	Sending and receiving Emails	Use social media platforms	Sending and receiving Emails and Use social media platforms	Not engaged
Primary	32(27.8%)	47(40.9%)	15(13.0%)	21(18.3%)
Secondary	322(49.8%)	110(17.0%)	140(21.6%)	75(11.6%)
Senior	99(52.7%)	33(17.6%)	47(25.0%)	9(4.8%)
Tertiary	87(42.0%)	34(16.4%)	66(31.9%)	20(9.7%)
Total	540 (46.67%)	224 (19.36%)	268 (23.16%)	125 (10.8%)

Table 4.39 shows, of the total, 23% were engaged in both activities, while 47% and 19% were sending/receiving emails and using social media platforms, respectively.

Table 4.40: Higher scale activities

Category	Doing online payments	Accessing bank accounts	Doing online payments And Accessing bank accounts	Not engaged
Primary	8(7.0%)	3(2.6%)	3(2.6%)	101(87.8%)
Secondary	32(4.9%)	31(4.8%)	33(5.1%)	551(85.2%)
Senior	21(11.2%)	10(5.3%)	11(5.9%)	146(77.7%)
Tertiary	12(5.8%)	16(7.7%)	17(8.2%)	162(78.3%)
Total	73 (6.3%)	60 (5.18%)	64 (5.53%)	960 (82.97%)

Table 4.40 shows, of the total, 83% were not conducting any kind of critical activities. Although, 5% were engaged in both critical activities, only 6% and 5% were engaged in online payments, and banking work, respectively.

The next vital step is to understand the degree of ICT education of the people who were engaged on both medium and higher scale activities. Based on the collected data, following distribution was made accordingly.

Figure 4.13: ICT education and medium scale activities

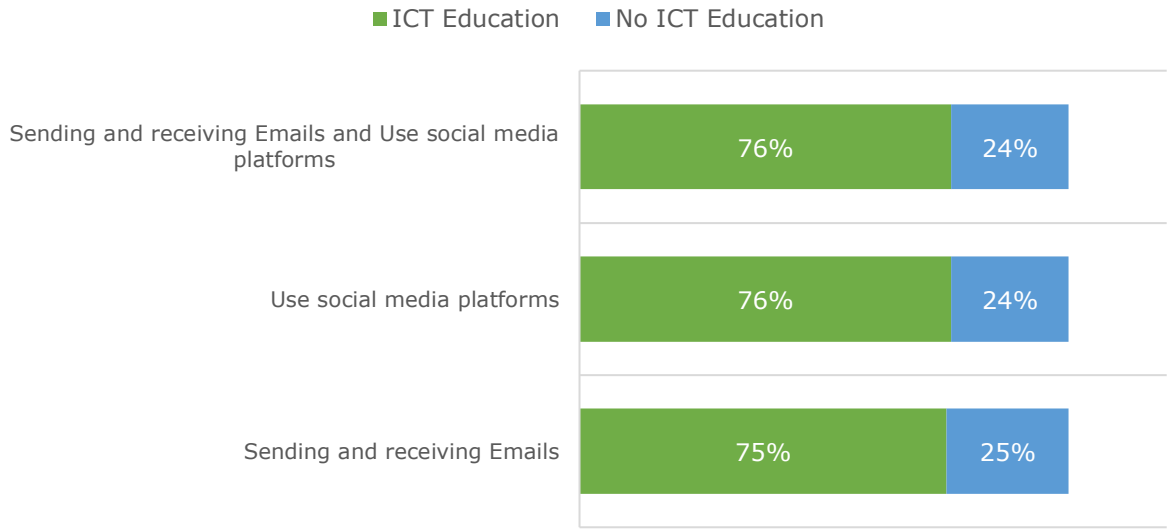


Figure 4.13 depicts the fact that majority users enrolled in these activities comprised some kind of ICT education. E.g., employees who were using Emails, around 75% of them were having ICT education. Following table represent the category wise distribution for medium scale activities.

Table 4.41: Medium scale activities and ICT education – category wise

Category (Having ICT Knowledge)	Sending and receiving Emails	Use social media platforms	Sending and receiving Emails and Use social media platforms	Not engaged
Primary	20(26.3%)	29(38.2%)	11(14.5%)	16(21.1%)
Secondary	242(46.8%)	87(16.8%)	131(25.3%)	57(11.0%)
Senior	70(50.0%)	26(18.6%)	37(26.4%)	7(5.0%)
Tertiary	72 (41.0%)	30(16.9%)	60(33.7%)	15(8.4%)
Total	404 (44.39%)	172 (18.9%)	239 (26.26%)	95 (10.43%)

Table 4.41 illustrate the category wise distribution of the results obtained and in the Figure 4.14 represent the total distribution.

Figure 4.14: ICT education and Higher scale activities.

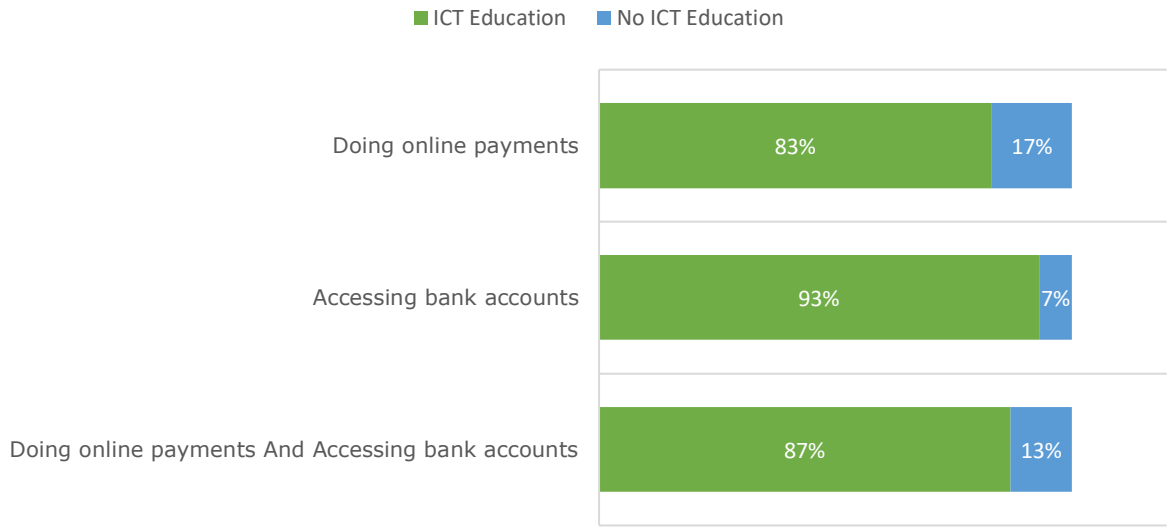


Figure 4.14 vouch for the fact that majority users enrolled in these activities comprised some kind of ICT knowledge. E.g., People who were doing online payments, 83% of them were having ICT knowledge and assessing bank accounts has 93%. Following table represent the category wise distribution for higher scale activities.

Table 4.42: Higher scale activities and ICT education – Category wise

Category	Doing online payments	Accessing bank accounts	Doing online payments And Accessing bank accounts	Not engaged
Primary	05(6.6%)	03(3.9%)	03(3.9%)	65(85.5%)
Secondary	28(5.4%)	28(5.4%)	30(5.8%)	431(83.4%)
Senior	19(13.6%)	09(6.4%)	08(5.7%)	104(74.3%)
Tertiary	09(5.1%)	16(9.0%)	15(8.4%)	138(77.5%)
Total	61 (6.69%)	56 (6.14%)	56 (6.14%)	738 (81%)

Table 4.42 illustrate the category wise distribution of the results obtained in Figure 4.15, which representing the total distribution.

Figure 4.15: Usage of Internet cafes and other communication centres

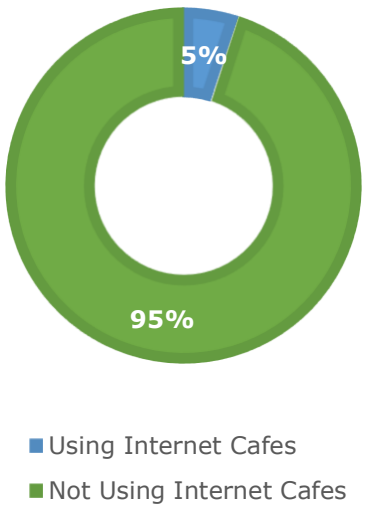


Figure 4.15 shows, majority (95%) were not using Internet cafes or communication centres for their official or personal work.

4.10. Data and Information

Table 4.43: Data loses

Category	Experienced some type of data losses	Not experienced any data losses
Primary	68(17.0%)	332(83.0%)
Secondary	458(24.7%)	139(75.3%)
Senior	91(21.7%)	329(78.3%)
Tertiary	147(24.8%)	445(75.2%)
Total	764 (38.02%)	1245 (61.97%)

Table 4.43 reveals, 38% of total employees had experienced some type of data losses. It is identified, that 62% has not experienced any data losses. The study also revealed that 84% of the employees were using a portable device (USB storage or other) in their daily routines.

Following table represent the sharing practices of portable devices with others.

Table 4.44: Sharing practice of a portable device

Category	Sharing the portable device	Not sharing the portable device
Primary	132(58.4%)	94(41.6%)
Secondary	1084(66.6%)	554(33.4%)
Senior	185(50.4%)	182(49.6%)
Tertiary	308(60.4%)	202(39.6%)
Total	1707 (62.32%)	1032 (37.67%)

Table 4.44 depicts, 62% of total employees were sharing their portable devices (USB or other) with Co-workers and external parties. Practices on keeping external storage media was evaluated and data were segmented into two groups.

1) Generic practices; store in a secure place (E.g., lockable cupboard), keeping always to themselves
2) High scale practice; Encrypt the content.

Table 4.45: Generic practices

Category	Store in a secure place	Keep it to myself	Store in a secure place and keep it to myself	None
Primary	47(11.8%)	127(31.8%)	11(2.8%)	215(53.8%)
Secondary	330(17.8%)	924(49.9%)	183(9.9%)	415(22.4%)
Senior	79(18.8%)	218(51.9%)	42(10.0%)	81(19.3%)
Tertiary	96(16.2%)	289(48.8%)	89(15.0%)	118(19.9%)
Total	552 (16.91%)	1558 (47.73%)	325 (9.95%)	829 (25.39%)

Table 4.45 shows, majority (48%) were keeping portable devices to themselves. Of the employees, 17% were storing in a secure place while 10% were doing both.

Table 4.46: High scale practices

Category	Encrypting the content	Not encrypting the content
Primary	11(2.8%)	389(97.3%)
Secondary	84(4.5%)	1768(95.5%)
Senior	19(4.5%)	401(95.5%)
Tertiary	25(4.2%)	567(95.8%)
Total	139 (4.25%)	3125 (95.74%)

Table 4.46 illustrates, 96% of total employees surveyed were not encrypting the content. It also tested with the people who had Cybersecurity education/training. The results signify, only 14% were encrypting the content, and there is no significance difference between two groups 1. People who had Cybersecurity education/training and 2. People who did not have Cybersecurity knowledge/training.

Employees who were not following any of the practices (high or medium) indicated in above were distributed in below with category wise.

- Primary (24%)
- Secondary (14%)
- Senior (11%)
- Tertiary (10%)

The questionnaire also tested against the storing behaviors of E-documents, including in the server, computer, and a portable (USB) device.

Table 4.47: Storing E-documents

Category	Server	Computer	Portable device	Server and Computer	Server and Portable device	Computer and Portable device	All places	None of the places
Primary	14 (3.5%)	118 (29.5%)	38 (9.5%)	3 (0.8%)	1 (0.3%)	50 (12.5%)	12 (3.0%)	164 (41.0%)
Secondary	65 (3.5%)	666 (36.0%)	121 (6.5%)	50 (2.7%)	21 (1.1%)	713 (38.5%)	111 (6.0%)	105 (5.7%)
Senior	18 (4.3%)	117 (27.9%)	31 (7.4%)	24 (5.7%)	2 (0.5%)	173 (41.2%)	34 (8.1%)	21 (5.0%)
Tertiary	20 (3.4%)	179 (30.2%)	33 (5.5%)	37 (6.3%)	3 (0.5%)	233 (39.5%)	33 (5.6%)	54 (9.1%)
Total	117 (3.58%)	1080 (33.08%)	223 (6.83%)	114 (3.49%)	27 (0.82%)	1169 (35.81%)	190 (5.82%)	344 (10.53%)

Table 4.47 included the employees who had an awareness on storing E-documents. This elaborate the fact that majority (36%) were storing E-documents in their computers and portable or USB devices, followed by 33% in their computers. Only 7% were storing in a portable device and 4% were storing in a server. However, 10% were not storing any of the places mentioned in this table. In addition, according to the respondnets,164 (5%) respondents had no idea on where his or her E-documents were storing.

Table 4.48: Backing-up E-Documents

Category	Backup E-documents	Not back-up E-documents	Never back-up Documents	Do not know
Primary	91(22.8%)	123(30.8%)	52(13.0%)	134(33.5%)
Secondary	1113(60.1%)	516(27.9%)	134(7.2%)	89(4.8%)
Senior	280(66.7%)	102(24.3%)	18(4.3%)	20(4.8%)
Tertiary	356(60.1%)	174(29.4%)	25(4.2%)	37(6.3%
Total	1840 (56.37%)	915 (28.03%)	229 (7%)	280 (8.57%)

Table 4.48 depicts, 56% of the total employees backed-up their E-documents, 28% did not back-up and 7% were never did a back-up. In addition, 9% were had no awareness on back-up process of the E-documents. Table indicated in below shows the frequency of E-documents backup by the people who had backed-up their documents.

Table 4.49: Frequency on E-documents back-up

Category	Daily	Monthly	Quarterly	Annually
Primary	22(26.2%)	35(41.6%)	16(19.0%)	11(13.2%)
Secondary	352(33.0%)	368(34.5%)	270(25.3%)	76(7.1%)
Senior	83(31.6%)	80(30.5%)	66(25.2%)	33(12.6%)
Tertiary	116(34.4%)	123(36.5%)	73(21.7%)	25(7.4%)
Total	573 (32.76%)	606 (34.64%)	425 (24.29%)	145 (8.29%)

As Table 4.49 illustrate, majority (35%) were backing-up their documents monthly, 33% were in daily basis and 24% were in quarterly basis. Following table represent the practices followed by employees when storing E-documents backups. For the analysis purposes, the behaviors segmented in to two components.

1) Highest exposure; maintaining a copy in same computer, in an external storage and keep outside the office
2) Lowest exposure; Keep a copy in the email, external storage media keep outside the office, remote or online storage facility.

Table 4.50: Highest exposure practices in maintaining storage

Category	Practice in maintaining storage			
	copy in the same computer	In an external storage media & kept outside the office	A copy in the same computer & in an external storage media & kept outside the office	None
Primary	65(16.3%)	33(8.3%)	06(1.5%)	296(74.0%)
Secondary	467(25.2%)	349(18.8%)	64(3.5%)	972(52.5%)
Senior	91(21.7%)	80(19.0%)	35(8.3%)	214(51.0%)
Tertiary	142(24.0%)	127(21.5%)	42(7.1%)	281(47.5%)
Total	765 (23.43%)	589 (18%)	147 (4.5%)	1763 (54%)

Table 4.50 reflects, majority (54%) were not following any of highest exposure practices. Only 23% and 18% were maintaining a copy in the same computer and storing in an external device which kept outside the office respectively.

Table 4.51: Lowest exposure practices

Category	Keep a copy in email	In an external storage media and kept inside the office	In a remote online storage facility/ data center/ server	A copy in email and In an external storage media and kept inside the office	A copy in email and In a remote online storage facility/ data center/ server	In an external storage media and kept inside the office And in a remote online storage facility/ datacenter/ server	Following all practice	None
Primary	44 (11.0%)	37 (9.3%)	14 (3.5%)	05 (1.3%)	03 (0.8%)	02 (0.5%)	-	295 (73.8%)
Secondary	246 (13.3%)	425 (22.9%)	123 (6.6%)	105 (5.7%)	37 (2.0%)	30 (1.6%)	24 (1.3%)	862 (46.5%)
Senior	59 (14.0%)	99 (23.6%)	21 (5.0%)	23 (5.5%)	13 (3.1%0	11 (2.6%)	11 (2.6%)	183 (43.6%)
Tertiary	113 (19.1%)	125 (21.1%)	27 (4.6%)	36 (6.1%)	21 (3.5%)	10 (1.7%)	08 (1.4%)	252 (42.6%)
Total	462 (14.15%)	686 (21%)	185 (5.66%)	169 (5.17%)	74 (2.26%)	53 (1.62%)	43 (1.31%)	1592 (48.77%)

Table 4.51 revealed, 48.7% of the total employees were not following any of good practices in storing E-documents backups. Only 09% were following more than one practice and 1.3 % were following all practices.

4.11. Behaviors

4.11.1. Generic behaviors

Following Table represent the practices ensuing by the employees when using their computers. As seen in above, practices are divided in to two categories, critical and non-critical.

1) Critical; keeping the computer logged in while they are away from the desk, letting co-workers to switch off the computers
2) Noncritical; logged out from the computer when it not using.

Table 4.52: Critical activities on using a computer

Category	I keep my computer logged in while I am away from my desk	I let my co-workers to switch off my computer	I keep my computer logged in while I am away from my desk and I let my co-workers to switch off my computer	None
Primary	58(14.5%)	62(15.5%)	05(1.3%)	275(68.8%)
Secondary	634(34.2%)	205(11.1%)	26(1.4%)	987(53.3%)
Senior	111(26.4%)	15(3.6%)	04(1.0%)	290(69.0%)
Tertiary	231(39.0%)	27(4.6%)	07(1.2%)	327(55.2%)
Total	1034 (31.67%)	309 (9.46%)	42 (1.28%)	1879 (57.56%)

Table 4.52 reveals that 57.6% were not following critical activities which means that 42.4% were following some critical activities on using a computer. Further, of the employees, 31.7 % were logged in while they were away from their desks, 9.5 % were letting Co-workers to switch off the computers and 1.3 % were doing both.

Table 4.53: Noncritical activities on using a computer

Category	Logged out from the computer when not using it	None
Primary	310(77.5%)	90(22.5%)
Secondary	799(43.1%)	1053(56.9%)
Senior	119(28.3%)	301(71.7%)
Tertiary	242(40.9%)	350(59.1%)
Total	1470 (45%)	1797 (55%)

Table 4.53 shows 55% of the total employees were not following the practice of logging out when they are away from desktops or laptops. Further, this behavior is tested with ICT education and Cybersecurity education/training. The statistical tests were based on Pearson Chi-square, and contingency coefficient (Appendix 7.1). The results are given in below.

1) ICT education and behaviors

Highly significant Chi-square value suggest that there is a relationship between ICT education and behaviors, which is separated in to critical and non-critical. Although, highly significant contingency coefficient and extremely low value of the coefficient imply, the behavior is random. This implicit, people who were having ICT education was not necessarily following good practices.

2) Cybersecurity education/training and behaviors

Mirroring results were generated as with the ICT education, highly significant Chi-square value suggest that there is a relationship between Cybersecurity education/training and behaviors. Although, highly significant contingency coefficient and extremely low value of the coefficient implies, the behavior is random. Surprisingly, the coefficient value is lower than that was tested against ICT education, increasing the degree of random behavior. This implies people who were having Cybersecurity education/training was not necessarily following good practices.

Following table represents usual actions taken, if they received an Email with an unknown attachment. The actions are split into two components, critical and non-critical.

1. Critical actions; open the attachment and check, ignore it completely, delete it immediately.
2. Noncritical actions; open the attachment based on the preview, check the attachment type and decide, and check the mail header.

