DEVELOPMENT OF CYBERSECURITY TRAINING PROGRAM FOR THE ACADEMIC COMMUNITY – A ROLE-BASED APPROACH

By

Sajjal Akram

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

July 2017

THESIS ACCEPTANCE CERTIFICATE

Certify that final copy of MS/MPhil thesis written by ~~Mr~~/MS **Sajjal Akram** Registration No. **NUST2013-62698-MMCS-25213F**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: ________________________

Name of Supervisor Col Baber Aslam, PhD

Date: ____________________________

Signature (HoD): ___________________

Date: ______________________________

Signature (Dean/Principal): ___________

Date: ____________________________

ABSTRACT

The IT security awareness is an ever increasing issue in today's world. It is generally believed by the IT security professionals' community that people are one of the weakest links in the process of systems and networks security. The foundation of information security is based on three major pillars; people, process and technology. When it comes to technology and its vulnerabilities, there are fixes and patches. When it comes to IT processes and their vulnerabilities, there are fixes and patches. But there is absolutely no patch to human misjudgment or unawareness. Organizations develop security procedures and policies to ensure the availability, confidentiality and integrity of information. But these security policies and procedures alone are not enough for the protection of information and IT assets of organization. Failure in paying attention to the security training poses greater risk to organizations because IT security is not merely a technology issue but also a human issue. The future of a nation relies largely on its youth and so does the future of its cyberspace. The nations' youth with extra-ordinary knowledge and skill in Internet usage help in creating a flourishing cyberspace and ultimately a powerful country. This is the reason why developed countries like US and UK have cyber security awareness programs for the children as young as four years old thereby producing the youth with security conscious attitudes and hence enhanced security posture. While the countries like Pakistan are only focusing on technology and processes and not on the people, rendering the people totally vulnerable to technology threats and attacks. Lack of awareness and training is a vacuum in IT security world and this research aims to fill this vacuum. This research aims at laying down a foundation for security awareness for the academic community for both the general users and the individuals having significant IT related responsibilities. The idea of role-based training is to recruit and educate the IT individuals according to their specific domain need to avoid lack of adequate training or over consumption of training. Role-based training is required within the security arena as it addresses the training specific to the IT role, functional job and responsibility of the individuals. This research has assessed security awareness levels and needs of the general and IT users in different domains and designed security training programs accordingly. This research shall help the academic community in gaining more and better understanding of cybersecurity awareness needs and increase the individuals' readiness to respond to security incidents and to stay one step ahead from the adversary.

ACKNOWLEDGMENTS

In the name of Allah, the Most Beneficent and the Most Merciful

All praises to Allah for the strengths and His blessing in completing this thesis. I would like to convey my gratitude to my supervisor, Dr. Baber Aslam, for his supervision and endless support. His invaluable help of constructive comments and suggestions throughout the experimental and thesis works are major contributions for the success of this research. Also, I would thank my committee members; Dr. Monis Akhlaq, Dr. Imran Rashid and Asst. Prof. Mian Mohammad Waseem Iqbal for their support and knowledge regarding this topic.

I would also thank system administration team of MIS Cell of Military College of Signals, for providing me with the required data.

Last, but not the least, I am highly thankful to my parents. They have always stood by my dreams and aspirations and have been a great source of inspiration for me. I would like to thank them for all their care, love and support through my times of stress and excitement.

TABLE OF CONTENTS

1. INTRODUCTION

2. LITERATURE REVIEW

. 3. ANALYSIS OF CYBERSECURITY EFFORTS IN THE ACADEMIC COMMUNITY OF PAKISTAN

. 4. ANALYSIS OF CYBERSECURITY AWARENESS LEVEL OF GENERAL USERS IN THE ACADEMIC COMMUNITY OF PAKISTAN

5. CYBER SECURITY TRAINING PROGRAM FOR THE GENERAL USERS

6. CYBER SECURITY ROLE-BASED TRAINING PROGRAM FOR THE IT STAFF

7. CONCLUSION

LIST OF FIGURES

FIGURE # CAPTION…………………………………………………...……………PAGE

LIST OF TABLES

ACRONYMS

CM	Configuration Management
HTTP	Hypertext Transmission Protocol
HTTPS	Secured Hypertext Transmission Protocol
IA	Information Assurance
IAM	Identity and Access Management
IM	Incident Management
InfoSec	Information Security
ISACA	Information System Audit and Control Association
ISMP	Information Security Program Model
IT	Information Technology
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
PCI	Payment Card Industry
QA	Quality Assurance
SANS	SysAdmin, Audit, Network and Security
SSL	Secure Socket Layer

Chapter 1

INTRODUCTION

1.1 Introduction

Cyberspace – The open IP-enabled worldwide network infrastructure for government, communications and commerce is expanding at ever increasing rate. This rapidly increasing interdependence and interconnectivity has now become an integral part of the world's social structure and economy. However, this humungous growth in usage of cyberspace has not been accompanied by appropriate and sufficient increase in security. Cyberspace which on one hand has resulted in many benefits such as social networking, e-commerce and user generated content, is on the other hand plagued with ever growing number of security threats and vulnerabilities that are exploited by spies, cyber criminals, hackers and terrorists. The computer users are at huge risk of being targeted by computer/cyber attacks, information warfare, espionage, identity theft and a number of other malicious threats [1].

The borderless nature of Internet, anonymity and ease of access have allowed inescapable computer crimes to become more numerous and common. The international security and Law enforcement organizations along with the private and public sectors have very recently started to pay attention to the intensity, scope and the very transnational nature of this problem.

As cited in periodicals, audit reports and conference presentations, it is generally believed by the IT security professionals' community that people are one of the weakest links in the process of systems and networks security [2].

1.2 Problem Statement

The IT security awareness is an ever increasing issue in today's world. Lack of awareness and training is a vacuum in IT security world and this research aims to fill this vacuum. As mentioned earlier, people are the weakest link in securing networks and systems and hence a properly organized and evaluated awareness and training program is needed for them. The academia sector of the developing nations seem to be lagging behind in paying attention to providing awareness and training to its people, that includes students, faculty and all the IT staff members. The training programs developed and being used in developed nations are meant for the mature organizations and cannot be mapped directly to the ones in developing nations. The studies show that cybersecurity training strategy is not a one size fits all and hence it must be customized for each country [5] [36]. Also, the resources that are available with the academia sector of the developing countries lie below the reasonable threshold which is significant to provide required level of training to their people. Hence, there is a need of a comprehensive awareness and training program for the academic community that is reflective of their needs and is implementable with their natural resources.