Table 4.54: Critical actions- in E mail handling

Category	Open and check	Ignore completely	Delete immediately	Open check & Ignore completely	Open, check and Delete immediately	Ignore & delete immediately	All actions	None
Primary	90 (22.5%)	89 (22.3%)	70 (17.5%)	01 (0.3%)	01 (0.3%)	05 (1.3%)	-	144 (36.0%)
Secondary	286 (15.4%)	431(23.3%)	236 (12.7%)	08 (0.4%)	12 (0.6%)	30 (1.6%)	08 (0.4%)	841 (45.4%)
Senior	56 (13.3%)	105 (25.0%)	58 (13.8%)	-	2 (0.5%)	13 (3.1%)	02 (0.5%)	184 (43.8%)
Tertiary	75 (12.7%)	154 (26.0%)	68 (11.5%)	02 (0.3%)	04 (2.9%)	17 (2.9%)	-	272 (45.9%)
Total	507 (15.53%)	779 (23.86%)	432 (13.23%)	11 (0.33%)	19 (0.58%)	65 (1.99%)	10 (0.3%)	1441 (44.14%)

Table 4.54 shows that employees, as a single critical practice, 15% of them open the attachment and checkout immediately, 23% were ignoring the emails, and 13% were deleting the mails with unknown attachments without knowing the importance of the attachments

Table 4.55: Noncritical actions

Category	Based on preview, delete or read	Check the attachment and decide	Check the mail header details	preview, delete or read & check the attachment and decide	preview, delete or read & check the mail header details	Check the attachment type and decide & check the mail header details	All actions	None
Primary	31 (7.8%)	16 (4.0%)	40 (10.0%)	04 (1.0%)	02 (0.5%)	-	01 (0.3%)	306 (76.5%)
Secondary	319 (17.2%)	197 (10.6%)	271 (14.6%)	58 (3.1%)	24 (1.3%)	33 (1.8%)	33 (1.8%)	917 (49.5%)
Senior	84 (20.0%)	55 (13.1%)	52 (12.4%)	09 (2.1%)	04 (1.0%)	08 (1.9%)	06 (1.4%)	202 (48.1%)
Tertiary	80 (13.5%)	74 (12.5%)	92 (15.5%)	12 (2.0%)	15 (2.5%)	06 (1.0%)	14 (2.4%)	299 (17.3%)
Total	514 (15.74%)	342 (10.47%)	455 (13.93%)	83 (2.54%)	45 (1.37%)	47 (1.43%)	54 (1.65%)	1724 (52.8%)

Table 4.55 shows, majority (52%) were not following these safe actions when they received an Email with an unknown attachment. Of the employees, as a single non-critical practice, 16% were referring to preview, 10% were checking the type of the attachment, 14% were checking the mail header. Only, 7% were engaged in more than one safe-side behaviors.

Further, this behavior is tested with ICT education and Cybersecurity education/training. The statistical tests were based on Pearson Chi-square, and contingency coefficient (Appendix 7.2). The results are given in below.

1) ICT education and behaviors

   Highly significant Chi-square value suggest that there is a relationship between ICT education and behaviors, which is separated in to critical and noncritical. Although, highly significant contingency coefficient and extremely low value which is closer to zero implies, the behavior is random. This implicit, people who were having ICT education was not necessarily following good practices.

2) Cybersecurity education/training and behaviors

   Highly significant Chi-square value suggest that there is a relationship between Cybersecurity education/training and behaviors. Although, highly significant contingency coefficient and extremely low value of the coefficient implies, the

behavior is random. There is no significant difference with the value of the coefficient that was tested against ICT education. This implies people who were having Cybersecurity education/training was not necessarily following good practices.

Following tables are testing the behaviors of the employees, in the scenario of, if they received an Email with an unknown link.

Table 4.56: Actions for unknown link in an Email

Category	Just click on the link.	Check the URL carefully.	Ignore it completely.	Delete it immediately.
Primary	93(23.3%)	46(11.5%)	204(51.0%)	57(14.2%)
Secondary	206(11.1%)	401(21.7%)	1019(55.0%)	226(12.2%)
Senior	24(5.7%)	97(23.1%)	234(55.7%)	65(15.5%)
Tertiary	56(9.5%)	141(23.8%)	322(54.4%)	73(12.3%)
Total	379 (11.61%)	685 (20.98%)	1779 (54.5%)	421 (12.89%)

Table 4.56 signifies, 11% were clicking the link without any awareness, 21% were checking the URL carefully, 54% were ignoring the link whether it is important or not, and 14% were deleting the link immediately.

In addition, this behavior was tested against the ICT education of the employees. The testing was based on best practice (Checking the URL carefully) Vs Other practices (Click on the link, ignoring, and deleting immediately).

Table 4.57: Practices followed by the employees who have ICT education

Category	Good practice	Other
Primary	37(18.7%)	161(81.3%)
Secondary	340(23.8%)	1086(76.2%)
Senior	75(25.6%)	218(74.4%)
Tertiary	115(25.4%)	338(74.6%)
Total	567 (23.92%)	1803 (76%)

This reveals the fact that 76% of total employees were not following good practices. In addition, a significant test was conducted (Appendix 7.3.) for category wise distribution based on the Chi-square and systematic measures. The purpose is to check the distribution of the behavior of the employees given ICT education.

1) For primary category There is an association between behavior after receiving an Email with ICT education. Lower degree of association between column and raw variables implying, having ICT education is not the case to engage in good practice.
2) For secondary category There is an association between behavior after receiving an Email with ICT education. Lower degree of association between column and

raw variables implying, having ICT education is not the case to engage in good practice.

3) For senior category There is an association between behavior after receiving an Email with ICT education. Lower degree of association between column and raw variables implying, having ICT education is not the case to engage in good practice.
4) For tertiary, marginally reject the null hypothesis. However, according to contingency coefficient, lower degree of association between column and raw variables, having ICT education is not the case to engage in good practice.
5) Following tables observed the behavior of the respondents given receiving various types of the Emails.

Table 4.58: Respond to an Email saying, "you have won a lottery".

Category	I will pay the $100 soon and will win the prize.	I will seek advice from some known party.	I will ignore the e-mail.
Primary	11(2.8%)	74(18.5%)	315(78.8%)
Secondary	18(1.0%)	345(18.6%)	1489(80.4%)
Senior	01(0.2%)	62(14.8%)	357(85.0%)
Tertiary	14(2.4%)	94(15.9%)	484(81.8%)
Total	44 (1.34%)	575 (17.61%)	2645 (81%)

In the questionnaire, this table reflect the question of when a respondent receives an Email saying that "you have won a lottery. To receive the prize $100 payment should be made to an account", while the respondents were tasked to pick an action mentioned in this table. This shows that majority (81%) would ignore the Email, while 18% would seek some advice from some known party.

Table 4.59: Responding to Email from the head of the organization

Category	I share the details without hesitation.	I verify with the sender of the e-mail and send the password.	I will call him.	I never share any login details with anyone
Primary	110(27.5%)	34(8.5%)	108(27.0%)	148(37.0%)
Secondary	124(6.7%)	270(14.6%)	669(36.1%)	789(42.6%)
Senior	11(2.6%)	52(12.4%)	141(33.6%)	216(51.4%)
Tertiary	34(5.7%)	80(13.5%)	220(37.2%)	258(43.6%)
Total	279 (8.54%)	436 (13.35%)	1138 (34.86%)	1411 (43.22%)

This scenario was tested in the form of, if an employee received an Email from the IT head of his or her organization requesting the password of official login, the respondents were tasked to select an action. Table 4.59 reveals that majority (43%) would not share their details, 35% would call for a verification, 13% would verify through an Email, and only 9% would share the details without any hesitation. Of the respondents who would provide

the details (9%) are assessed against their ICT and Cybersecurity education/training. The results are shown in the following graph.

Figure 4.16: ICT and Cybersecurity education/training in critical group

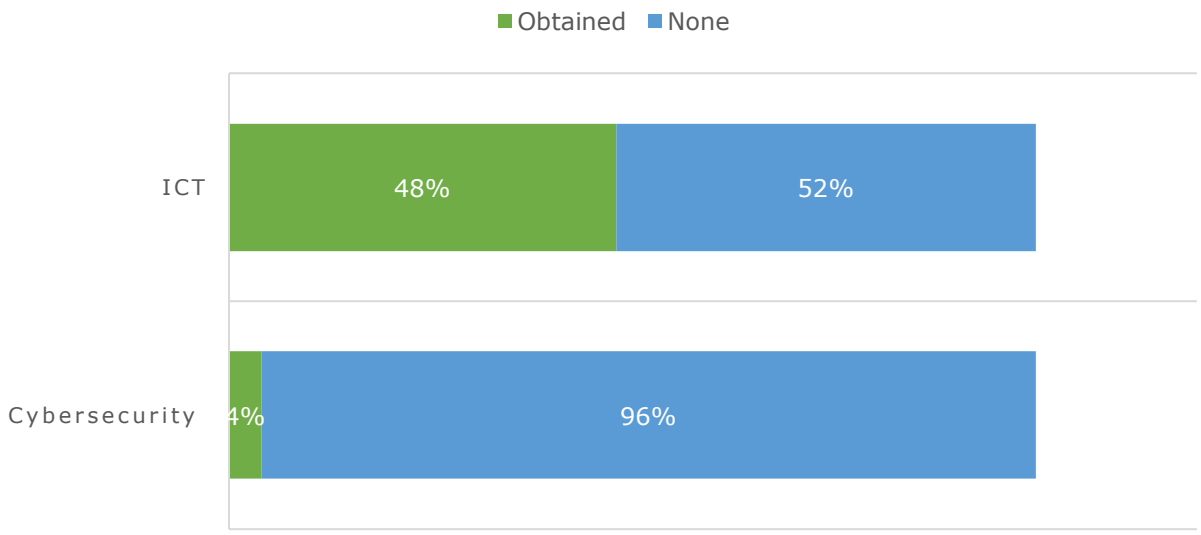


Figure 4.16 implicit, 48% people who would share the details had any kind of ICT education and 4% had Cybersecurity education/training.

Table 4.60: Responding to an Email from the bank

Category	I will click on the link and enter my username and password. – Non secure	I will click on the link, but I will not enter my username and password. – Non secure	I will call the customer care center of my bank and seek advice - Secure	I will ignore the e-mail. – non secure
Primary	12 (3.0%)	20 (5.0%)	255 (63.7%)	113 (28.2%)
Secondary	58 (3.1%)	120 (6.5%)	1411 (76.2%)	263 (14.2%)
Senior	5 (1.2%)	22(5.2%)	324(77.1%)	69 (16.4%)
Tertiary	14 (2.4%)	33 (5.6%)	431(72.8%)	114(19.3%)
Total	89 (2.72%)	195 (5.97%)	2421 (74.17%)	559 (17.12%)

In the questionnaire, the scenario was in the context of, if a respondent receives an Email saying his or her account will be deactivated soon unless they click the link and provide their username and password. Table 4.60 shows, majority (74%) would call the customer centre for advice, 17% would ignore the email, 6% would click the link, and 3% would send username and password.

To clarify the fact of whether this behavior of the majority would do something with the ICT education and Cybersecurity education/training, few tests were conducted (Appendix 7.4). The behaviors are segmented in to three components.

- High (Secure); click on the link and enter my username and password, click on the link, but I will not enter my username or password.
- Medium (Non-secure); Ignore the email
- Low (Secure); call the customer care center of my bank and seek advice.

The statistical tests were conducted based on the Chi-square and Contingency coefficient tests. The results could be summarized as indicated in below.

1. Highly significant Pearson Chi-square test suggests, there is a somewhat relationship between scale of practices and ICT education. Although, contingency coefficient value implies, this behavior is random and not necessarily based on the ICT education.

2. For the Cybersecurity education/training, null hypothesis is not rejected, showing there is no relationship between scale of behavior and Cybersecurity education/training. This also validated with the very lower level of contingency coefficient which is closer to zero.

Following table represent practices following when entering login credentials into a familiar website. For analysis purposes, the practices are segmented in to three categories.

- High scale practices (secure); before entering login credentials into a website, search for the (Green padlock in the address bar) https, check the content of the website, and always carefully check the URL (Website address) for accuracy.
- Medium scale practices (Non secure); I trust the links shared by my friends.
- Lower scale (severe); Never check anything.

Table 4.61: Higher scale practices

Category	I search for the (Green padlock in the address bar) https	I always carefully check the URL (Website address) for accuracy	I check the content of the website – Higher (secure)	I search for the https and I always carefully check the URL (Website address) for accuracy	I search for the https and I check the content of the website – Higher (secure)	I always carefully check the URL for accuracy and I check the content of the website – Higher (secure)	All practices	None
Primary	35 (8.8%)	27 (6.8%)	25(6.3 %)	5 (1.3%)	3(0.8%)	4 (1.0%)	4 (1.0%)	297 (74.3%)
Secondary	149 (8.0%)	267 (14.4%)	184 (9.9%)	60 (3.2%)	18 (1.0%)	84 (4.5%)	74 (4.0%)	1016 (54.9%)
Senior	24 (5.7%)	60 (14.3%)	35 (8.3%)	14 (3.3%)	4 (1.0%)	23 (5.5%)	17 (4.0%)	243 (57.9%)
Tertiary	65 (11.0%)	71 (12.0%)	53 (9.0%)	25 (4.2%)	6 (1.0%)	31 (5.2%)	31 (5.2%)	310 (52,4%)
Total	273 (8.36%)	425 (13.02%)	297 (9%)	104 (3.18%)	31 (0.94%)	142 (4.35%)	126 (3.86%)	1866 (57.16%)

Table 4.61 reveals, majority (57%) were not following any of the higher scale (secure) practices mentioned in above. Of the respondents, as a single practice, 8% were checking login credentials, 13% were checking URL, and 9% were checking the content, while 12% were in the wake of combinations of two or more practices. Of the employees, who do not follow any of the high-scale (secure) practices, are assessed against their ICT and Cybersecurity education/training. The results are shown in the following graph.

Figure 4.17: ICT and Cybersecurity education/training in the non-secure group.

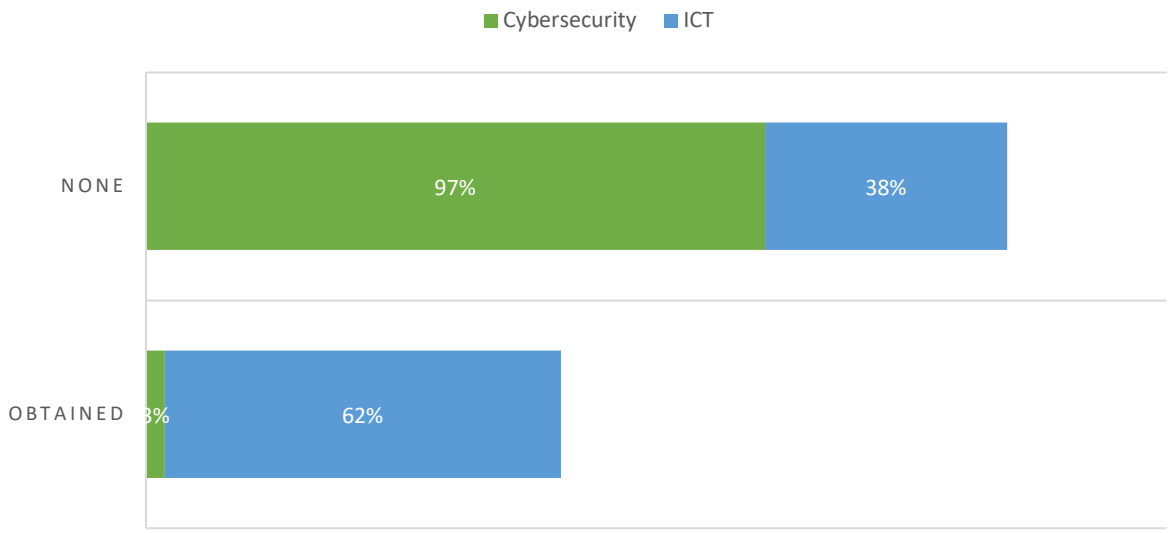


Figure 4.17 implicit, 62% people who would share the details had any kind of ICT education and 3% had Cybersecurity education/training.

Table 4.62: Medium scale practice: Trusting the links shared by friends

Category	Trusting the links	None
Primary	23(5.8%)	337(93.4%)
Secondary	97(5.2%)	1755(94.8%)
Senior	26(6.2%)	394(93.8%)
Tertiary	172(5.3%)	3092(94.7%)
Total	318 (5.39%)	5578 (94.6%)

Table 4.63: Lower scale (severe) practice

Category	Not following any practice	Following at least one High scale or medium scale practice
Primary	223(55.8%)	177(44.3%)
Secondary	837(45.2%)	1015(54.8%)
Senior	187(44.2%)	233(55.5%)
Tertiary	255(43.1%)	337(56.9%)
Total	1502 (46%)	1762 (53.98%)

Table 4.62 depicts, 94% of the total employees would not trust any links that would share by their friends. Table 4.63 shows, 46% were not checking any of these mentioned in above, when entering login credential into a website. Of the employees, who are in the vulnerable group, ICT and Cybersecurity education/training was assessed.

Figure 4.18: ICT and Cybersecurity education/training in the severe group.

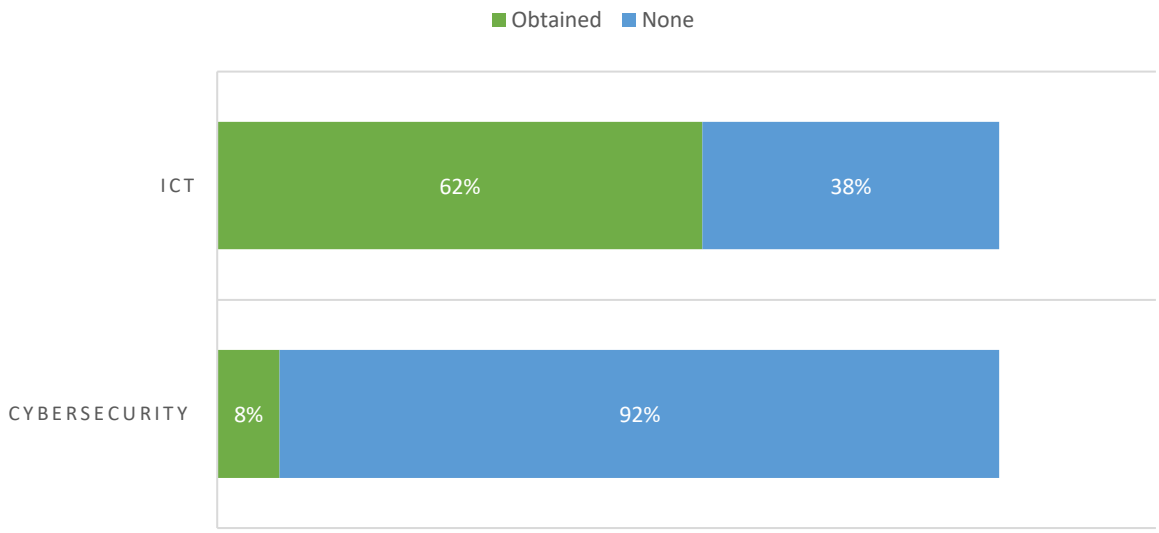


Figure 4.18 implicit, 62% people who would share the details had any kind of ICT education and 8% had Cybersecurity education/training.

Following tables represent the practices abide by the respondents in reference on using computers in internet cafes, communication centres, libraries etc. The behaviors are segmented in to three scales.

- High (Secure); never let browser to save login credentials, using private or safe browsing
- Medium (Not secure); Clear cache after usage, permanently delete downloaded documents.
- Lower (Sever); Do not use any of the practices and no awareness on these practices.

Table 4.64: High scale practices (Secure)

Category	I never let the browser to save my login credentials	I use private (safe) browsing	Both practices	None
Primary	21(5.3%)	18(4.5%)	2(0.5%)	359(89.8%)
Secondary	88(4.8%)	49(2.6%)	36(1.9%)	1679(90.7%)
Senior	19(4.5%)	8(1.9%)	5(1.2%)	388(92.4%)
Tertiary	42(7.1%)	8(1.4%)	4(0.7%)	538(90.9%)
Total	170 (5.2%)	83 (2.54%)	47 (1.43%)	2964 (90.8%)

Table 4.64 implies, majority (91%) were not using any of these secure practices on using a third-party computer. Perhaps, it may be the case that majority were not using communication centres and internet cafes.

Table 4.65: Medium scale practices

Category	Clear the cache after usage	Permanently delete all the downloaded documents to the computer I used	Following Both practices	None
Primary	8(2.0%)	13(3.3%)	4(1.0%)	375(93.8%)
Secondary	43(2.3%)	50(2.7%)	39(2.1%)	1720(92.9%)
Senior	5(1.2%)	12(2.9%)	9(2.1%)	394(93.8%)
Tertiary	8(1.4%)	14(2.4%)	7(1.2%)	563(95.1%)
Total	64 (1.96%)	89 (2.72%)	59 (1.8%)	3052 (93.5%)

Table 4.65 implies, majority (94%) were not using any of these secure practices on using a third-party computer. Perhaps, it may be the case that majority were not using communication centres and internet cafes. For the lower scale (severe) practices, the results were the same as above practices. Majority (77%) were not engaged in lower scale practices.

4.11.2. Sensitive Data and Information

Sensitive data and information sharing channels with Co-workers also segmented in to following categories based on the exposures to hazards. Sensitive data and information distribution channels with Co-workers.

- Higher scale (Secure); Via private Email, Via official Email
- Medium Scale (Non-secure); By copying to a storage (e.g.: HD, DVD, USB) devices.
- Lower scale (Severe); Through intranet (ex: shared folder, drive), using the cloud services (ex: iCloud, Drop Box, Google Drive), social media apps (WhatsApp, Viber, FB Messenger).

Table 4.66: Higher scale channels – with Co-workers

Category	Via Private Email	Via Official Email	Via Private Email and Official Email	None
Primary	52(13.0%)	33(8.3%)	7(1.8%)	308(77.0%)
Secondary	320(17.3%)	629(34.0%)	112(6.0%)	791(42.7%)
Senior	75(17.9%)	185(44.0%)	43(10.2%)	117(27.9%)
Tertiary	143(24.2%)	208(35.1%)	45(7.6%)	196(33.1%)
Total	590 (18%)	1055 (32.32%)	207 (6.34)	1412 (43.25%)

Table 4.66 shows, 43 % of total respondents were not using any of these channels of the employees, 18% were sharing information via private Email, 32% via official Email and 6% were using both for sharing purposes.

Table 4.67: Medium scale channels – with Co-workers

Category	copying to a Storage (e.g: HD, DVD, USB) devices	None
Primary	81(20.3%)	319(79.8%)
Secondary	605(32.7%)	1247(67.3%)
Senior	108(25.7%)	312(74.3%)
Tertiary	195(32.9%)	397(67.1%)
Total	989 (30.3%)	2275 (69.69%)

Table 4.67 depicts, 30% of total employees were using storage devices when they were sharing the sensitive information with Co-Workers.

Table 4.68: Lower scale channels – with Co-workers

Category	Through Intranet	Using the Cloud services	Social media apps	Through Intranet and Using the Cloud services	Through Intranet and Social media apps	Using the Cloud services and Social media apps	All channels	None
Primary	30 (7.5%)	13 (3.3%)	110 (27.5%)	-	9 (2.3%)	3 (0.8%)	4 (1.0%)	231 (57.8%)
Secondary	235 (12.7%)	64 (3.5%)	318 (17.2%)	37 (2.0%)	92 (5.0%)	22 (1.2%)	38 (2.1%)	1046 (56.5%)
Senior	40 (9.2%)	16 (3.8%)	62 (14.8%)	11 (2.6%)	23 (5.5%)	5 (1.2%)	13 (3.1%)	250 (59.5%)
Tertiary	54 (9.1%)	22 (3.7%)	84 (14.2%)	9 (1.5%)	26 (4.4%)	6 (1.0%)	20 (3.4%)	371 (62.7%)
Total	359 (10.9%)	115 (3.52%)	574 (17.58%)	57 (1.74%)	150 (4.59%)	36 (1.1%)	75 (2.29%)	1898 (58.14%)

Table 4.68 illustrate,58% is not engaged in lower scale channel which indicates that 42% of total employees were using any of lower scale channels to share sensitive data and information. It was identified, 11% were using intranet, 4% were using cloud services, 18% were using social media apps, and 10% were using combinations of two or more channels to share information. Further, above scaled channels are compared with ICT and Cybersecurity education/training level of the employees. The statistical tests (Appendix 7.5) are based on Pearson Chi-square for each, and every category and systematic measures based on contingency coefficient.

1) ICT education and choosing a sharing channel

The null hypothesis is not rejected for all category levels, accept secondary category. Although, it is also not rejected for total sample. It implies that choosing channels and ICT education do not have any association. This also validated with contingency value which is almost closer to zero. This suggest that choosing an information sharing channel do not have anything to do with their ICT education.

2) Cybersecurity education/training and choosing a sharing channel

The null hypothesis is not rejected for all category levels, accept senior category. Although, it is also not rejected for total sample. It implies that choosing channels and Cybersecurity education/training do not have any association. This also validated with contingency value which is almost closer to zero. This suggest that choosing an information sharing channel do not have anything to do with their Cybersecurity education/training.

As in above sensitive data and information sharing channels with External parties segmented in to following categories based on the exposures to risks.

Sensitive data and information distribution channels with External parties.

- Higher scale (Secure); Via private Email, Via official Email
- Medium Scale (Non-secure); By copying to a storage (e.g.: HD, DVD, USB) devices.
- Lower scale (Severe); Through intranet (ex: shared folder, drive), using the cloud services (ex: iCloud, Drop Box, Google Drive), social media apps (WhatsApp, Viber, FB Messenger).

Table 4.69: Higher scale channels – with External parties

Category	Via Official Email	Via Private Email	Via Private Email and Official Email	None
Primary	14(3.5%)	60(15.0%)	5(1.3%)	321(80.3%)
Secondary	305(16.5%)	573(30.9%)	44(2.4%)	930(50.2%)
Senior	81(19.3%)	175(41.7%)	17(4.0%)	147(35.0%)
Tertiary	108(18.2%)	213(36.0%)	17(2.9%)	254(42.9%)
Total	508(15.5%)	1021(31.28%)	83(2.54%)	1652(50.61%)

Table 4.69 depicts, 50% of total respondents were not using any of these channels. Of the employees, 31% were sharing information via private Email, 15% via official Email and 2% were using both for sharing purposes.

Table 4.70: Medium scale channels – with External parties

Category	copying to a Storage (e.g.: HD, DVD, USB) devices	None
Primary	56(14.0%)	344(86.0%)
Secondary	281(15.2%)	1571(84.8%)
Senior	56(13.3%)	364(86.7%)
Tertiary	96(16.2%)	496(83.8%)
Total	489(14.98%)	2775(85%)

According to table 4.70, only 15% of total employees were using storage devices when they are sharing the sensitive information with External workers.

Table 4.71: Lower scale channels – with External parties

Category	Through Intranet	Using the Cloud services	Social media apps	Through Intranet and Using the Cloud services	Through Intranet And Social media apps	Using the Cloud services and Social media apps	All channels	None
Primary	10 (2.5%)	7 (1.8%)	150 (37.5%)	-	1 (0.3%)	11 (2.8%)	3 (0.8%)	218 (54.5%)
Secondary	45 (2.4%)	58 (3.1%)	452 (24.4%)	5 (0.3%)	14 (0.8%)	42 (2.3%)	12 (0.6%)	1224 (66.1%)
Senior	8 (1.9%)	14 (3.3%)	108 (25.7%)	-	6 (1.4%)	11 (2.6%)	4 (1.0%)	269 (64.0%)
Tertiary	5 (0.8%)	17 (2.9%)	145 (24.5%)	1 (0.2%)	5 (0.8%)	12 (2.0%)	5 (0.8%)	402 (67.9%)
Total	68(2%)	96 (2.9%)	855 (26.1%)	6 (0.18%)	26 (0.79%)	76 (2.32%)	24 (0.73%)	2113 (64.73%)

Table 4.71 illustrate that 65% employees are not using any lower scale channels which implies that 35% of the employees are using any of lower scale channels to share sensitive data and information. It was identified, 2% were using intranet, 3% were using cloud services, 26% were using social media apps, and only 4% were using combinations of two or more channels to share information.

Further, above scaled channels with external parties are compared with ICT and Cybersecurity education/training level of the employees. The statistical tests (Appendix 7.6) are based on Pearson Chi-square for each, and every category and systematic measures based on contingency coefficient. The results are mirror reflection with the results obtained in appendix 7.5 in above.

1) ICT education and choosing a sharing channel

The null hypothesis is not rejected for all category levels, accept tertiary category. Although, it is also not rejected for total sample. It implies that choosing channels and ICT education do not have any association. This also validated with contingency value which is almost closer to zero. This suggest that choosing an information sharing channel do not have anything to do with their ICT education.

2) Cybersecurity education/training and choosing a sharing channel

The null hypothesis is not rejected for all category levels. It implies that choosing channels and Cybersecurity education/training do not have any association. This also validated with contingency value which is almost closer to zero. This suggest that choosing an information sharing channel do not have anything to do with their Cybersecurity education/training.

The next steps are to evaluate the practices following by the employees when they are sharing the sensitive information with Co-workers. To simplify the analysis, the group who were sharing information via emails (private and official) are considered, and assess the practices followed by this group. Given this group, following activities are scaled.

- High scale (secure); Encrypt the document using the receivers public key before sharing
- Medium scale (somewhat secure); create a Password protected document and send the password and the document through different channels.
- Lower scale (non-secure); create a Password protected document and send the password and the document through the same channel and not following any of these.

a) For primary category

Table 4.72: Primary category practices

	Create a Password protected document and send the password and the document through the same channel	Create a Password protected document and send the password and the document through different channels.	Encrypt the document using the receivers public key before sharing.	Do not follow any of these methods.
Via private Email	2(6.5%)	1(3.2%)	-	28(90.3%)
Via official Email	2(7.7%)	3(11.5%)	1(3.8%)	20(76.9%)
Via Private and Official Email	01 (100%)	-	-	-
Total	5(8.6%)	4(6.8%)	1(1.7%)	48(82.7%)

This implicit, 82% of total employees in primary category were not following any of these high and medium scale practices, while majority consist of highest vulnerability to hazards.

b) Secondary category

Table 4.73: Secondary category practices

	Create a Password protected document and send the password and the document through the same channel/	Create a Password protected document and send the password and the document through different channels.	Encrypt the document using the receivers public key before sharing.	Do not follow any of these methods.
Via private Email	19(9.3%)	14(6.9%)	10(4.9%)	161(78.9%)
Via official Email	17(4.1%)	27(6.5%)	11(2.7%)	359(86.7%)
Via private and official Email	2(15.4%)	3(23.1%)	-	8(61.5%)
Total	38(6%)	44(6.9%)	21(3.3%)	528(83.6%)

This implicit, 84% of total employees in secondary category were not following any of these high and medium scale practices, while majority having the highest vulnerability to hazards.

c) Senior category

Table 4.74: Senior category practices

	Create a Password protected document and send the password and the document through the same channel	Create a Password protected document and send the password and the document through different channels.	Encrypt the document using the receivers public key before sharing.	Do not follow any of these methods.
Via private Email	2(4.0%)	2(4.0%)	2(4.0%)	44(88.0%)
Via official Email	4(3.0%)	13(9.8%)	1(0.8%)	114(86.4%)
Via private and official Email	-	-	-	5(100%)
Total	6(3.2%)	15(8%)	3(1.6%)	163(87.1%)

This implicit, 87% of total employees in senior category were not following any of these high and medium scale practices, while majority having the highest vulnerability to hazards.

d) Tertiary category

Table 4.75: Senior category practices

	Create a Password protected document and send the password and the document through the same channel	Create a Password protected document and send the password and the document through different channels.	Encrypt the document using the receivers public key before sharing.	Do not follow any of these methods.
Via private Email	13(13.8%)	6(6.4%)	1(1.1%)	74(78.7%)
Via official Email	13(9.4%)	12(8.6%)	8(5.8%)	106(76.3%)
Via private and official Email	-	-	-	6(100%)
Total	26(10.8%)	18(7.5%)	9(3.7%)	186(77.8%)

This implicit, 77% of total employees in tertiary category were not following any of these high and medium scale practices, while majority having the highest vulnerability to hazards.

4.12. Protection

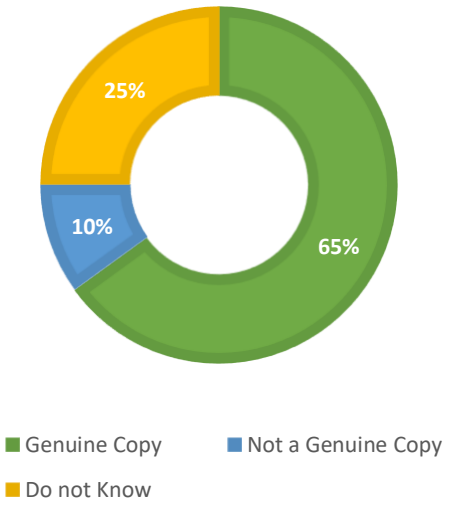
Following table represent the usage of anti-virus software.

Table 4.76: Usage of anti-virus software

Category	Using an anti-virus software	Not using an anti-virus software	No awareness
Primary	141(35.3%)	95(23.8%)	164(41.0%)
Secondary	1467(79.2%)	208(11.2%)	177(9.6%)
Senior	366(87.1%)	29(6.9%)	25(6.0%)
Tertiary	498(84.1%)	41(6.9%)	53(9.0%)
Total	2472(75.7%)	373(11.4%)	419(12.8%)

Table 4.76 reveals, 76% of total employees were using an anti-virus software while 11% were not using and 12% did not have any awareness on similar activity. Status (genuine copy or not) of the anti-virus software were assessed from the people who were using an anti-virus in their machines. Following graph exhibits the results of the observations.

Figure 4.19: Type of Anti-Virus Software



Above graph shows, 65% were using a genuine copy, 10% were not using a genuine copy, and 25% did not have an awareness of the status of anti-virus software. Following table represent the updating status of the genuine antivirus software users, that is 65% group in above figure.

Table 4.77: Update frequency of the anti-virus

Update frequency of the anti-virus	Monthly	Quarterly	Annually	Automatically	Never	I don't know how to do it.
Primary	6 (8.2%)	4 (5.5%)	8 (11.0%)	44 (60.2%)	4 (5.4%)	10 (13.7%)
Secondary	55 (6.1%)	21 (2.3%)	96 (10.6%)	669 (74.3%)	17 (1.8%)	42 (4.9%)
Senior	15 (56%)	10 (3.7%)	30 (11.2%)	204 (76.1%)	-	9 (3.3%)
Tertiary	21 (6.3%)	9 (2.7%)	30 (9.0%)	251 (76.0%)	7 (2.1%)	12 (3.6%)

Table 4.78: Identification of an infection

Category	Could identify an infection	Could not identify an infection
Primary	110(27.5%)	290(72.5%)
Secondary	1000(54.0%)	852(46.0%)
Senior	237(56.4%)	183(43.6%)
Tertiary	332(56.2%)	260(43.9%)
Total	1679(51.43%)	1585(48.56%)

Table 4.79: Scanning for viruses

Category	Scanning for viruses	Not scanning for viruses
Primary	136(34.0%)	264(66.0%)
Secondary	1299(70.1%)	553(29.9%)
Senior	291(69.3%)	129(30.7%)
Tertiary	408(68.9%)	184(31.1%)
Total	2134(65.37%)	1130(34.62%)

Table 4.78 shows, majority (72%) use automatic updates for their software, while table 4.79 depicts, 51% of employees had somewhat knowledge to identify an infection. However, when validation made on this, it is identified that majority was referred to a simple virus-infection. Table 8.4 signifies, 65% of total employees were scanning devices before plugging to their devices.

Two sections, including awareness on identification an infection and awareness on identification an unauthorized access is assessed with each other for triangular validation purposes on knowledge level of the employees. The results are indicated in following table, where subset of people who had a knowledge to identify an infection was extracted and assessed against whether they could identify an unauthorized access or none.

Table 4.80: Unauthorized identification for grouped employees who had knowledge to identify an infection

Category	Identify Unauthorized access	Could not identify unauthorized access
Primary	31(28.2%)	79(71.8%)
Secondary	340(34.0%)	660(66%)
Senior	77(32.5%)	160(67.5%)
Tertiary	102(30.7%)	230(69.3%)
Total	550(32.75%)	1129(67.24%)

Table 4.80 implies, of the people who had some knowledge to identify an unauthorized action 32.7%, while 67.2 % could not identify an unauthorized access to their machines.

4.13. Awareness

Awareness of following activities were tested for two groups, 1) General sample, 2) Group who had somewhat knowledge on Cybersecurity.

a) Malware
b) Computer virus
c) Trojan
d) Phishing
e) Website defacement
f) Cyber bulling
g) Impersonation
h) Credit card fraud
i) Locked out Email account
j) Hacked computer
k) Keystroke logging
l) Spyware
m) Spam
n) Adware
o) Ransomware

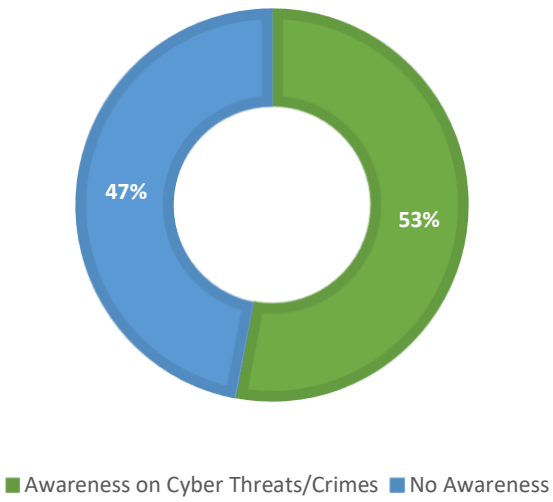
1. General sample	2. Cybersecurity group
Following represent the distribution of total employees who do not have an awareness on above activities.	Following represent the distribution of employees who had somewhat awareness on Cybersecurity
1) Malware (65%) 2) Computer virus (24%) 3) Trojan (70%) 4) Phishing (87%) 6) Website defacement (92%) 7) Cyber bulling (88%) 8) Impersonation (94%) 9) Credit card fraud (77%) 10) Locked out Email account (80%) 11) Hacked computer (55%) 12) Keystroke logging (93%) 13) Spyware (29%) 14) Spam (64%) 15) Adware (82%) 16) Ransomware (86%)	1) Malware (24%) 2) Computer virus (10%) 3) Trojan (29%) 4) Phishing (48%) 6) Website defacement (65%) 7) Cyber bulling (57%) 8) Impersonation (70%) 9) Credit card fraud (40%) 10) Locked out Email account (49%) 11) Hacked computer (32%) 12) Keystroke logging (67%) 13) Spyware (47%) 14) Spam (32%) 15) Adware (52%) 16) Ransomware (48%)
Above results shows, of the respondents, 65% did not have an awareness on Malware, 24% had no awareness on Computer virus, 70% had no awareness on Trojan etc. (Appendixes 09)	Above results shows, of the respondents who had some knowledge on Cybersecurity, 24% did not have an awareness on Malware, 10% had no awareness on Computer virus, 29% had no awareness on Trojan etc. Following table represent the awareness on social engineering activities.

Table 4.81: Social engineering activities

Category	Never heard of it	Heard, but don't know the activity	Yes
Primary	262(65.3%)	124(31.0%)	15(3.8%)
Secondary	1046(56.5%)	655(35.4%)	151(8.2%)
Senior	231(55.0%)	153(36.4%)	36(8.6%)
Tertiary	332(56.1%)	210(35.5%)	50(8.4%)
Total	1871(57.3%)	1142(34.9%)	252(7.7%)

Table 4.81 reveals, 57% of total employees have never heard of social engineering activities, 35% have heard but don't know the subject, and 7% were aware on similar activities.

Figure 4.20: Awareness on Cyber threats and crimes.



Majority (53%) do not have an awareness on Cyber threats and crimes. Category wise, 70% of primary, 53% of secondary, 42% of senior and 45% of tertiary employees did not have any awareness on similar activities. Appendix vii

Following tables represent the policy level awareness of the employees.

Table 4.82: Fair usage policy

Category	Never heard of this policy	Heard, but not having a written policy	Having a written policy
Primary	286(71.5%)	103(25.8%)	11(2.8%)
Secondary	1099(59.3%)	614(33.2%)	139(7.5%)
Senior	151(36.0%)	211(50.2%)	58(13.8%)
Tertiary	293(49.5%)	245(41.4%)	54(9.1%)
Total	1829(56%)	1173(35.9%)	262(8%)

Table 4.82 revealed that 56% has never heard of the policy, 36% have heard but not having a written policy and only 8% have a written policy. Category wise, only 13.8% of senior and 9.1% of tertiary employees stated that their organization having this kind of written policy document.