1.3 Research Objective

This research provides solution to the aforementioned problems by proposing cybersecurity awareness and training program for the academic community of Pakistan. This thesis aims primarily at achieving the following goals:

- Study of current state of cybersecurity awareness level in the academic community of Pakistan.
- Performing a gap analysis by conducting a survey of security awareness in general users and IT staff and their different roles.
- Developing role-based cybersecurity training program and proposing the method of measurement of effectiveness of the program.

1.4 Scope of Research

The research applies to the academic community of the developing countries owing to their similar security awareness level. The survey has been conducted in Pakistan, a developing country. The survey covers several universities of the academia sector of the country. The users who have been part of the survey include the *general users* i.e. students and faculty; and the *technical users* i.e. the staff members who have IT related responsibilities. The training modules have been designed on the basis of the results deduced from the survey.

1.5 Significance of Research

The research shall serve as a platform for providing cyber-security training to the individuals in the academic institutions. This shall contribute in developing a trained workforce having ability and willingness to deal with the security threats, hence enhancing the security posture of the organization. The research shall help the academic community in gaining more and better understanding of cybersecurity awareness needs and increase the individuals' readiness to respond to security incidents.

It will provide deeper awareness of cyber threats to the individuals including students, preparedness for the individuals to stay one step ahead from adversary and shall help organizations to make proactive, defensible, and data-driven decisions about cyber personnel and their work.

1.6 Research Methodology

The research is based on the risk assessment survey conducted in different institutes of Pakistan revealing current state of awareness of the people from both technical and non-technical domains. The survey was based on questionnaires and interviews based on SANS security awareness and training solution *'Securing the human'* [37]. The survey has been divided into three categories; *general users*, *IT Staff* and *senior management*, as explained in section 1.6.2. The survey sample space for general users includes about 1000 users from technical and non-technical educational backgrounds. The survey was completely manual and the questionnaires were explained to the survey takers by one-to-one interaction with them. The exact authenticity of the survey cannot be measured however, the interviews conducted after the written survey closely matched the questionnaires' results. The survey for IT staff has been conducted to identify their roles and responsibilities in their respective domain. The survey for senior management highlights the efforts and measures taken by the organizations to ensure better security posture. The training modules have been driven based on the results of the survey. The survey methodology for the general users has been explained in Chapter 4 and that of the IT staff has been explained in Chapter 6.

1.6.1 Literature Review

The research unfolds with the current efforts in the field of cyber security awareness and training worldwide. The current threat environment due to lack of awareness in the people will be discussed. Finally, the frameworks, models and programs that have brought change will be discussed.

1.6.2 Surveys

Surveys have been conducted in three different categories.

a. General users – The students and faculty

b. IT staff – Staff having IT related responsibilities

c. Senior management – Higher authorities of the institute

These categories cover all the concerned people who are part of the academic community and who vital play role when it comes to interaction with IT. The general users need security awareness because they interact with technology on daily basis and are more prone to cyber-attacks owing to their lesser knowledge. IT staff is the major component of the cyber security training workforce because they interact with technology not only on personal level but on professional level. They are bound to protect the IT assets they work on. Senior management is the driving force of any cyber security training initiatives. The management authorities will only be able to address the awareness and training issues if and only if they themselves are fully aware of the threats brought along by the technology their students interact with and their IT staff work on. Hence, for a fully prepared and cyber safe workforce, all three components of academic community; general users, IT staff and senior management must be trained on cyber security.

1.6.3 Risk Assessment

The survey for general users has been conducted in ten different cyber domains explained later. The three-point scale has been chosen for the questionnaires low, medium, high according to the users' IT habits. The aggregate response shows the level of the risk, low, medium or high in the particular domain according to the level of awareness. The survey for IT staff has been conducted based on NIST Standard 800-16 to identify tasks related to each role and associated functional perspective of that role. The survey for senior management has been conducted broadly in different security categories (Organizational, Physical, Digital etc.) to measure overall security posture.

1.7 Contribution

The survey conducted has identified the gap between the current state of security awareness and acceptable state of security awareness. The training modules have been designed on the basis of the survey results. The training modules of general users are based on SANS standard and training modules for technical users are based on NIST Role-Based training model. The respective training modules from these standards have been customized according to the survey results. The training programs proposed can be mapped to any technical roles in any academic organization with any level of competency.

1.8 Thesis Outline

The first chapter of the thesis is the introduction discussing the scope, significance, methodology of the research and how the overall research has been conducted. Chapter 2 is the literature review which highlights the importance of people in the information security domain, the ratio of cyber crimes in Pakistan and finally discusses some of the most effective global initiatives in cyber security awareness and training. Chapter 3 presents the analysis of the current cyber security efforts in the academia sector of the country. Chapter 4 presents the current cyber security awareness level of the general (non-technical users) in different cyber domains individually. Chapter 5 discusses the proposed training program for the general users based on the survey conducted. Chapter 6 is the main body of the research for the IT users proposing the role-based training program for the IT staff based on the tasks and job responsibilities they have or expected to have in near future. Chapter 7 concludes the research with the outcome and limitations of the research and concluding remarks.

1.9 Conclusion

Pakistan is one of the developing countries that are lagging behind the minimum required level of security awareness as the technology is advancing in order to prepare the nation to remain safe and secure online. This research aims at taking an initiative regarding this issue. The security training modules proposed for the users are based on the results of the survey conducted. The survey identifies the gap between the current and required level of awareness. The implementation of the training program proposed shall help bridge this gap for a better cyber savvy academic community. This chapter has covered scope and significance of this research and how the research has been conducted.

Chapter 2

LITERATURE REVIEW

2.1 Introduction

Organizations develop security policies and procedures to ensure the confidentiality, integrity and availability of information. But these security policies and procedures alone are not enough for the protection of information and IT assets of organization [3]. Failure to pay enough attention to IT security training poses organizations to huge risk because the security of IT is not just a technology issue but also a human issue. It is the individuals who create, manage and implement the policies and processes. It is the people who are integral to the success of maintaining a secure organization. Every individual who uses or owns, relies on, or gets to manage the information and the IT systems must completely understand their responsibilities specific to security. Information which requires security includes the information owned by them, the information shared with them as part of their job and the information they may get to interact or deal with [4] [5].