Table 4.83: Information security policy

Category	Never heard of this policy	Heard, but not having a written policy	Having a written policy
Primary	284(71.0%)	98(24.5%)	18(4.5%)
Secondary	1044(56.4%)	585(31.6%)	223(12.0%)
Senior	134(31.9%)	194(46.2%)	92(21.9%)
Tertiary	278 (47.0%)	236(39.9%)	78 (13.2%)
Total	1740(53.3%)	1113(34%)	411(12.59%)

Table 4.83 shows that 53% has never heard of the policy, 34% have heard but not having a written policy and 13% have a written policy. Category wise, only 21.9% of senior and 13.2% of tertiary employees stated that their organization having this kind of written policy document.

Table 4.84: Social Media Policy

Category	Never heard of this policy	Heard, but not having a written policy	Having a written policy
Primary	276(69.0%)	97(24.3%)	27(6.8%)
Secondary	985 (53.2%)	602(32.5%)	265 (14.3%)
Senior	129(30.7%)	217(51.7%)	74(17.6)
Tertiary	250(42.2%)	244(41.2%)	98(16.6%)
Total	1640(50.2%)	1160(35.5%)	464(14.21%)

Table 4.84 revealed that 50% has never heard of the policy, 36% have heard but not having a written policy and 114% have a written policy. Category wise only 17.6% of senior and 16.6% of tertiary employees stated that their organization having this kind of written policy document.

Table 4.85: User access policy

Category	Never heard of this policy	Heard, but not having a written policy	Having a written policy
Primary	285(71.8%)	97(24.3%)	18(4.5%)
Secondary	1050(56.7%)	592(32.0%)	210(11.3%)
Senior	131(31.2%)	199(47.4%)	90(21.4%)
Tertiary	275(46.5%)	245(41.4%)	72(12.2%)
Total	1741(53.3%)	1133(34.7%)	390(11.9%)

According to above table, 53% have never heard of the policy, 35% have heard but not having a written policy and only 12% has a written policy. Of the senior only 21.4% and of the tertiary 12.2% employees stated that their organization having this kind of written policy document.

Table 4.86: Data security policy

Category	Never heard of this policy	Heard, but not having a written policy	Having a written policy
Primary	286(71.5%)	97(24.3%)	17(4.3%)
Secondary	1057(57.1%)	596(32.2%)	199(10.7%)
Senior	134(31.9%)	199(47.4%)	87(20.7%)
Tertiary	275(46.5%)	249(42.1%)	68(11.5%)
Total	1752(53.6%)	1141(34.95%)	371(11.36%)

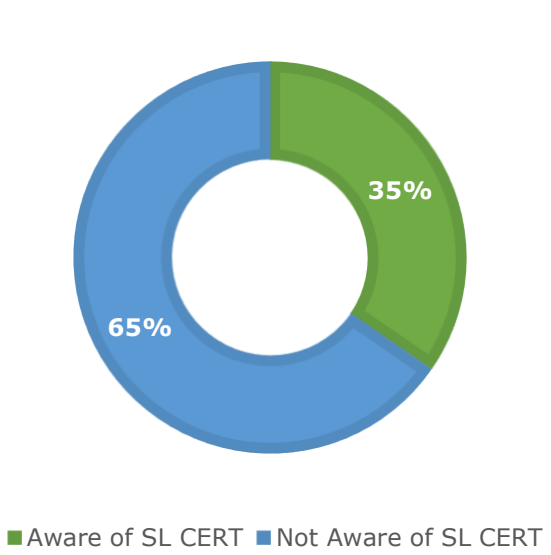
According to table 4.86, 54% have never heard of the policy,35% have heard but not having a written policy and only 11% has a written policy. Of the senior only 20.7% and of the tertiary 11.5% employees stated that their organization having this kind of written policy document.

Table 4.87: Disaster Recovery Policy

Category	Never heard of this policy	Heard, but not having a written policy	Having a written policy
Primary	290(72.5%)	96(24.0%)	14(3.5%)
Secondary	1082(58.4%)	630(34.0%)	140(7.6%)
Senior	150(35.7%)	217(51.7%)	53(12.6%)
Tertiary	286(48.3%)	251(42.4%)	55(9.3%)
Total	1808(55.3%)	1194(36.5%)	262(8.0%)

According to above table 55% have never heard of the policy,37% have heard but not having a written policy and only 8% has a written policy. Of the senior only 12.6% and of the tertiary 9.3% employees stated that their organization having this kind of written policy document.

Figure 4.21: Awareness of SLCERT



In category wise, 79% of primary, 68% of secondary, 53% of senior, and 58% of tertiary employees were not aware of SLCERT. (Based on the decomposition of figure 9.2)

CHAPTER FIVE
SURVEY RESULTS - CYBERSECURITY AWARENESS OF ICT OFFICERS

5.1. General Information

In the survey, ICT officers have identified through their own verbal conformation and infromation did not vlidate with their designation documents. For instance, if he or she stated that their designation as System Administrator, the survey had recorded the data wihtout validation with the respective documents of his or her designation.

Figure 5.1: Distribution of ICT officers

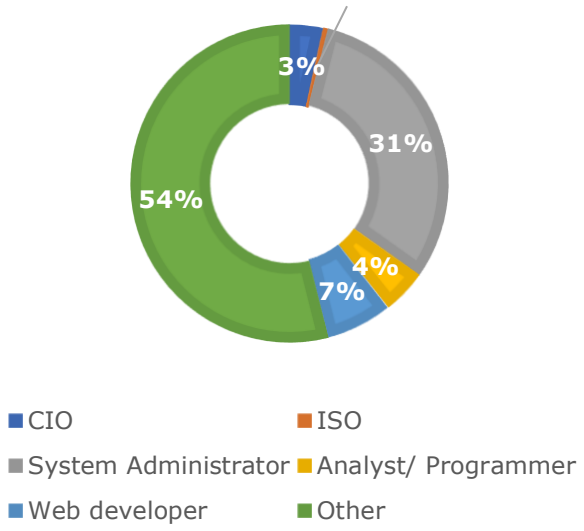


Figure 5.1 shows, total ICT officers were consisting of 8(4%) of Analysists, 6(3%) of CIOs, 01(1%) of ISOs, 55(31%) of System Administrators, 12 (7%) of web developers, and 96(54%) of other officers. Majority of the respondents were fall into the other category, and this category includes officers who were handling both ICT and other organizational work without having a designated job role as an ICT officer in their organizations. Following represent the composition of ICT officers under organizational wise comparison.

Table 5.1: Composition of ICT officers - Organizational wise distribution

Role/ Organization	District Secretariat & Institutes under DS & Divisional Secretariat	Ministries & Institutes under Line Ministry	Provincial Council & Institutes under PC	Special Spending Unit
System Administrator	26(47.3%)	26(47.3%)	1(1.8%)	2(3.6%)
CIO	-	6(100%)	-	-
ISO	1(100%)	-	-	-
Analyst	1(12.5%)	7(87.5%)	-	-
Web developer	6(50.0%)	6(50.0%)	-	-
Other	34 (35.4%)	51(53.1%)	8(8.3%)	3(3.1%)
Total	68(38.2%)	96(53.9%)	9(5.1%)	5(2.8%)

A small number of ICT officers were employed in both Provincial Councils and Special Spending units. This is mainly due to smaller number of organizations available in the

country under those two categories (Provincial Councils and Special spending units) compared with other two categories (Ministries, District and Divisional secretariate).

5.2. Basic Cybersecurity Knowledge

Table 5.2: Critical systems in the organizations

Organization/Critical System	Yes	No	No Awareness on critical systems
District Secretariat & Institutes under DS & Divisional Secretariat	5(7.4%)	28(41.2%)	35(51.5%)
Ministries & Institutes under Line Ministry	28(29.2%)	49(51.0%)	19(19.8%)
Provincial Council & Institutes under PC	-	8(88.9%)	1(11.1%)
Special Spending Unit	2(40.0%	2(40.0%)	1(20.0%)
Total	35(19.7%)	87(48.9%)	56(31.5%)

Majority of Organizations (49%) did not have a Critical System in place while 31% of the respondents were not aware the availability of critical systems in their respective organizations. Based on the calculations, respondents who "Do not Know", are distributed with, 1 (1.8%) of Analysts, 35 (62.5%) of Other Officers, 1 (1.8%) web developer, and 19 (33.9%) of System Administrators. According to the respondents, following Critical Systems were in placed in their organizations.

- Billing and Certificate issues
- Online sales
- Office website
- Fuel and Vehicle Management
- Human Resource Management
- ERP Systems
- Operational Management Systems
- Budget formulation.

Table 5.3: IPS/IDS (Intrusion Prevention Systems OR Intrusion Detection Systems) in the Critical Systems

Organization/IPS OR IDS Systems	Yes	No	No Awareness on IPS/IDS
District Secretariat & Institutes under DS & Divisional Secretariat	1(20.0%)	4(80%)	-
Ministries & Institutes under Line Ministry	14(50.0%)	9(32.1%)	5(17.9%)
Provincial Council & Institutes under PC	-	-	-
Special Spending Unit	1(50%)	-	1(50.0%)
Total	16(45.7%)	13(37.1%)	6(17.1%)

Table 5.3 depicts, majority (37%) of Organizations which had a critical system did not have Intrusion Prevention Systems or Intrusion Detection Systems (IPS/IDS) in their critical systems.

Table 5.4: Awareness on CIA Triad of Information Security

Role/ CIA Awareness	Yes	Some Awareness on CIA	No Awareness on CIA
System Administrator	18(32.7%)	12(21.8%)	25(45.5%)
CIO	4(66.7%)	2(33.3%)	-
ISO	-	1(100%)	-
Analyst	5(62.5%)	2(25.0%)	1(12.5%)
Web developer	10(83.3%)	2(16.7%)	-
Other	31(32.3%)	13(13.5%)	52(54.2%)
Total	68(38.2%)	32(18.0%)	78(43.8%)

Table 5.4 shows majority (44%) of the ICT officers did not have an awareness on CIA Triad of information security. Of the respondents, 18% had a somewhat awareness but they did not have an understanding on same which indicate the lack of knowledge on Information Security indicators. The respondents who indicated they had an awareness on CIA, the level of knowledge was validated with the following statements.

	Agree	Not Agree	Do not Know
Confidentiality means you are protecting your data from getting disclosed.	56(82.4%)	10(14.7%)	2(2.9%)
Integrity means the protection of data from modification by unknown users.	56(82.4%)	11(16.2%)	1(1.5%)
Confidentiality means only authorized users are capable of accessing the information.	50(73.5%)	15(22.1%)	2(4.4%)
Nonrepudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message	34(50.0%)	14(20.6%)	20(29.4%)

Following represent activities to include establishment of institutional framework to secure ICT assets.

Table 5.5: Activities to include establishment of institutional framework to secure ICT assets

Activities	Institute	No Awareness	No	Yes
Policies/Procedures implemented for securing systems	District Secretariat & Institutes under DS & Divisional Secretariat	17 (25.0%)	42 (61.8%)	9 (13.2%)
	Ministries & Institutes under Line Ministry	18 (18.8%)	39 (40.6%)	39 (40.6%)
	Provincial Council & Institutes under PC	3 (33.3%)	6 (66.7%)	-
	Special Spending Unit	2 (40.0%)	1 (20.0%)	2 (40.0%)
Total		**40 (22.5%)**	**88 (49.4%)**	**50 (28.1%)**
Information security unit of the organization	District Secretariat & Institutes under DS & Divisional Secretariat	19 (27.9%)	45 (66.2%)	4 (5.9%)
	Ministries & Institutes under Line Ministry	19 (19.8%)	52 (54.2%)	25 (26.0%)
	Provincial Council & Institutes under PC	3 (33.3%)	5 (55.6%)	1 (11.1%)
	Special Spending Unit	2 (40.0%)	2 (40.0%)	1 (20.0%)
Total		**43 (24.2%)**	**104 (58.4%)**	**31 (17.4%)**
Tasks/roles assigned to officers to secure systems	District Secretariat & Institutes under DS & Divisional Secretariat	21 (30.9%)	38 (55.9%)	9 (13.2%)
	Ministries & Institutes under Line Ministry	24 (25.0%)	44 (45.8%)	28 (29.2%)
	Provincial Council & Institutes under PC	3 (33.3%)	6 (66.7%)	-
	Special Spending Unit	3 (60.0%)	1 (20.0%)	1 (20.0%)
Total		**51 (28.7%)**	**89 (50.0%)**	**38 (21.3%)**
Incidents reporting structures	District Secretariat & Institutes under DS & Divisional Secretariat	19 (27.9%)	37 (54.4%)	12 (17.6%)
	Ministries & Institutes under Line Ministry	27 (28.1%)	44 (45.8%)	25 (26.0%)
	Provincial Council & Institutes under PC	3 (33.3%)	5 (55.6%)	1 (11.1%)
	Special Spending Unit	2 (40.0%)	2 (40.0%)	1 (20.0%)
Total		**51 (28.7%)**	**88 (49.4%)**	**39 (21.9%)**

Among organizations, only 22% had implemented one or more activities while 52% of them had not implemented any of activities mentioned in above table. Of the respondents, 26% had no awareness on whether his or her organization had implemented these activities or not.

5.3. Asset Classification

Following figure represent importance of securing the information assets as per ICT officers' viewpoint.

Figure 5.2: Securing information Assets

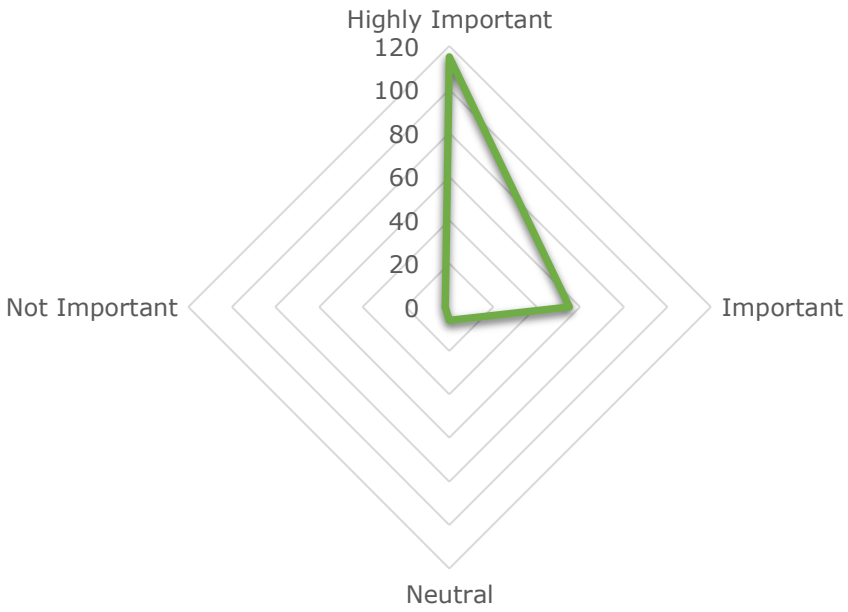


Figure 5.2 depicts, majority (65%) stated securing information assets are highly important.

Table 5.6: Awareness on asset classification

Role/ CIA Awareness	Yes	Some awareness on asset classifications	No awareness on asset classification
System Administrator	11(20.0%)	26(47.3%)	18(32.7%)
CIO	4(66.7%)	1(16.7%)	1(16.7%)
ISO	-	1(100%)	-
Analyst	5(62.5%)	2(25.0%)	1(12.5%)
Web developer	6(50.0%)	4(33.3%)	2(16.7%)
Other	20(20.8%)	39(40.6%)	37(38.5%)
Total	46(25.8%)	73(41.0%)	59(33.1%)

This shows, 33% did not had an awareness on asset classification while 41% had a somewhat awareness but they did not have a technical knowledge on the asset classification.

Table 5.7: Awareness on information asset inventory

Role/ CIA Awareness	Yes	Some awareness on information asset inventory	No awareness on information asset inventory
System Administrator	16(29.1%)	12(21.8%)	27(49.1%)
CIO	3(50.0%)	3(50.0%)	-
ISO	-	1(100%)	-
Analyst	4(50.0%)	3(37.5%)	1(12.5%)
Web developer	4(33.3%)	4(33.3%)	4(33.3%)
Other	19(19.8%)	33(32.4%)	44(45.4%)
Total	46(25.8%)	56(31.5%)	76(42.7%)

This shows, 42% did not had an awareness on information asset inventory while 31% had a somewhat awareness but they did not have a technical knowledge on information asset inventory. Following table represent the involvement in developing or mapping information asset inventory of the ICT officers who had a somewhat knowledge on information asset inventory.

Table 5.8: Developing or mapping asset inventory

Role/ CIA Awareness	Yes	No
System Administrator	3(18.8%)	13(81.3%)
CIO	1(33.3%)	2(66.7%)
ISO	-	1(100%)
Analyst	3(75.0%)	1(25.0%)
Web developer	2(50.0%)	2(50.0%)
Other	8(42.1%)	11(58.9%)
Total	17(37.0%)	29(63.0%)

These results illustrate majority (63%) of ICT officers who had somewhat knowledge on asset inventories were not involving developing or mapping process for their organizations.

Following represent viewpoints of ICT officers regarding external stakeholder relationships.

	Agree	Agree to some extent	Not Agree
It is essential to defining the types of information which could be given access to different types of external stakeholders	105 (59.0%)	55 (30.9%)	18 (10.1%)
It is essential to have information sharing policy/ agreements with different external stakeholders	121 (68.0%)	46 (25.8%)	11 (6.2%)

Table 5.9: Data classification mechanisms

Institute	Yes	No	No awareness on data classification mechanisms
District Secretariat & Institutes under DS & Divisional Secretariat	8(11.8%)	26(38.2%)	34(50.0%)
Ministries & Institutes under Line Ministry	25(26.0%)	40(41.7%)	31(32.3%)
Provincial Council & Institutes under PC	1(11.1%)	7(77.8%)	1(11.1%)
Special Spending Unit	1(20.0%)	2(40.0%)	2(40.0%)
Total	35(19.7%)	75(42.1%)	68(38.2%)

Table 5.9 depicts, majority of organizations (42%) did not have a data classification mechanism. Of the respondents in the organizations, 38% did had no awareness on their organizational data classifications.

Following table represent the awareness of ICT officers about the gravity of the data set handling in different parts of the organization. This analysis was conducted in role-wise distribution to capture the awareness under each category of ICT officer.

Table 5.10: Awareness on data handling in different parts of the organization

Role/ CIA Awareness	Yes	No
System Administrator	14(25.5%)	41(74.5%)
CIO	4(66.7%)	2(33.3%)
ISO	-	1(100%)
Analyst	3(37.5%)	5(62.5%)
Web developer	7(58.3%)	5(42.7%)
Other	18(18.8%)	78(82.0%)
Total	46(25.8%)	132(74.2%)

Majority (74.2%) had no awareness on the gravity of data handling in different parts of their organizations.

Table 5.11: Sensitive data classification

Role/ CIA Awareness	Yes	Some awareness on data classification	No awareness on sensitive data
System Administrator	18(32.7%)	13(23.6%)	24(43.6%)
CIO	5(83.3%)	-	1(16.7%)
ISO	-	1(100%)	-
Analyst	2(25.0%)	3(37.5%)	3(37.5%)
Web developer	7(58.3%)	3(25.0%)	2(16.7%)
Other	21(21.9%)	20(20.8%)	55(57.3%)
Total	53(29.8%)	40(22.5%)	85 (47.8%)

This shows, majority (48%) did not have awareness on classify data as per sensitive data needs while 22% had somewhat awareness but they had no knowledge on classify the data as sensitive data requirements.

5.4. ICT policies and procedures

Table 5.12: Separate IT related rules/regulations OR policies

Institute	Yes	No Separate IT rules/ regulations OR policies	No Awareness on Separate IT rules/ regulations OR policies
District Secretariat & Institutes under DS & Divisional Secretariat	14(20.6%)	39(57.4%)	15(22.1%)
Ministries & Institutes under Line Ministry	31(32.3%)	47(49.0%)	18(18.8%)
Provincial Council & Institutes under PC	1(11.1%)	8(88.9%)	-
Special Spending Unit	2(40.0%)	2(40.0%)	1(20.0%)
Total	48(27.0%)	96(53.9%)	34(19.1%)

This illustrates, majority of organizations (54%) did not have IT related rules or regulations or policies. In addition, 19% of respondents in respective organizations were not aware of IT related procedures (rules or regulations) and policies. Following table represent the distribution of stakeholders developed organizational IT rules/regulations OR polices for the organizations.

Table 5.13: Stakeholders involved in developing IT related rules/regulations OR policies

Institute	External	Internal	No awareness on who involved
District Secretariat & Institutes under DS & Divisional Secretariat	4(28.6%)	4(28.6%)	6(42.9%)
Ministries & Institutes under Line Ministry	5	25	-
Provincial Council & Institutes under PC	-	-	1 (100%)
Special Spending Unit	1(50%)	1(50%)	-
Total	10(20.8%)	30(62.5%)	7(14.6%)

This depicts, higher share of internal stakeholders was involved (62%) in developing IT related rules or regulations, and policies in the organizations. Following represent the role of contribution of ICT officers in developing IT related rules or regulations, and policies.

Table 5.14: Involvement in developing IT related rules or regulations, and policies

Role/ CIA Awareness	Involved in developing IT related rules or regulations, and policies	Not involved
System Administrator	11(68.7%)	4(31.25%)
CIO	1(50%)	1(50%)
ISO	-	-
Analyst	2(100%)	-
Web developer	-	4(100%)
Other	9(42.8%)	13(57.3%)
Total	23 (51.1%)	22(48.9%)

Table 5.14 shows, marginally higher (51%) of respondents were involved in developing rules or regulations, and polices in their organizations.

Table 5.15: Awareness of security policy

Role/ CIA Awareness	Yes	Some awareness on security policy	No awareness on security policy
System Administrator	5(9.1%)	29(52.7%)	21(38.2%)
CIO	-	4(66.7%)	2(33.3%)
ISO	-	-	1(100%)
Analyst	1(12.5%)	4(50.0%)	3(37.5%)
Web developer	3(25.0%)	5(41.7%)	4(33.3%)
Other	11(11.5%)	31(32.3%)	54(56.3%)
Total	20(11.2%)	73(41.0%)	85(47.8%)

Table 5.15 reveals, majority (48%) did not have any awareness on information security policy while 41% had an awareness but did not sign or read any information security related policy provided by the organization.

Table 5.16: Awareness on access control policy

Role/ CIA Awareness	Yes	No	No Awareness on access control policy
System Administrator	16(29.1%)	16(29.1%)	23(41.8%)
CIO	4(66.7%)	2(33.3%)	-
ISO	1(100%)	-	-
Analyst	3(37.5%)	3(37.5%)	2(25.0%)
Web developer	3(25.0%)	5(41.7%)	4(33.3%)
Other	20(20.8%)	30(31.3%)	46(47.9%)
Total	47(26.4%)	56(31.5%)	75(42.1%)

Majority (42%) had no awareness on access control policy while 31% had somewhat awareness but they did not have the knowledge on the purpose of access control policy. Following represent the degree of awareness of ICT officers on password or user accounts policies in their organizations.

	Agree	Disagree	No Awareness
Having administrator access for general users	32(18.0%)	118(66.3%)	28(15.7%)
Enabling computers to prompt change passwords frequently (Give timing)	108(60.7%)	28(15.7%)	42(23.6%)
Sharing administrator password for urgent matters	26(14.6%)	120(67.4%)	32(18.0%)
Use of combination of characters for passwords	129(72.5%)	12(6.7%)	37(20.8%)
Restricting privilege users to access log files (System logs or Audit trails)	110(61.8%)	18(10.1%)	50(28.1%)
Share a password between group of users	31(17.4%)	112(62.9%)	35(19.7%)
Creating user accounts for temporary/ third party users	85(47.8%)	53(29.8%)	40(22.5%)
Block the user access when employee transferred or retired	129(72.5%)	10(5.6%)	39(21.9%)
When creating a new account for employees, standard pattern of password is sent over an Email.	91(51.1%)	44(24.7%)	43(24.2%)

5.5. Storage and Media Policy

Following figure represent the ICT officer's perception on permanently disposing data storage media

Figure 5.3: Disposing data storage media

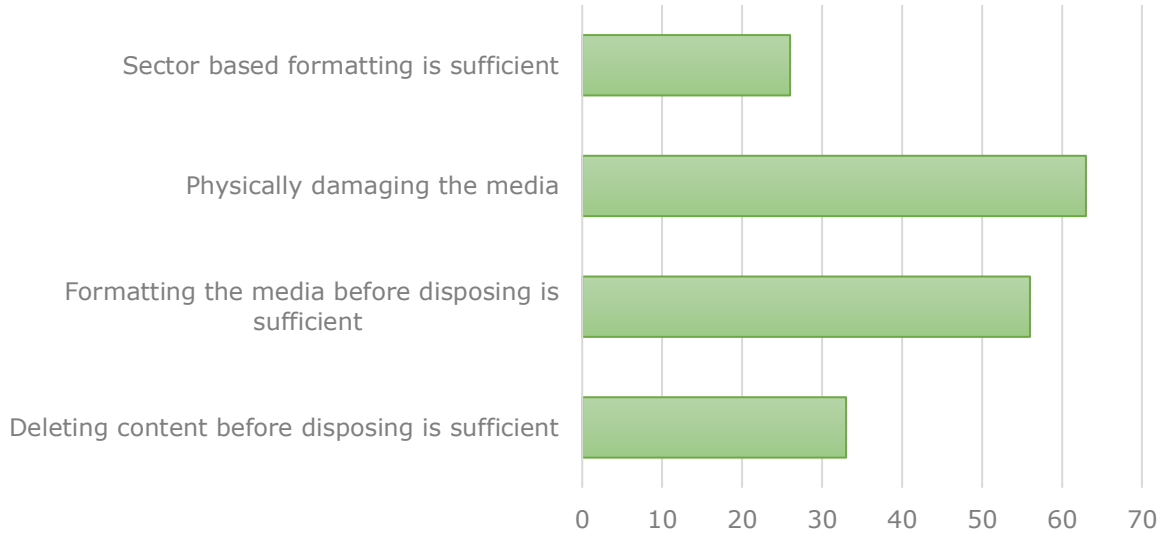


Figure 5.3 depicts, majority 35% stated physically damaging the media is the best option to dispose the storage media while 31% were in favor of format the media before disposing. Only 14% indicated sector-based formatting is adequate.

Table 5.17: Formatting a storage media that need to be disposed

Role/ CIA Awareness	Yes	No
System Administrator	28(50.9%)	27(49.1%)
CIO	5(83.3%)	1(16.7%)
ISO	1(100%)	-
Analyst	5(37.5%)	3(62.5%)
Web developer	11(91.7%)	1(8.3%)
Other	49(51.0%)	47(49.0%)
Total	99(55.6%)	79(44.4%)

This shows, 44% of ICT officers were not aware of formatting a storage media that required to be disposed.

Table 5.18: Sector based formatting

Role/ CIA Awareness	Yes	No
System Administrator	17(30.9%)	38(69.1%)
CIO	5(83.3%)	1(16.7%)
ISO	-	1(100%)
Analyst	4(50.0%)	4(50.0%)
Web developer	7(58.3%)	5(41.7%)
Other	27(28.1%)	69(71.9%)
Total	60(33.7%)	118(66.3%)

Table 5.18 shows, majority (66%) had no awareness on performing a sector-based formatting.

5.6. Physical access control

Table 5.19: CCTV Usage

Institute	Yes	No	Do not know
District Secretariat & Institutes under DS & Divisional Secretariat	20(29.4%)	34(50.0%)	14(20.6%)
Ministries & Institutes under Line Ministry	70(72.9%)	21(21.9%)	5(5.2%)
Provincial Council & Institutes under PC	7(77.8%)	2(22.2%)	-
Special Spending Unit	2(40.0%)	1(20.0%)	2(40.0%)
Total	99(55.6%)	58(32.6%)	21(11.8%)

Table 5.19 Shows that 11.8% do not know the CCTV usage.

Table 5.20: Managing CCTV

Role/ CIA Awareness	Yes	No	No awareness on CCTV
System Administrator	18(32.7%)	19(34.5%)	18(32.7%)
CIO	3(50.0%)	2(33.3%)	1(16.7%)
ISO	-	1(100%)	-
Analyst	3(37.5%)	5(62.5%)	-
Web developer	4(33.3%)	7(58.3%)	1(8.3%)
Other	22(22.9%)	62(64.6%)	12(12.5%)
Total	50(28.1%)	96(53.9%)	32(18.0%)

This depicts, majority (55%) of organizations were having a CCTV, while majority (54%) had somewhat awareness on CCTV, although, they did not know how to manage a CCTV while 18% of respondents did not have an awareness regarding managing a CCTV.

Table 5.21: Security practices of CCTV data

Role/ CIA Awareness	Yes	No	No awareness on practices of CCTV
System Administrator	15(27.3%)	22(40.0%)	18(32.7%)
CIO	3(50.0%)	2(33.3%)	1(16.7%)
ISO	-	1(100%)	-
Analyst	4(50%)	4(50%)	-
Web developer	4(33.3%)	6(50.0%)	2(16.7%)
Other	13(13.5%)	69(71.9%)	14(14.6%)
Total	39(21.9%)	104(58.4%)	35(19.7%)

Table 5.21 shows, majority (58%) of respondents had somewhat awareness but no knowledge on the security practices of handling CCTV data. Of the respondents, 18% had no awareness regarding these practices.

5.7. Network and Application security

Table 5.22: Computer network

Institute	Yes	No	Do not Know
District Secretariat & Institutes under DS & Divisional Secretariat	56(82.4%)	12(18.1%)	5(7.4%)
Ministries & Institutes under Line Ministry	85(88.5%)	11(11.5%)	2(2.1%)
Provincial Council & Institutes under PC	5(55.6%)	4(44.4%)	-
Special Spending Unit	4(80.0%)	-	1(20.0%)
Total	150(84.3%)	28(15.7%)	8(4.5%)

Table 5.23: Awareness on organizational architecture

Role/ CIA Awareness	Yes	Some awareness on organizational architecture	Not aware of organizational architecture
System Administrator	39(70.9%)	4(7.3%)	12(21.8%)
CIO	6(100%)	-	-
ISO	1(100%)	-	-
Analyst	5(62.5%)	1(12.5%)	2(25.0%)
Web developer	5(41.7%)	5(41.7%)	2(16.7%)
Other	47(49.0%)	26(27.1%)	23(24.0%)
Total	103(57.9%)	36(20.2%)	39(21.9%)

Among organizations, 84% had computer networks. Majority (58%) stated that they were aware of their own architectures. Although, 22% of respondents had no awareness regarding their organizational architecture while 20% had somewhat awareness but they did not have knowledge on same.

Table 5.24: VPN Connections

Institute	Yes	No	Do not know
District Secretariat & Institutes under DS & Divisional Secretariat	3(4.4%)	36(52.9%)	29(42.6%)
Ministries & Institutes under Line Ministry	24(25.0%)	55(57.7%)	17(17.7%)
Provincial Council & Institutes under PC	1(11.1%)	4(44.4%)	4(44.4%)
Special Spending Unit	1(20.0%)	3(60.0%)	1(20.0%)
Total	29(16.3%)	98(55.1%)	51(28.7%)

Table 5.25: Awareness of configuring VPNs

Role/ CIA Awareness	Yes	Some awareness on configuring VPNs	No awareness on configuring VPNs
System Administrator	17(30.9%)	21(38.2%)	17(30.9%)
CIO	4(66.7%)	2(33.3%)	-
ISO	-	-	1(100%)
Analyst	3(37.5%)	4(50.0%)	1(12.5%)
Web developer	4(33.3%)	5(41.7%)	3(25.0%)
Other	19(19.8%)	42(43.8%)	35(36.5%)
Total	47(26.4%)	74(41.6%)	57(32.0%)

Table 5.25 depicts, 55% of organizations did not have VPN connections to the users while 29% of ICT officers did not have an awareness on VPN users in their respective organizations. Although, majority (42%) did have some awareness but no knowledge relating to configuring VPNs. Among ICT officers, 32% did not have awareness on configuring VPNs.

Table 5.26: VLANs

Institute	Yes	No	No awareness on VLANs
District Secretariat & Institutes under DS & Divisional Secretariat	1(1.5%)	36(52.9%)	31(45.6%)
Ministries & Institutes under Line Ministry	25(26.0%)	54(56.3%)	17(17.7%)
Provincial Council & Institutes under PC	-	7(77.8%)	2(22.2%)
Special Spending Unit	2(40.0%)	2(40.0%)	1(20.0%)
Total	28(15.7%)	99(55.6%)	51(28.7%)

This illustrates, majority (56%) did not have VLANs in their organizations while 29% of ICT officers in their respective organizations had no awareness on VLANs. Following represent the awareness on firewall usage for the organizations which had VLANs.

Table 5.27: Awareness on firewall system

Institute	Yes	No	No Awareness on Firewall system
District Secretariat & Institutes under DS & Divisional Secretariat	-	1(100%)	-
Ministries & Institutes under Line Ministry	20(80.0%)	4(16.0%)	1(4.0%)
Provincial Council & Institutes under PC	-	-	-
Special Spending Unit	2(100%)	-	-
Total	22(78.6%)	5(17.9%)	1(3.6%)

Table 5.27 Majority of organizations (79%) which had VLANs were running firewall systems

Table 5.28: Configuring firewall rules

Role/ CIA Awareness	Yes	Some awareness on configuring firewall rules	No awareness on configuring firewall rules
System Administrator	6(66.7%)	3(33.3%)	-
CIO	3(100%)	-	-
ISO	-	-	-
Analyst	2(50.0%)	2(50.0%)	-
Web developer			
Other	3(33.3%)	5(55.6%)	1(11.1%)
Total	15(53.6%)	12(42.9%)	1(3.6%)

Table 5.28 shows, 43% had somewhat awareness but they did not had knowledge on configuring firewall rules. This distribution was obtained only from the organizations which had VLANs.

Table 5.29: Auditing firewall rules

Role/ CIA Awareness	Yes	Some awareness on auditing firewall rules	No awareness on auditing firewall rules
System Administrator	5(55.6%)	4(44.4%)	-
CIO	3(100%)	-	-
ISO	-	-	-
Analyst	1(25.0%)	3(75.0%)	-
Web developer	-	3(100%)	-
Other	2(22.2%)	6(66.7%)	1(11.1%)
Total	11(39.3%)	16(57.1%)	1(3.6%)

Table 5.29 shows, 57% has somewhat awareness on auditing firewall rules, but they had no knowledge on process of conducting an audit. This distribution was obtained only from

the organizations which had VLANs. Following represent the ICT officer's position on conducting official operational tasks.

	Yes	No	Do not know
I always encrypt sensitive data when sending via external Email	51(28.7%)	89(50.0%)	38(21.3%)
I know how my device data should be encrypted	82(46.1%)	56(31.5%)	40(22.5%)
My sensitive/critical data is backed up on a routine basis	87(48.9%)	49(27.5%)	42(23.6%)
Recovery is tested periodically	53(29.8%)	80(44.9%)	45(25.3%)
I know my responsibilities on my Department's Business Continuity Plans.	110(61.8%)	26(14.6%)	42(23.6%)
I am aware of using security measures when using my personal computing devices.	115(64.6%)	21(11.8%)	42(23.6%)

Table 5.30: Experience in server administration

Role/ CIA Awareness	Yes	Some experience on server administration	No experience on server administration
System Administrator	24(43.6%)	19(34.5%)	12(21.8%)
CIO	5(83.3%)	1(16.7%)	-
ISO	1(100%)	-	-
Analyst	2(25.0%)	6(75.0%)	-
Web developer	5(41.7%)	7(58.3%)	-
Other	17(17.7%)	51(53.1%)	28(29.2%)
Total	54(30.4%)	84(47.2%)	40(22.5%)

This depicts, 47% had no experience in server administration while 22% had some awareness but had no knowledge on server administration. Following represent the tasks perform by the ICT officers who had experience in server administration. And, it shows all ICT officers had some experience on patch updating, setting privileges, activity monitoring, and server hardening.

Table 5.31: Patch updating

Role/ CIA Awareness	Yes	No	Do not know
System Administrator	10(41.6%)	12(50.0%)	2 (8.4%)
CIO	5(100%)	-	-
ISO	-	1(100%)	-
Analyst	1(50%)	1(50%)	-
Web developer	4(80.0%)	1(20.0%)	-
Other	11(64.7%)	5(29.4%)	1(5.9%)
Total	31(57.4%)	20(37.0)	3(1.9%)

Table 5.32: Setting privileges

Role/ CIA Awareness	Yes	No	Do not know
System Administrator	14(58.3%)	10(41.7%)	-
CIO	5(100%)	-	-
ISO	-	1(100%)	-
Analyst	1(50.0%)	1(50.0%)	-
Web developer	5(100%)	-	-
Other	10(58.8%)	6(35.3%)	1(5.9%)
Total	35(64.8%)	18(33.3%)	1(1.9%)

Table 5.33: Activity monitoring

Role/ CIA Awareness	Yes	No	Do not know
System Administrator	20(83.3%)	3(12.5%)	1(4.2%)
CIO	5(100%)	-	-
ISO	1(100%)	-	-
Analyst	2(100%)	-	-
Web developer	5(100%)	-	-
Other	12(70.6%)	5(29.4%)	-
Total	45(83.3%)	8(14.8%)	1(1.9%)

Table 5.34: Server hardening

Role/ CIA Awareness	Yes	No	Do not know
System Administrator	10(41.7%)	10(41.7%)	4(16.6%)
CIO	3(60.0%)	1(20.0%)	1(20.0%)
ISO	-	1(100%)	-
Analyst	1(50%)	1(50%)	-
Web developer	2(40.0%)	3(60.0%)	-
Other	6(35.3%)	9(52.9%)	2(11.8%)
Total	22(40.7%)	25(46.3%)	7(12.9%)

Table 5.35: Accessibility to the organizational servers

Institute	Administrator only	Anyone who needs the service	Employees only	IT staff only	Management only	Other outside parties
District Secretariat & Institutes under DS & Divisional Secretariat	16 (23.5%)	3 (4.4%)	5 (7.4%)	22 (32.4%)	8 (11.8%)	14 (20.6%)
Ministries & Institutes under Line Ministry	27 (28.1%)	3 (3.1%)	-	29 (30.2%)	7 (7.3%)	30 (31.3%)
Provincial Council & Institutes under PC	3 (33.3%)	2 (22.2%)	-	3 (60.0%)	1 (11.1%)	-
Special Spending Unit	1	-	-	3 (60.0%)	-	1 (20.0%)
Total	47 (26.4%)	8 (4.5%)	5 (2.8%)	57 (32.0%)	16 (9.0%)	45 (25.3%)

Table 5.35 shows, outside parties had an accessibility to organizations servers, in 25% of organizations being interviewed.

Table 5.36: Awareness on administrate organizational servers

Role/ CIA Awareness	Yes	Some awareness on administrating organizational servers	No awareness on administrating organizational servers
System Administrator	12(21.8%)	24(43.6%)	19(34.5%)
CIO	5(83.3%)	1(16.7%)	-
ISO	-	1(100%)	-
Analyst	3(37.5%)	4(50.0%)	1(12.5%)
Web developer	3(25.0%)	8(66.7%)	1(8.3%)
Other	11(11.5%)	49(51.0%)	36(37.5%)
Total	34(19.1%)	87(48.9%)	57(32.0%)

Table 5.36 depicts, 49% of respondents had somewhat awareness on administration of the organizational servers, although they did not have knowledge on organizational server administration.

Table 5.37: Managing organizational website

Role/ CIA Awareness	Yes	No
System Administrator	20(36.4%)	9(63.6%)
CIO	5(83.3%)	1(16.7%)
ISO	-	1(100%)
Analyst	5(62.5%)	3(37.5%)
Web developer	11(91.7%)	1(8.3%)
Other	45(46.9%)	51(53.1%)
Total	86(48.3%)	92(51.7%)

Table 5.37 illustrate 52% of respondents did not have a knowledge to manage their organizational website. Following represent the operational activities of ICT officers who had knowledge to manage their organization website.

Table 5.38: Managing website administration

Role/ CIA Awareness	Yes	No	No awareness on website administration
System Administrator	8(40.0%)	9(45.0%)	3(15.0%)
CIO	2(40.0%)	3(60.0%)	-
ISO	-	-	-
Analyst	3(60.0%)	2(40.0%)	-
Web developer	9(81.8%)	2(18.2%)	-
Other	15(33.3%)	26(58.4%)	4(8.9%)
Total	37(43.0%)	39(48.8%)	7(8.1%)

This illustrate, majority (49%) was not enrolled on managing website administrations in their organizations. Following represent the security patches updates on the websites of each organization.