2.2 People – The weakest link in the process of security

As they say *'There's no patch to human misjudgment'*, people tend to be the weakest link in the process of information and network security [6]. The foremost reason of any cyber threat is the unawareness of the individuals. Some of the most impactful attacks on the cyber space globally today mostly aim to exploit the user behavior. Some of these include phishing attacks via email, exfiltration of personal data via social engineering, and induction of malicious software via drive-by-download attacks. These attacks and increased complexities demand greater focus on training of the IT staff to avoid any misconfigurations, strengthen hardening and increase the appropriate response. Training these users (both unprivileged and privileged) along with those having access to any other sensitive information is a must to deter these attack methods.

2.3 Why Academic Community

There is a dire need of moving from mere awareness to tangible behaviors. The primary purpose of security awareness is to render people amenable to change.

The future of a nation relies largely on its youth and so does the future of its cyberspace. The nations' youth with extra-ordinary knowledge and skill in Internet usage can create a flourishing cyberspace and ultimately a powerful country." Lu Wei, head of the Office of the Central Leading Group of Cyber Administration, was quoted as saying [7].

Universities and Colleges are a community unto themselves, with a blend of departments, offices and even small on campus businesses. The student and employee information has to be protected, as well as financial records, research and other sensitive information. The institutes at the same time need flexibility in allowing access for all kinds of systems, devices and software [8]. In all these tasks, the security awareness and training of the students as well as the staff having significant IT related responsibilities play a vital role. In Pakistan, there have not been any efforts in proposing and promoting IT security awareness and training programs in the academia sector. In the developed nations, the awareness programs have started for the age groups as low as 4 (The campaigns are discussed in section 2.5), thereby producing the youth with security conscious attitudes and hence enhanced security exposure.

2.4 Ratio of cyber crimes in Pakistan

Cyber crimes are on the rise in Pakistan. Approximately 68 complaints have been reported to National Response Centre for Cyber crimes (NR3C) Pakistan [38]. These include cases like children's kidnapping, women harassment and blackmailing via social media cases. The investigations have revealed that in most of the cases the victims had shared their personal information like pictures, passwords etc. with the adversary which later were used for extortion purposes. These are the cases that have been reported, there are a hundreds of others that go unreported especially ones that involve female victims due to societal taboos. But prevention is better than cure, an effort to instill a sense of ability in the people to defend themselves, to be technically savvy, to be cyber safe and to respond to security incident immediately is way more important than reporting the incident after the damage has been done.

2.5 Global cyber security awareness initiatives

There are a number of security awareness campaigns being run worldwide. Most effective campaigns and programs however are originated in the developing countries like US, UK, France etc. Following sections discuss some of the most renowned campaigns from across the world.

2.5.1 National Cyber Security Awareness Month (United States)

In United States, the month of October is celebrated as the National Cyber Security awareness month every year. This is so far the most successful and renowned awareness campaign in the cyber world. The campaign is run by the Department of Homeland Security under the administration of President Obama. The purpose of the campaign is to spread awareness and train the American public on cyber security risks and threats. The campaign is designed to engage the both public and private sectors through several events and initiatives in order to spread awareness regarding cyber security and to enhance the resiliency of the nation in case of a cyber incident [11].

Table 2.1 Awareness campaign United States

Item	**Notes**
Campaign name	"National Cyber Security Awareness Campaign Challenge"
Host	Safe Internet Alliance and National Cyber Security Alliance
Organization	United Nations Department of Homeland Security under the administration of President Obama
Main URL	https://www.dhs.gov/national-cyber-security-awareness-month#1
Topics covered	• Personal Internet Security • Safe practices for personal computer and Internet Use
Target Audience	All U.S. citizens
Methodology	• President Obama is personally approaching the American public via most efficient means proposed by the citizens with the aim of spreading the message of Cyber Security significance. • The citizens responded to the campaign by proposing most suitable ways according to them that best spread the awareness of Cyber security threats and risks posed to the people [12].

2.5.2 Identity theft; Don’t become a victim (United Kingdom)

This campaign provide a wide range of the Fraud prevention services to its audience, also offering a Fraud avoidance system that are being consumed by approximately 262 UK organizations in a number of public and business sectors [13].

Table 2.2 Awareness campaign United Kingdom

Item	**Notes**
Campaign name	Identity theft; Don’t become a victim (United Kingdom)
Organization	Identity Theft UK
Main URL	http://www.identitytheft.org.uk/
Topics covered	• How to protect yourself • Identity Theft • What can be done • Who can help • Are you a victim
Target Audience	Businesses General Public
Methodology	• Videos on the official website • Online Literature [14]

2.5.3 EU Safer Internet Program

The safer Internet program is meant to teach and training the European community on the safe Internet usage especially to address the risks on the young people. ‘Parents, teachers, young people and carers must be aware of all the risks that may be posed to the the youth. The ultimate motto is to fight against harmful and illegal content. The major goals are to promote and encourage safe usage of internet and technologies, especially for the young generation, to educate and train the users mainly parents, teachers, educators and children to defend themselves against illegal and harmful content online [15].

Table 2.3 EU Safer Internet Program

Item	**Notes**
Campaign name	EU Safer Internet Program
Organization	Europe’s Information Society
Main URL	http://ec.europa.eu/information_society/activities/sip/index_en.htm
Topics covered	• Raising awareness • Harmful conduct • Illegal contect • Promoting a safe online environment
Target Audience	Young people, children
Methodology	• Community consultation regarding Internet issues • Fund Safer Internet Centers in European Union Nations • Pan-European content labeling and content filtering

2.5.4 Safe and Secure Online (United States)

Safe and secure online is an international cyber security awareness campaign led by (ISC)² which is a non-profit global organization having offices in London and Tokyo and headquarters in the United States.

Through this Safe and Secure Online program, the volunteers help and train the young children to remain safe online. This awareness program bridges the security gap that is present in the children’s safety outreach efforts. This program began with the support of Childnet International which is a UK based charity which has the major goal of making Internet a safer place for children [16].

Table 2.4 Safe and Secure Online

Item	**Notes**
Campaign name	(ISC)² Safe and Secure Online
Organization	(ISC)²
Main URL	http://cyberexchange.isc2.org/safe-secure.aspx
Topics covered	Broad range of topics including • Cyber predators • Spyware • Passwords • Phishing • Application and Website Security • Online shopping • Information Protection • Malware • SPAM
Target Audience	General Public
Methodology	• Provide vendor • Professors’ Gold Standard services • Career services • Presenting material not only online but also to schools • Availability of Security tools for awareness for download

2.5.5 Watch your Web (Germany)

This security awareness campaign is led by the German Federal Ministry of Family Affairs, Women, Youth and European Commission. This campaign targets general public particularly the youth to spread awareness regarding safe Internet usage [17].

Table 2.5 Watch your Web

Item	Notes
Campaign name	Watch your Web
Organization	Jugend online von IJAB
Main URL	http://www.watchyourweb.de/
Topics covered	• Threats of joining social networks • Data security • Risks of Internet browsing
Target Audience	Young generation
Methodology	• Awareness events for youth • Video clips [18] • Online tutorials • Web test [19] • Twitter service available [20]

2.5.6 Information Security Education and Awareness (ISEA) Project (India)

ISEA is another big initiative in the area under discussion. The project is being run by the Indian government. Ministry of Electronic and Information Technology (MeitY) approved this project back in 2005 titled Information Security Education and Awareness (ISEA) which was completed in 2014 and Phase II of the Project was then approved in April 2014 with a total outlay of Rs. 96.08 crore for a period of 5 years [39].

Table 2.6 ISEA India

Item	**Notes**
Campaign name	Information Security Education and Awareness (ISEA)
Organization	Ministry of Electronic and Information Technology (MeitY)
Main URL	https://www.isea-pmu.in/home/About
Topics covered	Not disclosed publicly
Target Audience	• Academic users • General users • Government users
Methodology	• Online training • Workshops

2.6 Conclusion

Security policies and procedures alone are not enough to keep an organization safe rather accompanying them with a trained workforce is a sensible approach to build a good security posture. This research has chosen academic community as a target audience owing to the fact that it’s the youth who when trained on cyber security can build a prosperous country. Cybercrimes are on the rise in Pakistan and currently there are no efforts to provide the young people enough awareness to keep them safe and secure online. This chapter has discussed various strong security awareness campaigns running worldwide that have made a difference in this field. Such awareness campaigns and programs are a must in developing countries as well in order to reduce the ratio of cybercrimes that happen every day in these countries due to lack of awareness among people.

Chapter 3

ANALYSIS OF CYBERSECURITY EFFORTS IN THE ACADEMIC COMMUNITY OF PAKISTAN

3.1 Introduction

This chapter presents the analysis of current efforts being made in the domain of IT/cyber security in/by the academic community. The survey has been conducted via the questionnaires and interviews with the management and authority involved in the IT/technical domain. The basic purpose of this survey section is to assess the 'sense' of security that the institutes' concerned authorities have and the extent to which they are catching up with the latest security trends.

3.2 Objective of this survey

The objective of this particular survey is to analyze the current efforts that are being put in the academia sector by the management for the enhancement of their security posture. This analysis has identified the gap between the current level of awareness and the required level of awareness.

3.3 Survey methodology

The survey has been conducted in 12 universities of different sizes in Pakistan that have been divided into categories of small, medium and large for some sections to differentiate the survey results. The categories of universities are on the basis of the number of disciplines they offer, size and the number of cities they are expanded in. The 4 large universities are the top universities in the country and are expanded i.e. have their campuses in different cities. The 4 medium universities are the ones that are renowned, have a good mark but are not very expanded i.e. do not have their campuses in all major cities. The 4 small universities are beginner level private universities that are small in every aspect. The names of the universities have been kept anonymous for privacy purpose. The results are presented in graphs and tables and the values are average of the answers of the universities. (Appendix-A)

3.4 Survey format

The survey has been conducted to assess following areas:

- Security positions/roles
- Security policies
- Hacks, attacks and flaws
- Security threats
- Organizational security
- Physical security
- Digital security
- Assets and threats

3.5 Security Positions

Table 3.1 presents a comprehensive list of IT/ security roles that are being introduced worldwide. The survey audiences were asked to check mark the roles that are currently functional in their departments or the ones that are required to be put in action. The unchecked roles are considered neither functional nor required. The final results are the answers from the majority. In most of the institutes, the multiple roles are being performed by the same individual due to lack of resources. The training modules presented in this research includes modules for all the roles; roles that are currently functional in the academia sector, roles that are required and the roles that are proposed.

Table 3.1 Security Positions

Position	Status		Position	Status	
	Present	Required		Present	Required
Database Administrator	□	✓	Security Training Coordinator	□	✓
Data Manager	□	✓	Information Security Policy Analyst	□	✓
Database Developer	□	✓	Policy writer and Strategist	□	□
Information Dissemination Manager	□	□	Information security Policy Manager	□	✓
Network Administrator	✓	□	Network Engineer	□	□

CND Specialist	□	□	Cybersecurity Intelligence Analyst	□	□
Network Analyst	✓	□	Defense Technician (Network)	□	✓
SystemsAnalyst	✓	□	Network Security Engineer	✓	□
Telecommunications Engineer/Personnel/ Specialist	✓	□	Security Operator	✓	□
Local Area Network (LAN) Administrator	✓	□	Cyber Crime Investigator	□	□
Security Administrator	✓	□	Incident responder	□	✓
Server Administrator	✓	□	Incident Response Analyst	□	✓
Systems Administrator	✓	□	Blue Team Technician	□	□
Website Administrator	✓	□	Ethical Hacker	□	□
Computer Programmer	✓	□	Penetration Tester	□	□
Research & Development Engineer	✓	□	Red Team Technician	□	□
Software Developer	✓	□	Reverse Engineer	□	□
Web Application Developer	✓	□	Risk/Vulnerability Analyst	□	✓
Firewall Engineer	✓	□	Vulnerability Manager	□	✓
Systems Engineer	✓	□	Computer Forensic Analyst	□	✓
Security Engineer	✓	□	Digital Forensic Examiner	□	□
Information Assurance (IA) Developer	□	□	Digital Media Collector	□	□
Cyber Trainer	□	✓	Forensic Analyst	□	✓
Information Security Trainer	□	✓	Computer Crime Investigator	□	✓

3.6 Security Policies

This section includes questions about the policies and procedures that the institutes have in place. The purpose is to collect information about the number of IT employees the respective institutes have, their minimum qualification, the institutes that provide training to the employees, reasons of not providing the required training, institutes that provide security certifications and frequency of risk and vulnerability assessment of the critical assets of the organizations. On the y-axis is the number of institutes and on the x-axis is the required information against the institutes. The required information has been separated for all three categories of institutes because of the difference in the maturity of their IT infrastructures.

Figure 3.1 gives the stats of the number of IT employees the institutes have. The four large universities have an average of 25 IT employees, medium have 18 and the four small universities have an average number of 12 IT employees. These include only those employees that have strictly IT related responsibilities.