Table 5.39: Security patches for the website

Institute	Yes	No	No awareness on security patches updates	Not Managing the Website
District Secretariat & Institutes under DS & Divisional Secretariat	2(2.9%)	6(8.8%)	23(33.8%)	37(54.4%)
Ministries & Institutes under Line Ministry	20(20.8%)	11(11.5%)	20(20.8%)	45(46.9%)
Provincial Council & Institutes under PC	-	1(11.1%)	-	8(88.9%)
Special Spending Unit	2(40.0%)	-	1(20.0%)	2(40.0%)
Total	24(13.5%)	18(10.1%)	44(24.7%)	92(51.7%)

This shows, majority (25%) had no awareness on their organizations on the security patches updates in their respective organizations. Only 13% of the organizations had run the updates.

Table 5.40: SSL Certificate

Institute	Yes	No	No awareness on SSL certificate	Not Managing the website
District Secretariat & Institutes under DS & Divisional Secretariat	4(5.9%)	4(5.9%)	23(33.8%)	37(54.4%)
Ministries & Institutes under Line Ministry	18(18.8%)	11(11.5%)	22(22.9%)	45(46.9%)
Provincial Council & Institutes under PC		1(11.1%)	-	8(88.9%)
Special Spending Unit	2(40.0%)	-	1(20.0%)	2(40.0%)
Total	24(13.5%)	16(9.0%)	46(28.8%)	92(51.7%)

Table 5.40 depicts, only 13% of the organizations had obtained the SSL certificate for their websites. Further, 29% of ICT officers in respective organizations were not aware of the SSL certificate.

Table 5.41: Security assessment

Institute	Yes	No	No awareness on security assessment
District Secretariat & Institutes under DS & Divisional Secretariat	2(2.9%)	18(26.5%)	48(70.6%)
Ministries & Institutes under Line Ministry	33(34.4%)	21(21.9%)	42(43.8%)
Provincial Council & Institutes under PC	2(22.2%)	6(66.7%)	1(11.1%)
Special Spending Unit	1(33.3%)	-	2(66.7%)
Total	39(21.9%)	46(25.8%)	93(52.2%)

This reflects the fact, only fewer organizations (22%) had undergone a security assessment. Of the respondents interviewed, 52% of ICT officers had no awareness on security assessments in their organizations. Following table represent, the point of time the security assessment was conducted for the websites of the organizations which had undergone this assessment.

Table 5.42: Time of the security assessment

Institute	After launch	Before launch	Do not know
District Secretariat & Institutes under DS & Divisional Secretariat	1(50.0%)	1(50.0%)	-
Ministries & Institutes under Line Ministry	14(42.4%)	14(42.4%)	5(15.2%)
Provincial Council & Institutes under PC	-	2(100%)	-
Special Spending Unit	-	2(100%)	-
Total	15(38.5%)	19(48.7%)	5(12.8%)

This shows, majority of the organization websites (49%) had conducted security assessment before the launch. SLCERT had conducted security assessment of 15 of the organizations that was interviewed under this survey.

Table 5.43: Awareness on administration of email server

Role/ CIA Awareness	Yes	No	No awareness on administration of email server
System Administrator	26(47.3%)	11(20.0%)	18(32.7%)
CIO	3(50.0%)	3(50.0%)	-
ISO	1(100%)	-	
Analyst	5(62.5%)	3(37.5%)	-
Web developer	4(33.3%)	8(66.7%)	-
Other	26(27.1%)	46(47.9%)	24 (25.0%)
Total	65(36.5%)	71(39.9%)	42(23.6%)

Table 5.43 illustrate, majority (40%) of the respondents had somewhat awareness but no knowledge on the administration of the Email server while 24% had no awareness on email server administration.

Table 5.44: Spam filtering

Role/ CIA Awareness	Yes	No	No Awareness on Spam Filtering
System Administrator	25(45.5%)	11(20.0%)	19(34.5%)
CIO	4(66.7%)	2(33.3%)	-
ISO	1(100%)	-	-
Analyst	4(50%)	4(50%)	
Web developer	6(50.0%)	6(50.0%)	-
Other	25(26.0%)	47(49.0%)	24(25.0%)
Total	65(36.5%)	70(39.3%)	43(24.2%)

This shows, 40% of the respondents had no knowledge on setting up a spam filtering while 24% had no awareness on same process.

Table 5.45: Measure against cyberattacks

Institute	Taken measures	Not taken measures
District Secretariat & Institutes under DS & Divisional Secretariat	50(73.5%)	18(26.5%)
Ministries & Institutes under Line Ministry	62(64.6%)	34(35.4%)
Provincial Council & Institutes under PC	8(88.9%)	1(11.1%)
Special Spending Unit	3(60.0%)	2(40.0%)
Total	123(69.1%)	55(30.9%)

Table 5.45 depicts, majority organizations (69%) had taken measures to harden (reducing the attack surface) the computers under the purview against cyber-attacks. Majority of actions were based on following activities.

- Using virus guards
- Password updates
- Building firewall system

Table 5.46: Role base access control

Institute	Yes	No	No Awareness on role-based control
District Secretariat & Institutes under DS & Divisional Secretariat	15(22.1%)	14(20.6%)	39(57.4%)
Ministries & Institutes under Line Ministry	37(38.5%)	25(26.0%)	34(35.4%)
Provincial Council & Institutes under PC	4(44.4%)	4(44.4%)	1(11.1%)
Special Spending Unit	2(40.0%)	2(40.0%)	1(20.0%)
Total	58(32.6%)	45(25.3%)	75(42.1%)

Table 5.46 depicts, majority of respondents (42%) in their respective organizations had no awareness on role-based access control while 25% of organization did not have a role-based access control system.

Table 5.47: Security logs

Institute	Yes	No	No Awareness on security logs
District Secretariat & Institutes under DS & Divisional Secretariat	18(26.5%)	13(19.1%)	37(54.4%)
Ministries & Institutes under Line Ministry	39(40.6%)	23(24.0%)	34(35.4%)
Provincial Council & Institutes under PC	3(33.3%)	5(55.6%)	1(11.1%)
Special Spending Unit	3(60.0%)	2(40.0%)	-
Total	63(35.4%)	43(24.2%)	72(40.4%)

Table 5.47 shows, majority (40%) of the ICT officers in their organizations were not aware of security logs in the organizations while 24% of organizations had not enabled their security logs.

Table 5.48: Monitoring security logs

Role/ CIA Awareness	Yes	No	No awareness on monitoring security logs
System Administrator	25(45.5%)	9(16.4%)	21(38.2%)
CIO	6(100%)	-	-
ISO	1(100%)	-	-
Analyst	2(25.0%)	5(62.5%)	1(12.5%)
Web developer	4(33.3%)	5(41.7%)	3(25.0%)
Other	20(20.8%)	29(30.2%)	47(49.0%)
Total	58(32.6%)	48(27.0%)	72 (40.4%)

This reflect the fact, majority (40%) had no awareness on monitoring the security logs while 27% were not monitoring the logs.

Table 5.49: Information security assessment

Institute	Yes	No	Do not know
District Secretariat & Institutes under DS & Divisional Secretariat	5(7.4%)	24(35.3%)	39(57.4%)
Ministries & Institutes under Line Ministry	18(18.8%)	48(50.0%)	30(31.3%)
Provincial Council & Institutes under PC	2(22.2%)	6(66.7%)	1(11.1%)
Special Spending Unit	1(20.0%)	3(60.0%)	1(20.0%)
Total	26(14.6%)	81(45.5%)	71(39.9%)

Table 5.49 shows, 45% of the organization have not conducted an information security assessment for its information systems. Also, 40% of ICT officers in their respective organizations were not aware on undergoing a security assessment. Following figure 5.4 represent the importance on conducting an information security assessment.

Figure 5.4: Importance of conducting information security assessment

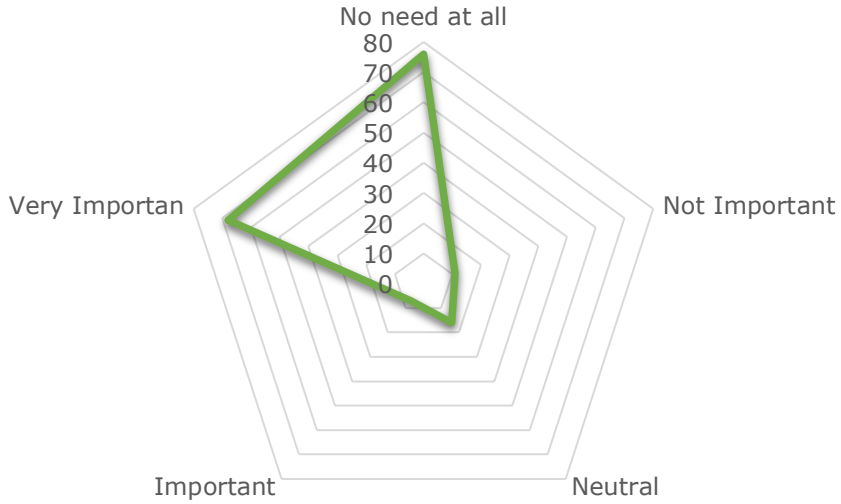


Figure 5.4 illustrate the standpoint of the ICT officers were in two extremes. Majority 43% stated no need to conduct an information security assessment while 38% was stated it is very important.

Figure 5.5: Importance of vulnerability assessment OR penetration testing

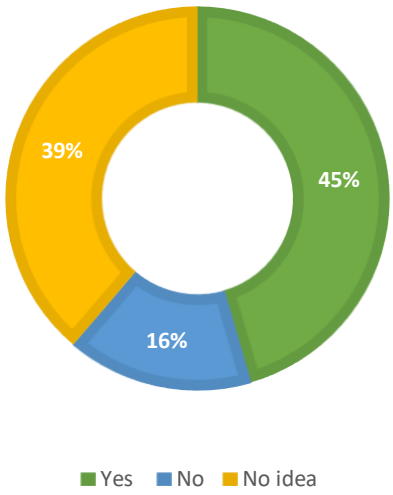


Figure 5.5 shows, 45% indicated the importance of conducting a vulnerability assessment OR penetration testing. Although, 39% of ICT officers had no awerness on vulnerability assessment or penetrating testing.

5.8. Disaster Recovery

Table 5.50: Disaster recovery plan

Institute	Yes	No
District Secretariat & Institutes under DS & Divisional Secretariat	1(1.5%)	67(98.5%)
Ministries & Institutes under Line Ministry	20(20.8%)	76(79.3%)
Provincial Council & Institutes under PC	-	9(100%)
Special Spending Unit	2(40.0%)	3(60.0%)
Total	23(12.9%)	155(87.1%)

Table 5.51: Preparation of disaster recovery plan

Role/ CIA Awareness	Yes	No	No Awareness on preparation a disaster recovery plan
System Administrator	16(29.1%)	25(45.5%)	14(25.5%)
CIO	-	2(33.3%)	4(66.7%)
ISO	1(100%)	-	-
Analyst	-	4	4
Web developer	1(8.3%)	7(58.3%)	4(33.3%)
Other	44(45.8%)	35(36.5%)	17(17.7%)
Total	62(34.8%)	73(41.0%)	43(24.2%)

Table 5.50 shows, majority of organizations (87%) had no disaster recovery plan, while table 5.51 depicts, 41% of ICT officers had somewhat awareness but no knowledge to prepare a disaster recovery plan while 24% had no awareness on process of disaster recovery plan. Following represent few validations checks on ICT officers regarding their awareness on key factors of disaster recovery.

	Agree	Not Agree	Do not know
The DR site shall be tested periodically to ensure it is ready to operate at any time if a disaster occurs	92(51.7%)	4(2.2%)	82(46.1%)
DR site can be established in-house at the same premises with the operational site	36(20.2%)	54(30.3%)	88(49.4%)
Employee awareness	94(52.8%)	8(4.5%)	76(42.7%)
Business impact analysis and a risk assessment shall be carried out before finalizing the DR plan	80(44.9%)	6(3.4%)	92(51.7%)
Updating the DR plan is important	99(55.6%)	2(1.1%)	77(43.3%)

Table 5.52: Usage of Disaster Recovery site

Institute	Yes	No	No Awareness on usage of disaster recovery site
District Secretariat & Institutes under DS & Divisional Secretariat	-	38(55.9%)	30(44.1%)
Ministries & Institutes under Line Ministry	7(7.3%)	67(69.8%)	22(22.9%)
Provincial Council & Institutes under PC	-	9(100%)	-
Special Spending Unit	-	3(60.0%)	2(40.0%)
Total	7(3.9%)	117(65.7%)	54(30.3%)

This reflects the fact; majority of the organizations (66%) have not used disaster recovery site in their organizations. Further, 30% of ICT officers in their respective organizations were not aware the process of using a disaster recovery site. Perhaps, majority of organizations did not have a disaster recovery was the case they did not have an awareness on this process.

Table 5.53: ICT risk assessment

Institute	Yes	No	No awareness on ICT risk assessment
District Secretariat & Institutes under DS & Divisional Secretariat	2(2.9%)	24(35.4%)	42(61.8%)
Ministries & Institutes under Line Ministry	10(10.4%)	46(47.9%)	40(41.7%)
Provincial Council & Institutes under PC	-	7(77.8%)	2(22.2%)
Special Spending Unit	2(40.0%)	2(40.0%)	1(20.0%)
Total	14(7.9%)	79(44.4%)	85(47.8%)

Table 5.53 signifies, majority of organization's ICT officers had no awareness on ICT risk assessment while 44% of organizations had not conducted and ICT risk assessment.

Following represent the distribution of ICT officers who had somewhat awareness on ICT risk assessment.

Table 5.54: Familiarity with risk assessment approaches

Role/ CIA Awareness	Yes	No	Do not know
System Administrator	1(33.3%)	1(33.3%)	1(33.3%)
CIO	1(100%)	-	-
ISO	-	-	-
Analyst	1(100%)	-	-
Web developer	1(50%)	-	1(50%)
Other	5(71.6%)	1(14.2%)	1(14.2%)
Total	9(6.4%)	2(14.3%)	3(21.4%)

This implies only 6% had some understanding on ICT risk assessment approaches.

Table 5.55: Familiarity on risk management process

Role/ CIA Awareness	Yes	No	Do not know
System Administrator	-	2(66.7%)	1(33.3%)
CIO	1(100%)	-	-
ISO	-	-	-
Analyst	1(100%)	-	-
Web developer	1(50%)	-	1(50%)
Other	5(71.4%)	1(14.2%)	1(14.2%)
Total	8(57.2%)	3(21.4%)	3(21.4%)

This shows, 57% of respondents had a some understanding with risk management process.

Table 5.56: Familiarity on risk identification

Role/ CIA Awareness	Yes	No	Do not know
System Administrator	1(33.3%)	2(66.7%)	-
CIO	-	1(100%_	-
ISO	-	-	-
Analyst	1(100%)	-	-
Web developer	1(50%)	-	1(50%)
Other	4(57.1%)	2(28.6%)	1(14.2%)
Total	7(50%)	5(35.7%)	2(14.3%)

This shows, 50% of ICT officers had a some understanding with risk identification process.

5.9. Incident Management

Table 5.57: Awareness on incidents

Role/ CIA Awareness	No	Yes
System Administrator	21(38.2%)	34(61.8%)
CIO	1(16.7%)	5(83.3%)
ISO	-	1(100%)
Analyst	3(37.5%)	5(62.5%)
Web developer	4(33.3%)	8(66.7%)
Other	52(54.2%)	44(45.8%)
Total	81(45.5%)	97(54.5%)

This signifies, 45% of ICT officers had no awareness on incidents. Following represent the Cybersecurity incidents faced by the ICT officers who had somewhat awareness on incidents.

Table 5.58: Experience on Cybersecurity incidents

Role/ CIA Awareness	Yes	No	No Awareness on Cybersecurity incidents
System Administrator	13(38.2%)	18(52.9%)	3(8.8%)
CIO	2(40.0%)	2(40.0%)	1(20.0%)
ISO	-	1(100%)	-
Analyst	3(60.0%)	2(40.0%)	-
Web developer	3(37.5%)	4(50.0%)	1(12.5%)
Other	11(25.0%)	29(65.9%)	4(9.1%)
Total	32(33.0%)	56(57.7%)	9(9.3%)

Table 5.58 depicts, majority (58%) has not experienced on Cybersecurity incidents, while 9% had no awareness on incidents faced by their respective organizations.

Table 5.59: Incident handling process

Institute	Yes	No	No awareness on incident handling process
District Secretariat & Institutes under DS & Divisional Secretariat	6(8.8%)	38(55.9%)	24(35.3%)
Ministries & Institutes under Line Ministry	19(19.8%)	48(50.0%)	29(30.2%)
Provincial Council & Institutes under PC	-	5(55.6%)	4(44.4%)
Special Spending Unit	1(20.0%)	1(20.0%)	3(60.0%)
Total	26(14.6%)	92(51.2%)	60(33.7%)

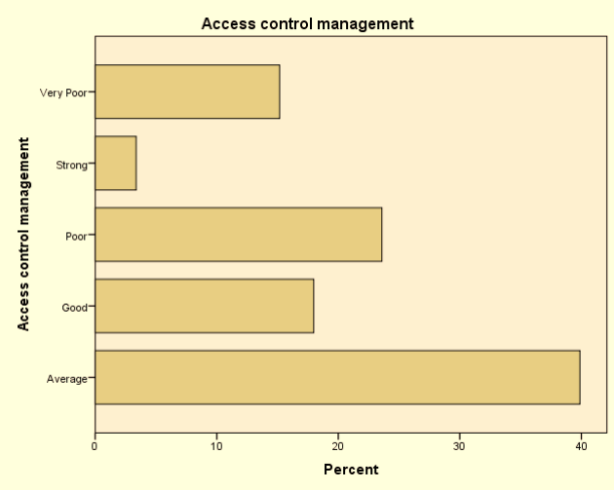
Table 5.59 depicts, only 15% of organizations were having incident handling process and 51% do not have such processes while 34% of respondents had no awareness on incidents handling process in their respective organizations.

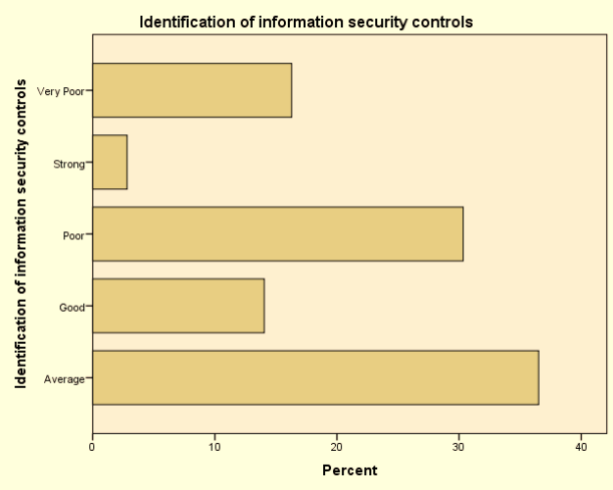
Table 5.60: Respond to incidents

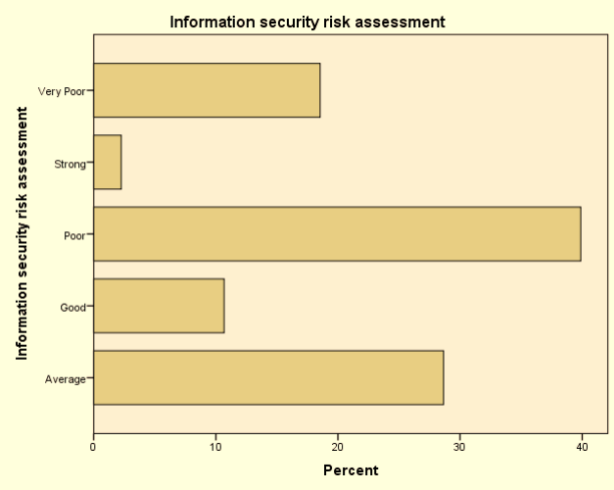
Role/ CIA Awareness	No	Yes
System Administrator	25(45.5%)	30(54.5%)
CIO	5(83.1%)	(16.7%)
ISO	-	1(100%)
Analyst	3(37.5%)	5(62.5%)
Web developer	4(33.3%)	8(66.7%)
Other	71(74.0%)	25(26.0%)
Total	108(60.7%)	70(39.3%)

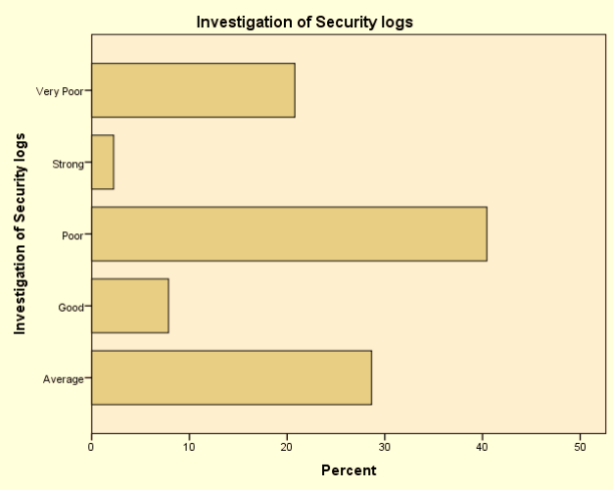
This shows majority (61%) did not know how to respond to an incident request from their staff in the organizations.

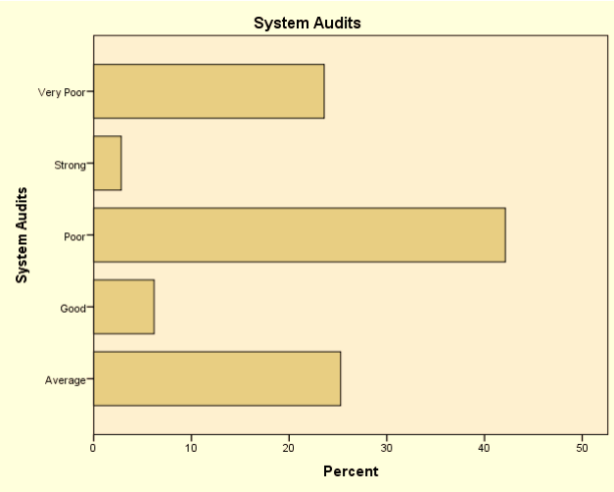
Awareness level on influencing variables for Cybersecurity

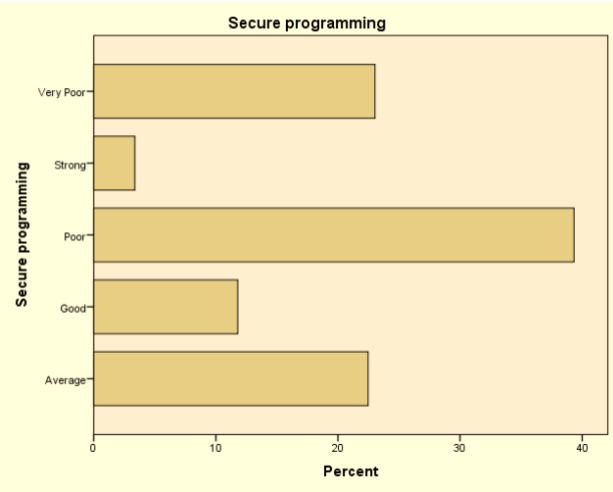


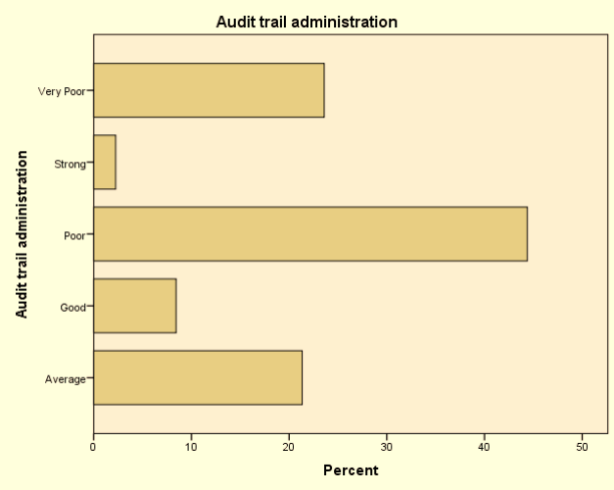


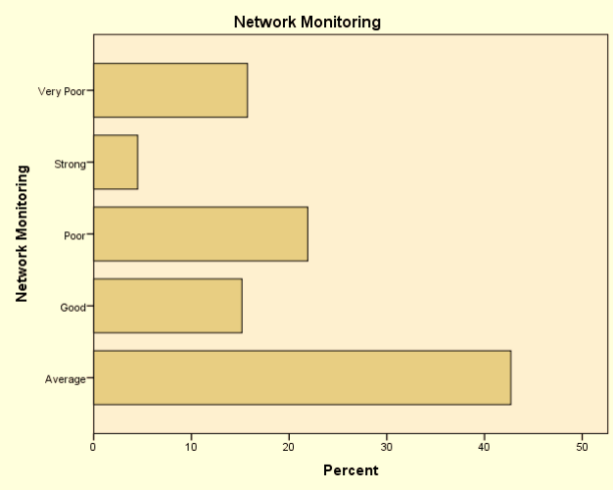


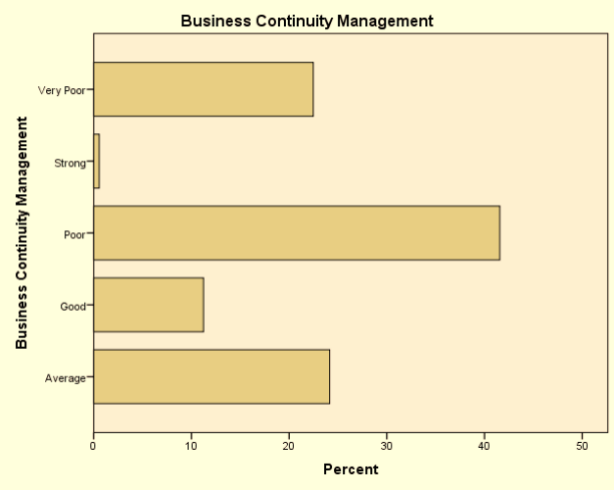


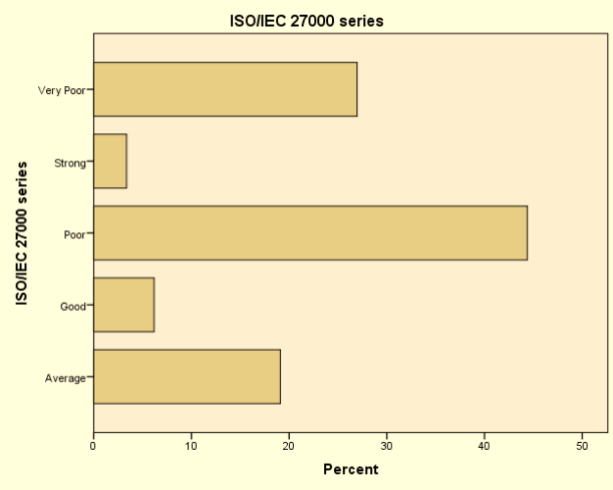

System Audits
System Audits
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
50
Percent


Secure programming
Secure programming
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
Percent

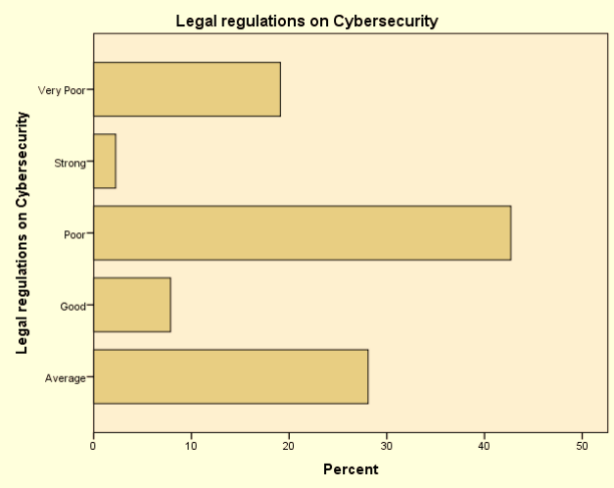

Audit trail administration
Audit trail administration
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
50
Percent

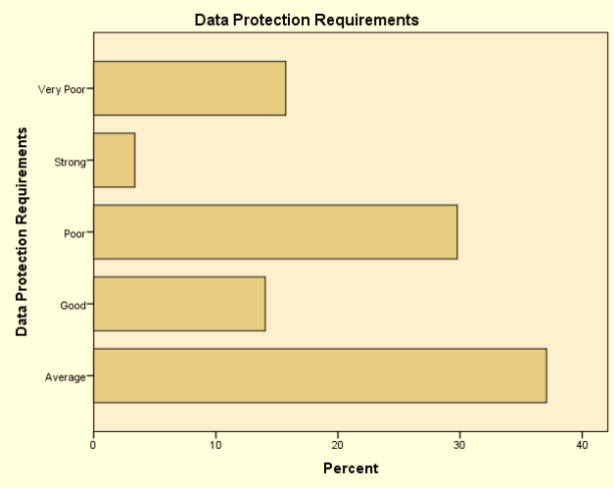

Network Monitoring
Network Monitoring
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
50
Percent

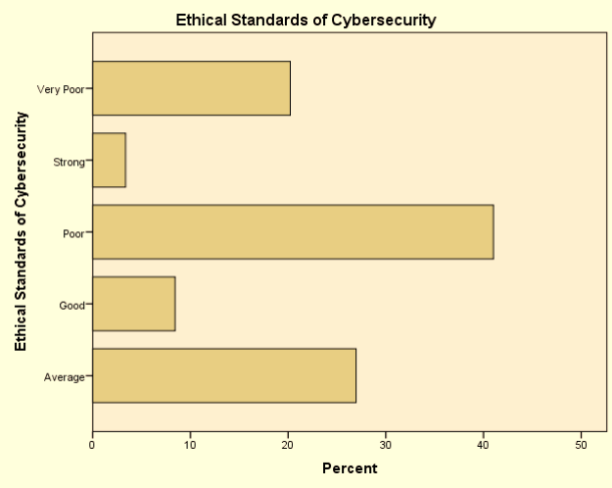

Business Continuity Management
Business Continuity Management
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
50
Percent

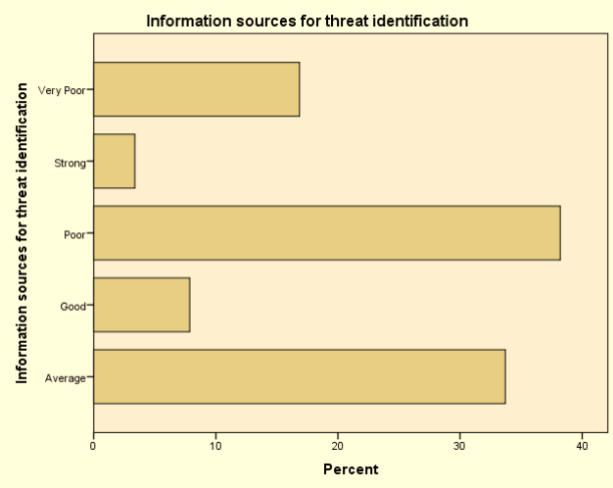

ISO/IEC 27000 series
ISO/IEC 27000 series
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
50
Percent


Data encryption methods
Data encryption methods
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
Percent

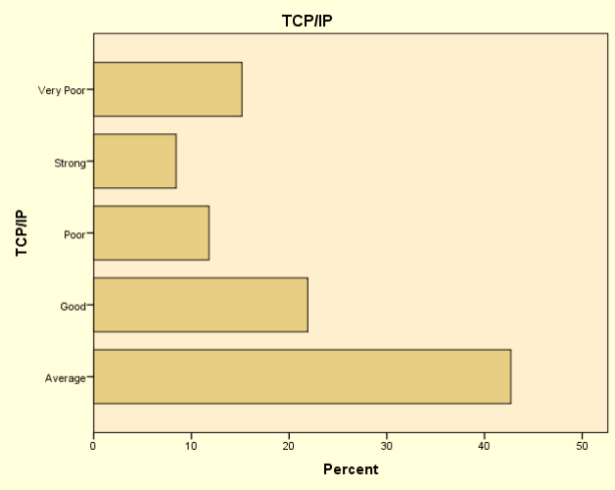

Legal regulations on Cybersecurity
Legal regulations on Cybersecurity
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
50
Percent

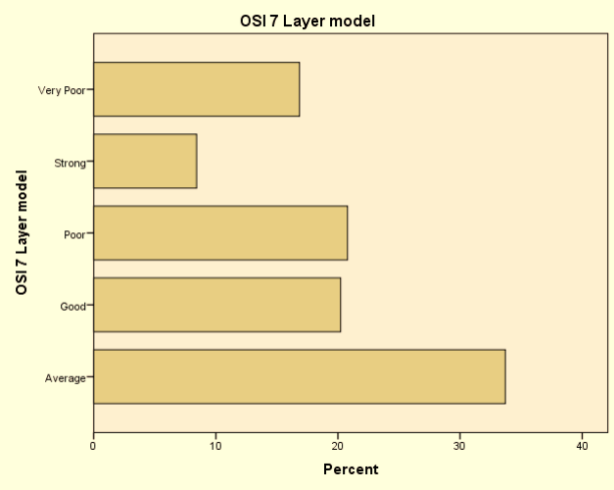

Data Protection Requirements
Data Protection Requirements
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
Percent

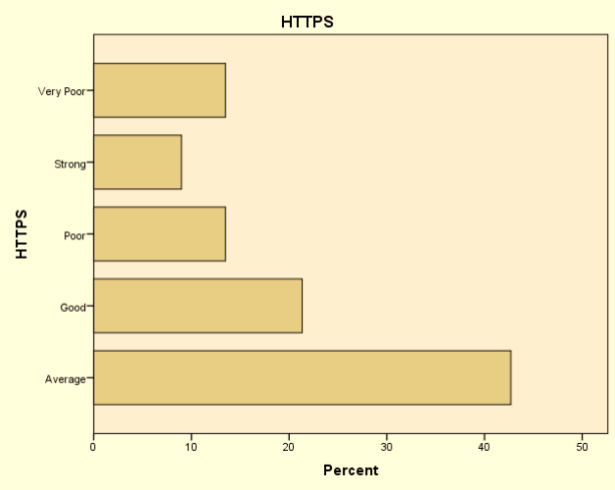

Ethical Standards of Cybersecurity
Ethical Standards of Cybersecurity
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
50
Percent

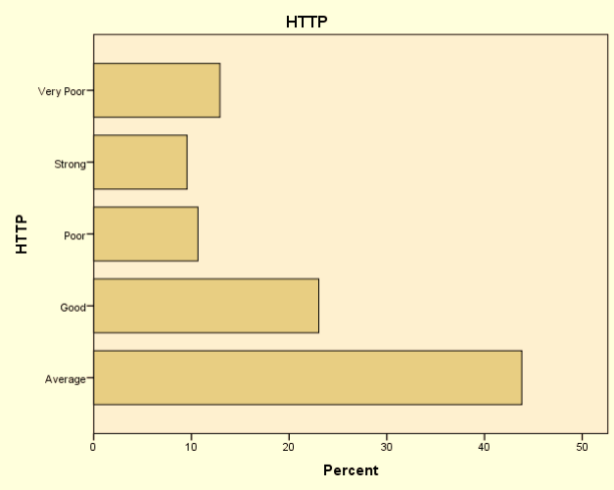

Information sources for threat identification
Information sources for threat identification
Very Poor
Strong
Poor
Good
Average
0
10
20
30
40
Percent

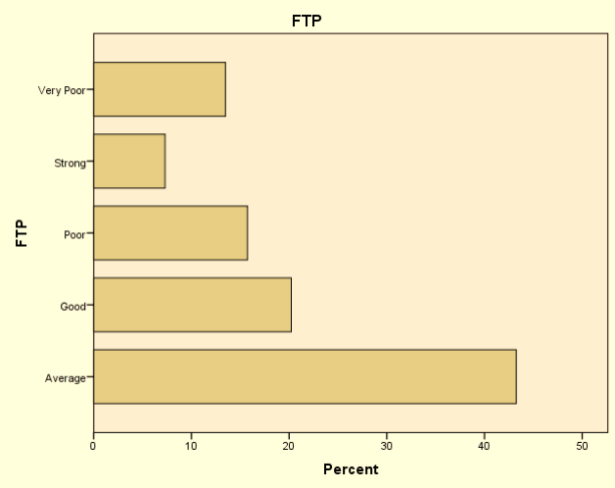
Awareness level on technical processes and protocols related to the Cybersecurity