(Note: N/A corresponds to 'Not attempted')

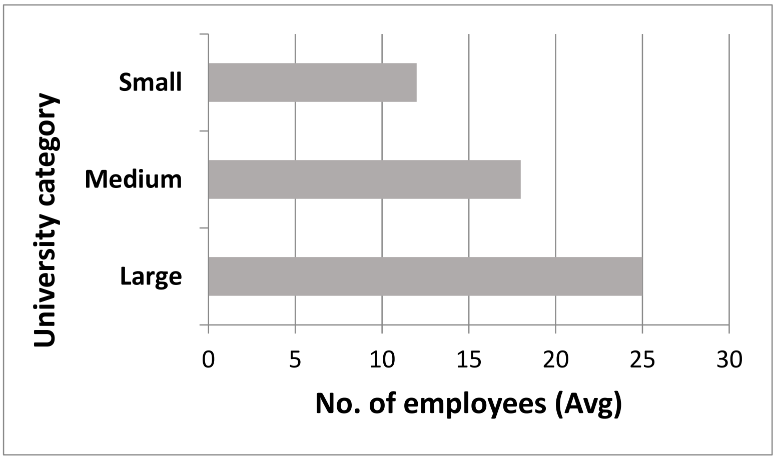


Figure 3.1 Number of employees having IT related responsibilities

Figure 3.2 shows stats of the minimum qualification these employees have. 2 large universities have MS as minumum qualification for IT employees, 1 medium university has MS as minimum qualification and all small universities have BS as munimum qualification.

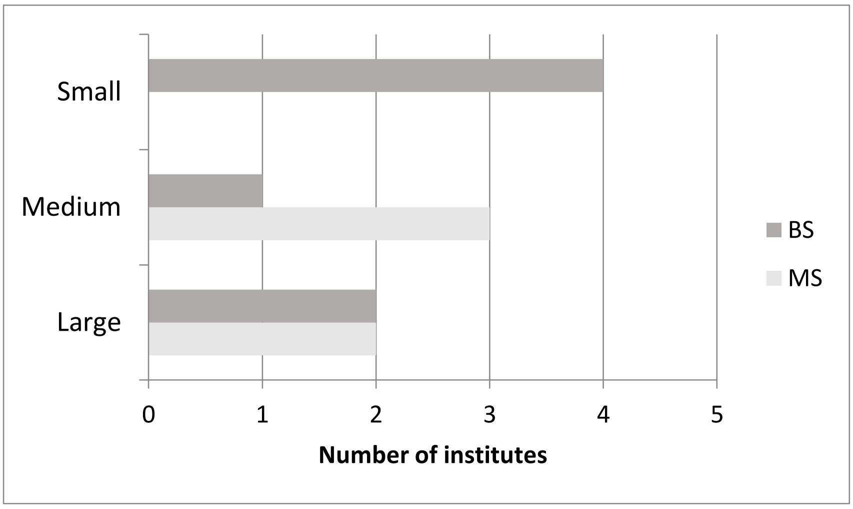


Figure 3.2 Minimum qualifications of employees

Figure 3.3 shows stats of the institutes that provide IT training to their employees. Ironically, none of the small universities provide proper IT training to their employees.

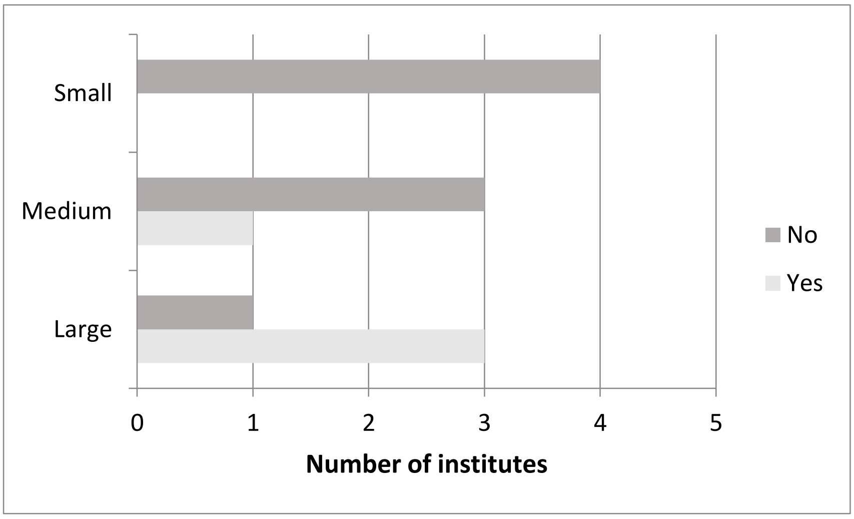


Figure 3.3 Number of institutes that provide training to the employees

Figure 3.4 shows stats giving reasons shared by universities for not providing the required training to their IT employees. 7 institutes chose reason of insufficient funding and 1 university chose reason of insufficient time. Rest of the institutes however did not share any reasons.

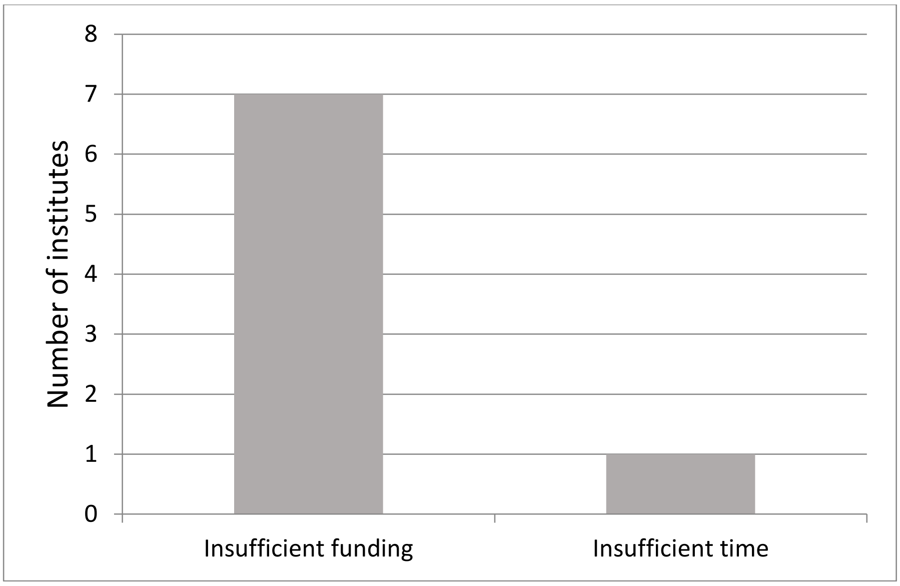


Figure 3.4 Reason of not providing appropriate training

Figure 3.5 shows stats of the basis of how institutes provide training to their employees. 4 institutes provide need based training, 6 institutes provide training to approximately 50% of employees on priority basis and 2 institutes claimed of providing training to all the employees.

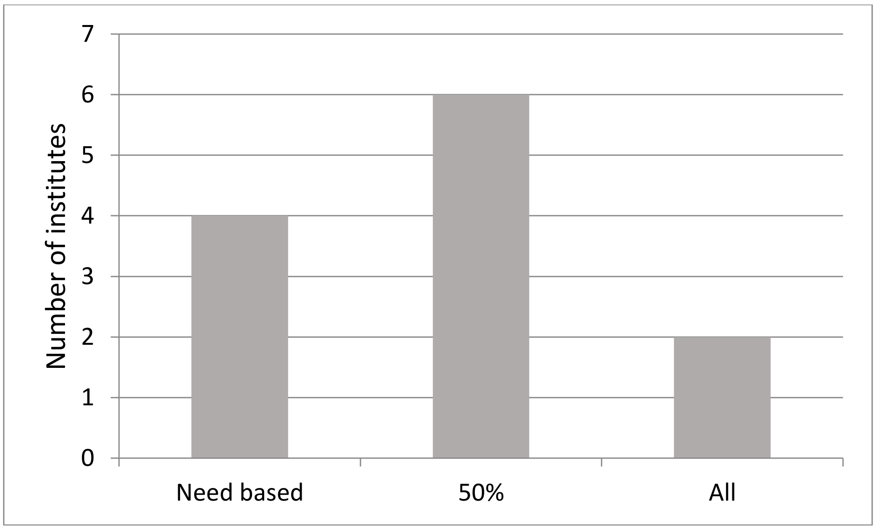


Figure 3.5 Number of employees having IT related responsibilities that have received the required training .

11 of the institutes surveyed were not found to be providing any security certifications to the employees. 1 institute claimed to do so.

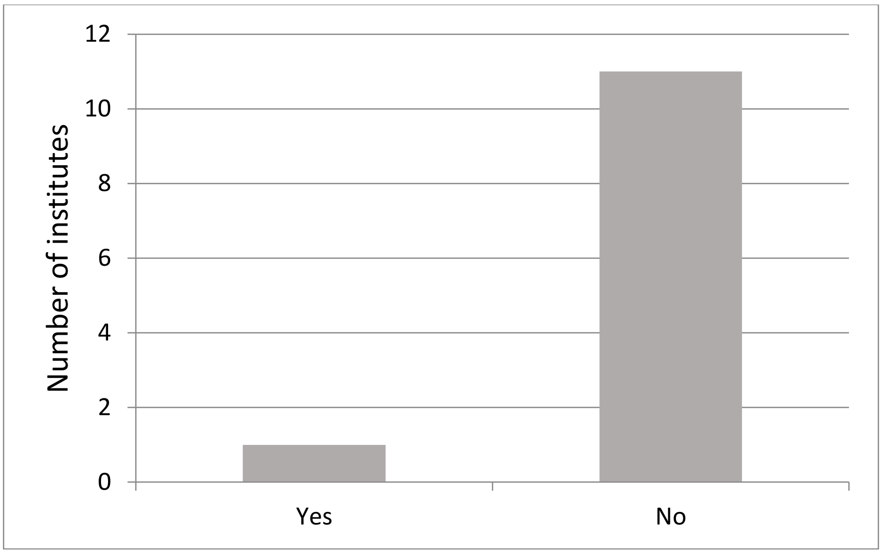


Figure 3.6 Number of institutes that provide security certifications

None of the institutes were found to be incorporating policy of ‘separation of duties’. Alarmingly, some of the people interviewed were not even familiar with the said term.

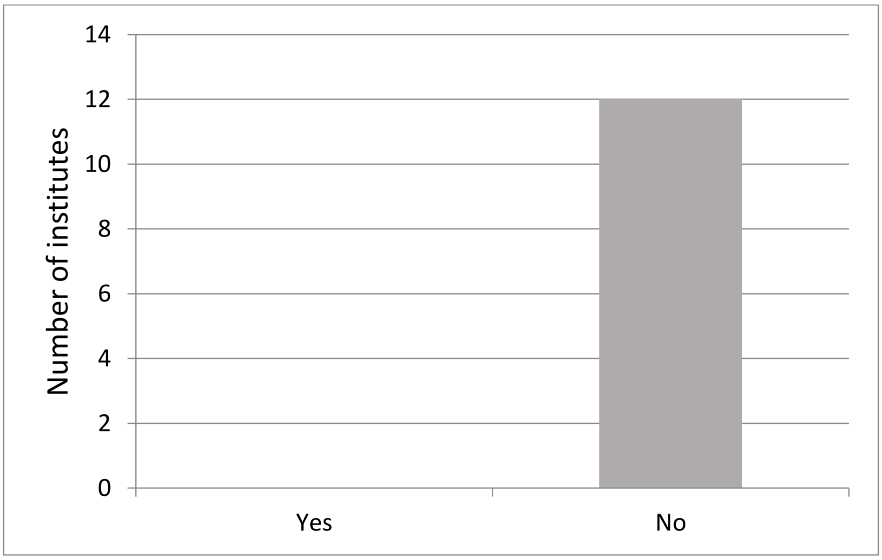


Figure 3.7 Number of institutes that have the policy of ‘separation of duties’

Figure 3.8 and 3.9 show stats of the frequency of conducting risk and vulnerability assets of the critical assets of the institute. Alarmingly, most of the institutes do not have a proper policy of conducting risk and vulnerability assessment of the critical assets.