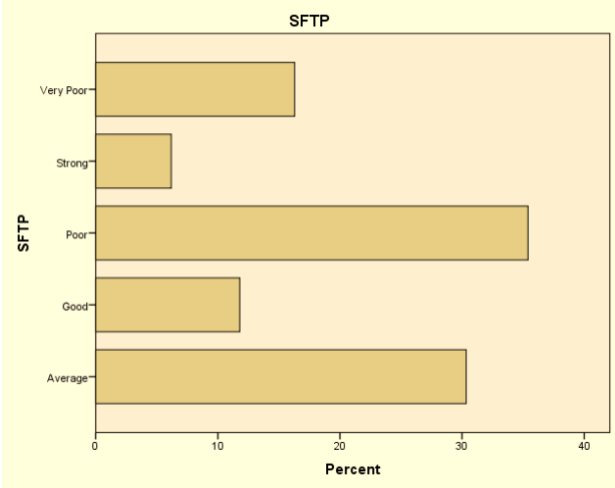


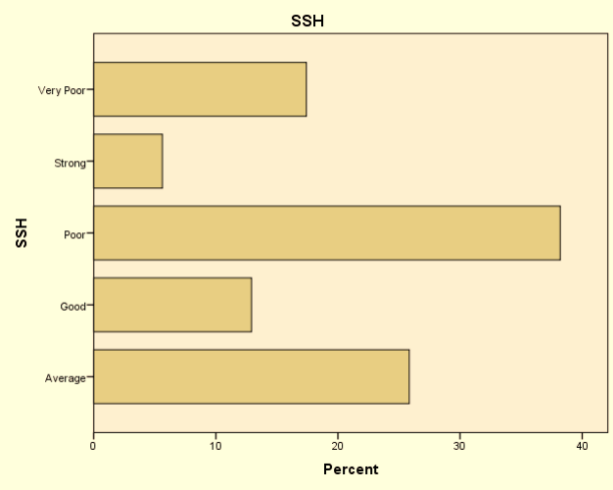


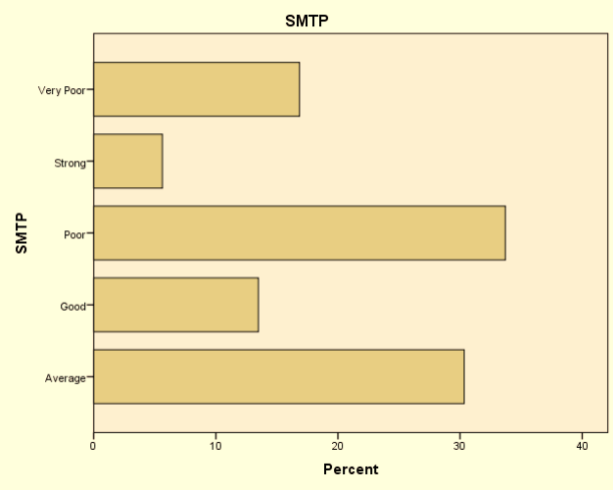


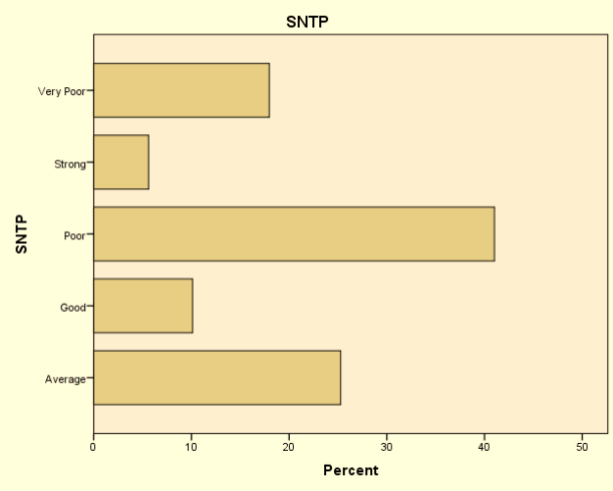


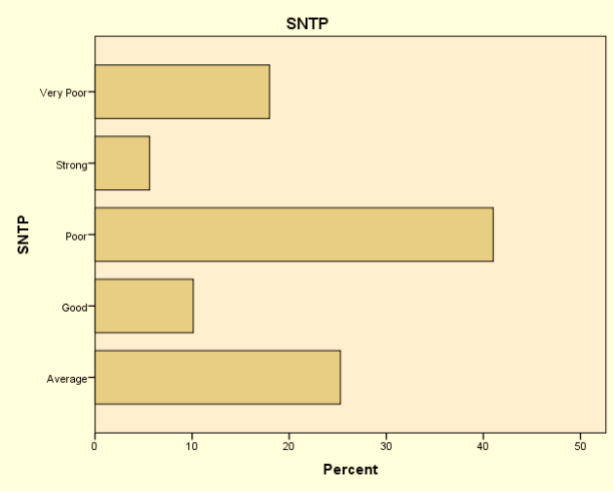


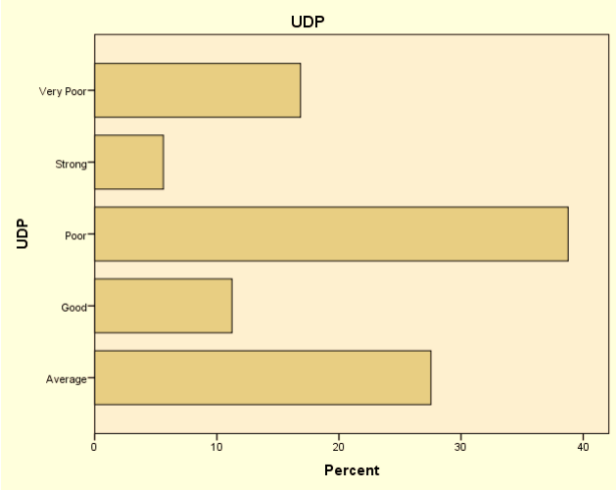


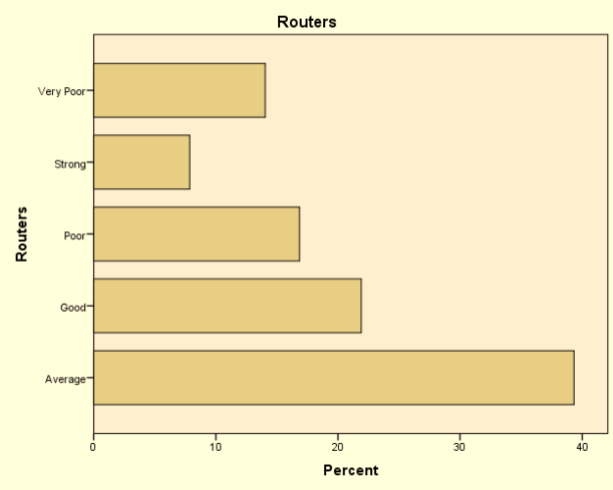

SSH
Very Poor
Strong
Poor
Good
Average
SSH
0
10
20
30
40
Percent

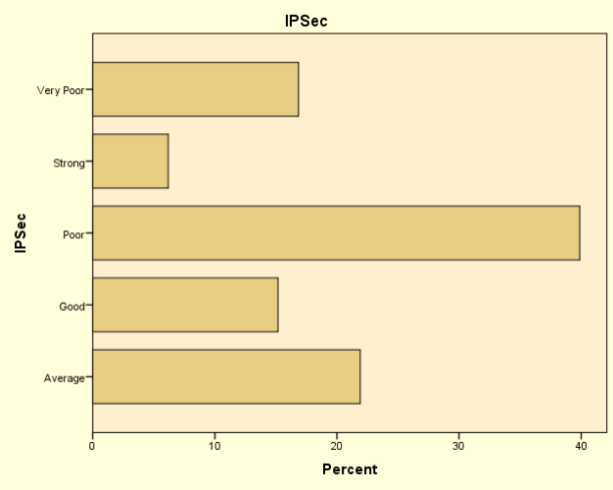

SMTP
Very Poor
Strong
Poor
Good
Average
SMTP
0
10
20
30
40
Percent

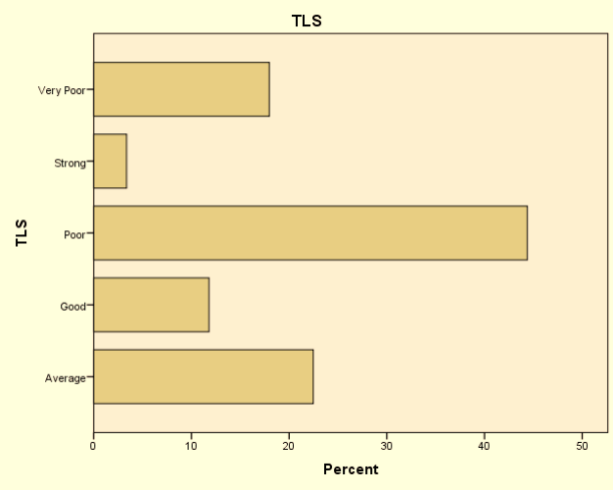

SNTP
Very Poor
Strong
Poor
Good
Average
SNTP
0
10
20
30
40
50
Percent

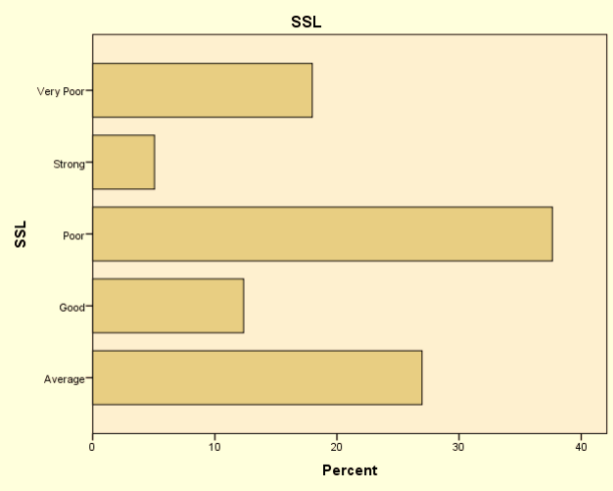

SNTP
Very Poor
Strong
Poor
Good
Average
SNTP
0
10
20
30
40
50
Percent

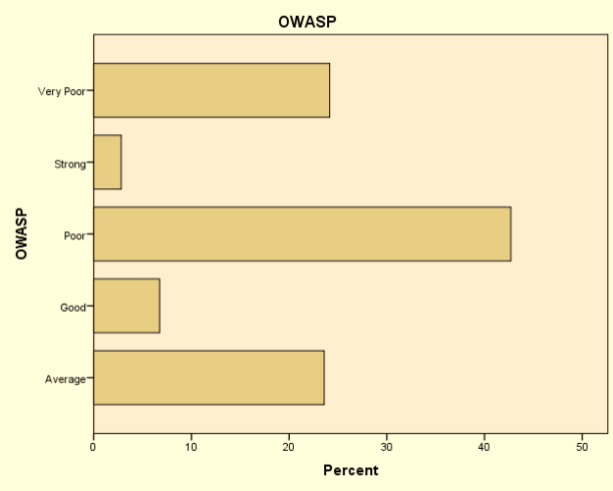

UDP
Very Poor
Strong
Poor
Good
Average
UDP
0
10
20
30
40
Percent


Routers
Very Poor
Strong
Poor
Good
Average
Routers
0
10
20
30
40
Percent


IPSec
Very Poor
Strong
Poor
Good
Average
IPSec
0
10
20
30
40
Percent


TLS
Very Poor
Strong
Poor
Good
Average
TLS
0
10
20
30
40
50
Percent


SSL
Very Poor
Strong
Poor
Good
Average
SSL
0
10
20
30
40
Percent


OWASP
Very Poor
Strong
Poor
Good
Average
OWASP
0
10
20
30
40
50
Percent

CHAPTER 6
CONCLUDING REMARKS AND HIGHLIGHTS

6.1. General employees' Summary and Highlights

Majority (73%) of Government employees have obtained some-type of ICT-based education. Although, very few have obtained direct ICT qualification while most of them obtained their education as an integral part of a major study programme. Interestingly, this study reveals that existing ICT-based education has not influenced their Cybersecurity KSA competencies. Perhaps, it may be the case that, majority of programmes may not have included the Cybersecurity related modules. Primary category of employees has shown very low-level exposure to formal ICT education or training. Further, very few employees (only 6%) have obtained Cybersecurity education or training through various types of programmes. In the context of literacy, most of the employees (75%) were comfortable with working in English language when they are using a device regardless to their residential province (E.g., Northern and Eastern Provinces).

Many employees were having access to the internet while this study also shows, there were no significant differences between different age groups (E.g., 25-34 and 55 and above) on using the internet in their devices. majority (65%) were engaged with one or more critical activities. including online banking, buying goods and services, selling goods and services, online social networks etc. These findings also show a positive correlation with internet usage and device usage. Many of them were using at least one device in their workplace, maybe personal or office property. Although lowest usage observed among primary category employees (recorded as 76%). In their office premises, a major portion were using a separate computer for their official work while a considerable amount which is 19%, were using shared computers. This shows the usage of both devices and internet is fairly high among employees and it would be prone to open-up many pathways for cyber threats.

The survey findings were showing a somewhat moderate level of good password practices among employees. For instance, 50% were randomly changing the passwords, 82% were keeping passwords memorized and 51% were using at least one good practice in creating a password (E.g., combinations of numbers, uppercase/lowercase letters and special characters). A highlight is, both ICT and Cybersecurity education or training has not influenced this moderate level practice of the employees, therefore, sometimes it was solely influenced by other factors including personal experience, awareness from media and others. In the context of information confidentiality and securing, very few employees were having Cybersecurity related KSA competencies. So, for example, only 8% were aware of encrypting a document and 15% were hiding their folders or documents. Accordingly, this could be grown to be a major issue when dealing with sensitive materials since lesser level of KSA competencies would create easy access to outsiders.

Major fraction of employees (95%) was having an Email address while only the median number of employees (56%) were having an official Email account for their office work. The exposure is relatively high when considering information communication channels. For the reason that, 48% were using private Emails and 34% were using shared Email for official communication purposes without having proper Cybersecurity KSA competencies. An interesting result was that a modest number of employees (40%) did not know whether their Email account had been hacked or not. Further adding to this, 40% had no awareness

of spam filtering options in their Emails and majority of these employees were having any-type of ICT-based education or training.

More than 90% of employees were using two or more social media platforms including Facebook, WhatsApp, You Tube etc. Average number of users were using these platforms without changing default security settings. Further, approximately 38% were using the practices of enabling two factor authentications and enabling security questions. When it was tested against ICT and Cybersecurity education/training, none of these factors were influenced by choosing lower exposure or non-critical practices. A notable finding is, even though employees are using social media only 8% of them have somewhat awareness of social engineering activities. This implies, employees could become highly exposed when using social networks.

Survey results showcase, 35% of employees were using public Wi-Fi showing less usage of public networks. As a positive stance, findings show very few employees (approximately 5-7%) were engaged in critical activities by using public networks. In addition, only 5% were using internet cafes, which was one of the hotspots for many people who were likely to do their work by using the internet in a decade back history.

Around 62% of employees were sharing their portable devices with respective co-workers and external parties. The biggest threat is nearly 95% of employees were not encrypting the content, possibly it may be the case that they do not know how to encrypt the content. When comparing the two groups of employees who did not have Cybersecurity education/training with those who had, there was no significant difference between practices followed by both groups. Consequently, it can be concluded that these practices are not influenced by Cybersecurity education or their training level. Data losses also could be inevitable since only 36% of employees are backing-up their E-documents to another place mostly to a portable device. After further testing, it reveals that the average number of employees were using highest exposure practices including maintaining a copy in the same computer or/and in an external storage and keeping outside the office. This implies unavailability of good practices in organizations, whereas it could be enabled to increase data loss incidents in future.

According to the behaviors of the employees, a moderate number of workers (43%) were following one or more critical behaviors when using a computer, including keeping the computer logged in while they are away from the computer and letting coworkers switch off their computers. It also discovered, current level of ICT and Cybersecurity education/training has not influenced the behaviors of the employees, which shows employees are likely to follow critical behaviors when using computers. Further, the average number of employees were not aware of responding to generic day-to-day activities including receiving an unknown email, link, message, or any other type of material from an outside party, since most of them were not checking the critical aspects (E.g., Email header, URL, verification with relevant parties etc.). For instance, 56% of employees were to open an unknown attachment or/and check or/and ignore it completely or/and delete it immediately. When entering login credentials into a familiar website, the majority (57%) were not searching for the (Green padlock in the address bar) https or/and not checking the content of the website or/and the URL (Website address) for accuracy. This shows lack of awareness on security measures when browsing through websites. Most importantly, when sharing the sensitive data and information, moderate number of employees (43%) of were not using secure information sharing channels (via private or

official Email) when sharing the information with co-workers and average (50%) number of employees were also not using these secure channels when sharing the information with external parties, showing a higher degree of risk associated with sharing information and data in these organizations.

The survey results illustrate, significant number of employees (76%) were using anti-virus software while most of them (65%) were using a genuine copy. Majority had set their software for automatic updates and these findings suggest basic awareness of protection is at a somewhat higher level. Further average number of employees (51%) had somewhat KSA competencies on identifying an infection while 67% could not identify unauthorized access to their machines. This tells, higher degree of awareness on protection is not available among employees. Although, this level of awareness is sometimes referred to as the basic level in advanced countries like U.S and U.K.

Only an average number of employees (53%) had some type of awareness on cyber threats/crimes. Also, 66% of employees were not aware of the SLCERT indicating lack of promotional activities on SLCERTs' role in cyberspace. Under policy level awareness, the majority of organizations did not have a written policy on fair usage, information security, social media, user access, data security, disaster recovery which showed a less conducive environment on Cybersecurity related strategy implementation.

SPOTLIGHT 1

- Majority (73%) has obtained some-type of ICT based education. However, ICT education has not influenced their Cybersecurity KSA.
- However, the Primary category of employees have shown very low-level exposure to formal ICT education or training.
- Very poor ICT security related policy level awareness was observed. Generally, Fair usage (88%), Information security (82%), social media (83%), User access (83%), Data security (83%), and Disaster recovery (89%) policies are not available in the majority of the organizations.
- ICT education or Cybersecurity related education/training has not influenced all the practices that were tested in this survey. Very few (6%) had Cybersecurity education or training obtained by the sample. However, Cybersecurity training/education has not influenced their KSA level.
- While having this type of policy level freedom and lower KSA levels in Cybersecurity, Government employees are not using information technology in a subsequent manner. Consequently, there is a grave danger of going towards E-Government or digitalization.
- Manly, Primary and Secondary category employees are enrolled in using ICT in their offices (E.g., documentation). This population does not have a proper KSA level, specifically primary category employees. This imposes a higher risk on Cybersecurity.
- General awareness of Cybersecurity threats is also shown at a very low level where it stresses a properly planned upliftment of KSA regarding Cybersecurity through formal training

6.2. ICT Officials' Summary and Highlights

Average number of officials (54%) surveyed, were handling both ICT and other office work without having a proper designated job scope. For instance, an ICT graduate or an employee who were having somewhat ICT related knowledge or skill could be permitted to engage in ICT materialized work in their organizations. Other officials designated as Analysts, CIOs, ISOs, System Administrators, and Web Developers. Even though some of the designations are not officially published by the Government (E.g., System Administrator). When examining the awareness of various Cybersecurity facets, Moderate number of officials did not have an awareness of the CIA triad (confidentiality, integrity, and availability) of information security. Further, average number of officials were aware of Cybersecurity related tasks including encrypting and backing up sensitive data, recovery process, and other security measures Also, it was recorded a very poor awareness level on other critical aspects including administration of Email server and spam filtering, monitoring security logs, ICT risk assessment, risk management, risk identification, indicating huge vacuum in their knowledge and skills , which implying lack of experience, training, education, and other factors on obtaining Cybersecurity awareness.

Average number of organizations (49%) did not place a critical system. For other organizations, several critical systems were identified including, online sales, ERP systems, Operational Management Systems, Budget Formulation, Human Resources, Management office website, Fuel and Vehicle Management. Fair number of organizations (37%) which had critical systems in place did not have an IPS/IDS in their systems. When considering the awareness on asset classification, approximately 74% did have very poor awareness and sometimes they did not know the definition of asset classification. This pattern was also repeated under awareness of information asset inventory. Further, officials who had an awareness on asset inventories had no experience on developing or mapping processes showing a lack of skills on the same. Majority of officials agreed or agreed to some extent on defining the types of information which could be given access to different types of external stakeholders, including to have an information sharing policy. Majority of their institutions (79%) under four stratums were not practicing the data classification mechanisms. Although at Ministry level (26% of institutions) were somewhat implemented the activities but not enough to cope with prevailing digitalization trend. Surprisingly, most of the officials (74%) had no awareness of the gravity of information handling. Corresponding to disaster recovery, tragically, 87% of organizations under consideration did not have a disaster recovery plan while only 34% of officials had knowledge on preparation of this type of plan. Although, at least as a positive posture, 24% of organizations were preparing the plan at the time of this survey conducted.

According to ICT policies and procedures, Ministries were playing a leading role alone with special spending units. Most other organizations including DS and PCs had no separate ICT rules/regulations or policies. For the organizations which had ICT policies and regulations, the majority (62%) of stakeholders involved in making them were identified as internal. Average number of officials (49%) had no awareness of information security policy while 41% of organizations have not implemented this policy. These results also validate other findings as for example 45% of organizations had not conducted an information security assessment on its information systems. Moreover, this is also true for access control policy showing unsatisfactory conditions on policy level implementation. Further, Awareness on password or user account policies were equivocal among approximately 30% of officials and critically, some of officials, specifically System

Administrators had poor technical knowledge on some aspects that could be an inclusive part of policy implementation (E.g., sector-based formatting, good practices on password usage, information sharing etc.)

Majority of organizations (55%) were using CCTVs while DS and PCs had a lower usage. However, managing CCTV activities was done by external parties. Importantly, 58% of organizations were not applying the CCTV security practices. Majority of organizations (84%) had computer network systems. It also identified that awareness on configuring VPNs was lower (around 26%). The organizations (79%) which had VLANs were running a firewall system. Even though, average number of officials had somewhat knowledge on configuring firewall rules, a smaller number of them (39%) had awareness on firewall auditing rules. In addition, most of the organizations (85%) had no incident handling process and it was assessed that the majority of ICT officials had no knowledge on how to respond to an incident.

SPOTLIGHT 2

- Majority of employees who were handling ICT related work in their organizations were system administrators (30.9%) and other officers (53.9%). According to findings, it seems they did not have the required level of technical knowledge or skills to handle Cybersecurity related functions.
- Small number of CIOs were available, and out of them the majority comprised an average level of knowledge and skills compared to other officials.
- In an average, less than 40% had a basic security knowledge, which shows about less than 20% had knowledge on system protection
- Approximately, between 20-25% had awareness on ICT asset identification, asset classification, and asset inventory classification. Also, less than about 20% had taken actions to secure their organizational assets.
- Organizations which had employees who had an awareness of ICT asset identification, classification and asset inventory, less than about 40% were implementing the security procedures.
- Approximately, 20-30% of officials comprised awareness on data classification and sensitive data classification. At the Ministry level, officials have shown the highest level of awareness compared to other organizations.
- General awareness on ICT policies were very low and less than half of officials were involved in making policies and procedures out of which were implemented.
- The knowledge level could be defined as very low on disaster recovery policies, implementation, and current usage.
- About 45% of officials had no awareness of incidents
- Out of officials who acquired awareness, very poor implementation strategies were shown within the organization with respect to Cybersecurity functions

Among officials, 30% had experience in server administration whereas approximately 40% of employees had experience on patch updating, setting privileges, activity monitoring, and server hardening. Under accessibility to the servers, 25% organizations have provided access to the outside parties indicating increasing likelihood for direct exposures. Although, taking measures to reduce the attack surface was at somewhat moderate condition since the majority were using virus guards, password updates, and firewall systems. Amongst organizations, approximately 48% were managing their websites while half of them were managed by outside stakeholders. Very few organizations had obtained

SSL certificates. Nearly half of them (40%) conducted their security assessment before the launching.