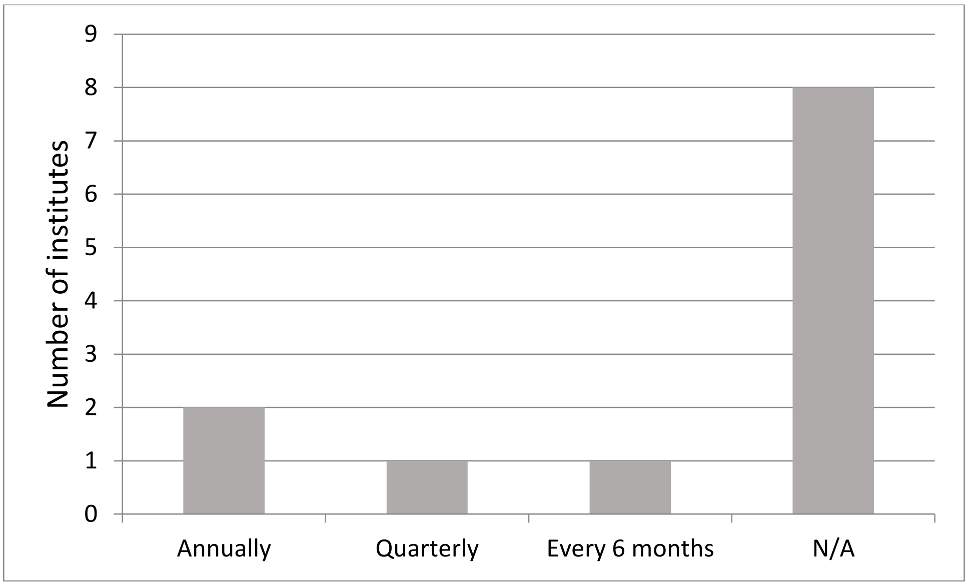


Figure 3.8 Frequency of risk assessment of the critical assets of the organization

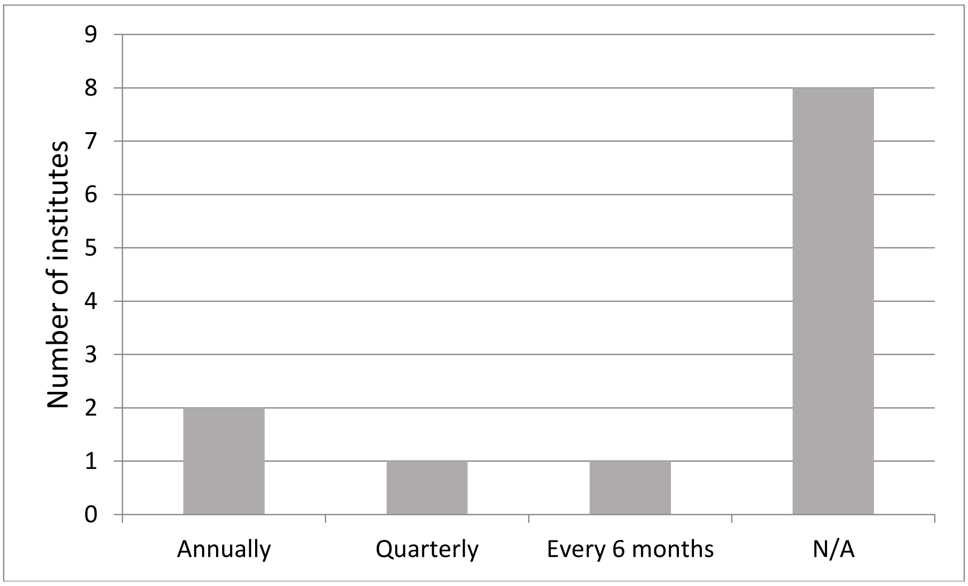


Figure 3.9 Frequency of vulnerability assessment of the critical assets of the organization

3.7 Hacks, Attacks and Flaws

This section aims at collecting the information about the overall threat environment of the organizations. It focuses on gathering information about the threat factors that exploited the institute in the previous two years and the types of attacks that these institutes have faced lately. 4 institutes chose 'non-malicious' insiders as the threat factor they faced in years 2014 and 2015. 7 chose 'none' and 1 chose 'malicious insiders', as shown in figure 3.10.

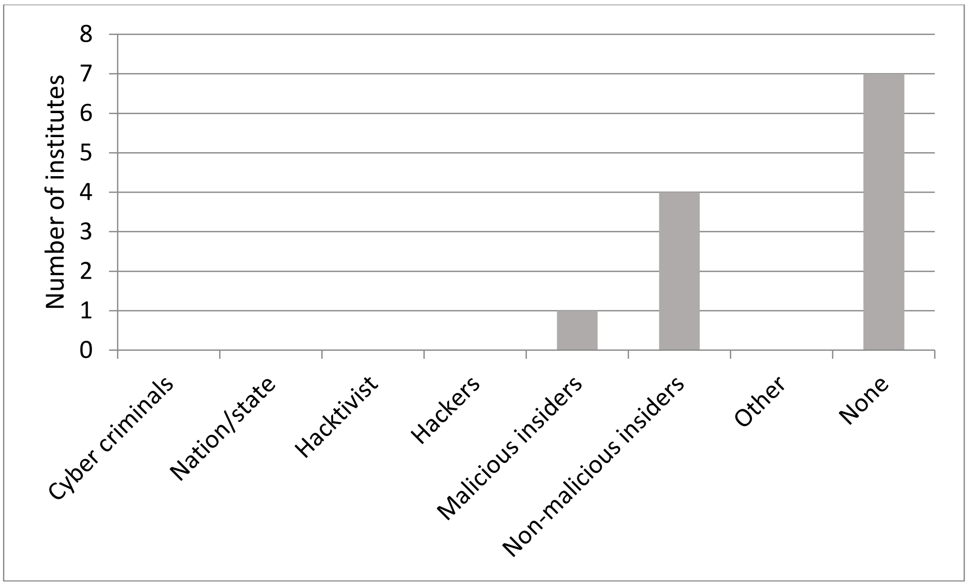


Figure 3.10 Threat factors that exploited the institutes in 2014 and 2015

Figure 3.11 shows the stats about the attack types that the institutes faced in previous two years. 11 institutes chose 'Malware' and 9 chose 'Loss of mobile phones'. The remaining stats are given in figure 3.11. *(Note: Institutes could choose more than one attack types').*

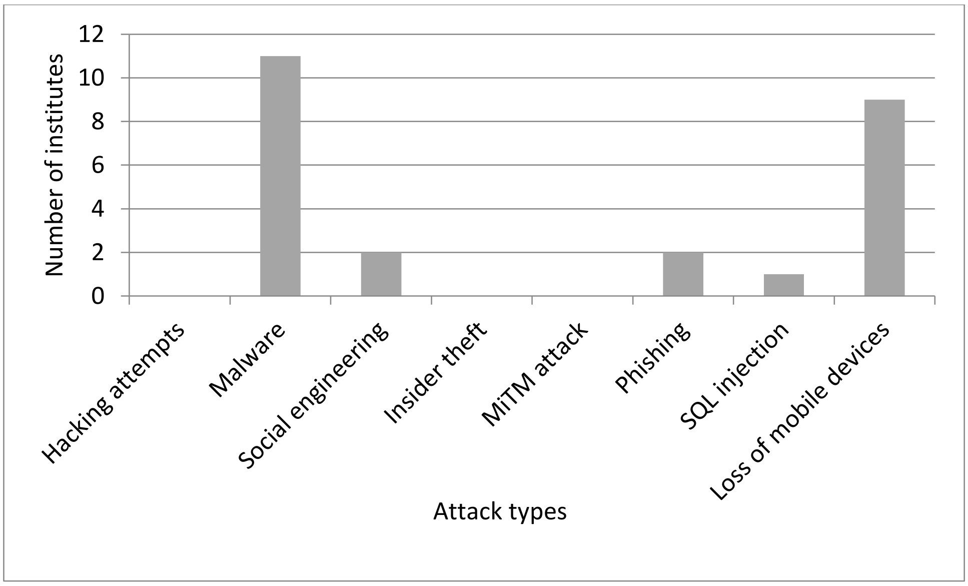


Figure 3.11 Attack types that exploited the institutes in 2014 and 2015

3.8 Security Threats

This section aims at collecting specifically threat related information like increase or decrease in the attacks, the motivation behind the attack as per the assessment of the organization and loss of the physical assets that they have faced.

Figure 3.12 shows that out of total 12, 4 institutes experienced increase in attacks (more attacks) from the previous year, 6 chose fewer attacks i.e. experienced decrease in attacks from the previous year, 1 institute left the question unanswered.

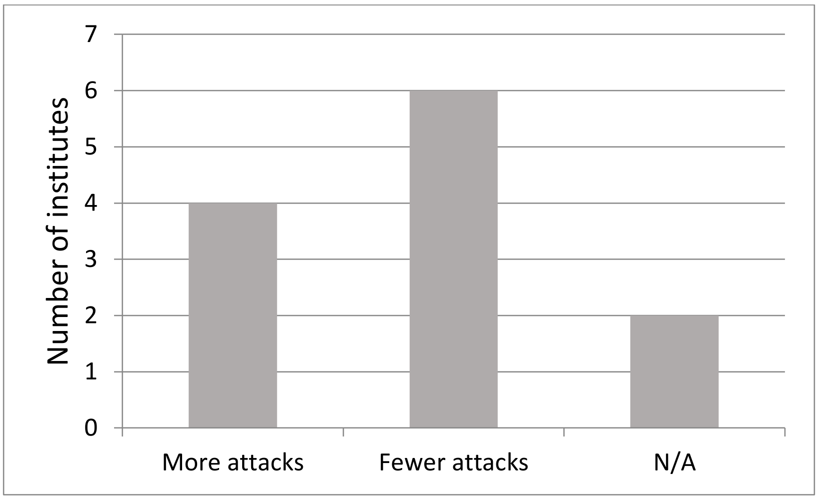


Figure 3.12 Increase or decrease in security attacks as compared to previous year?

Figure 3.13 shows the stats about incidents' motivation according to different institutes. Note that all the institutes chose 'Theft of personally identifiable information', 11 chose 'Intellectual property gain' and 10 chose 'Theft of classified data. The details are shared in Figure 3.13

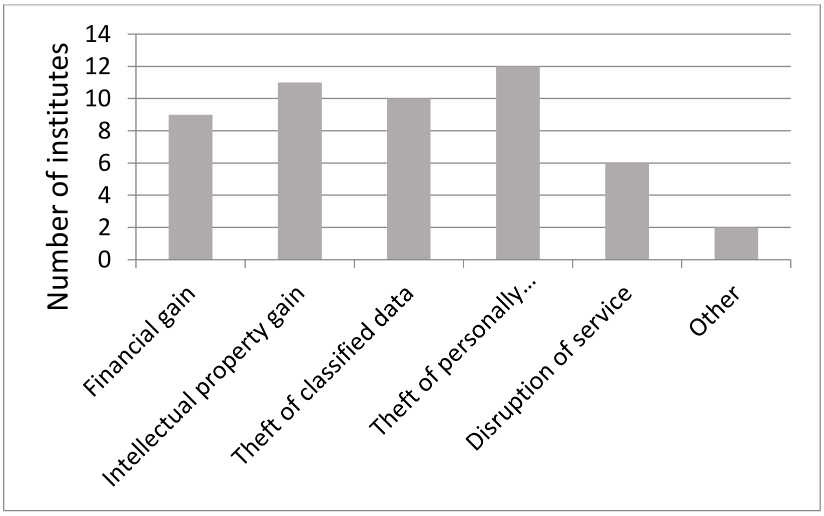


Figure 3.13 Incident motivations according to different institutes

Figure 3.14 shows that 3 institutes chose 'Mobile devices' as among the loss of physical assets faced by the institute. 9 chose not to answer.

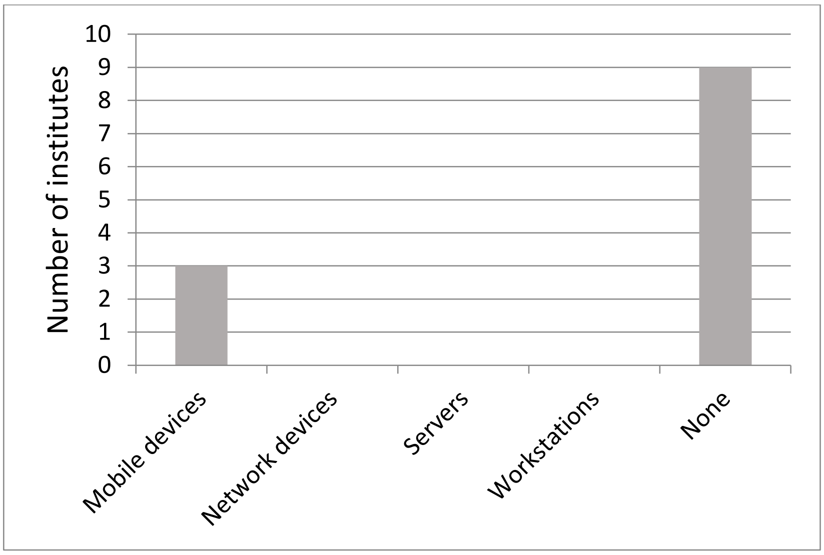


Figure 3.14 Loss of physical assets

3.9 Organizational Security

This section focuses on information gathering related to security efforts at an organizational level i.e. the efforts put in by the senior management to put proper security measures in place.

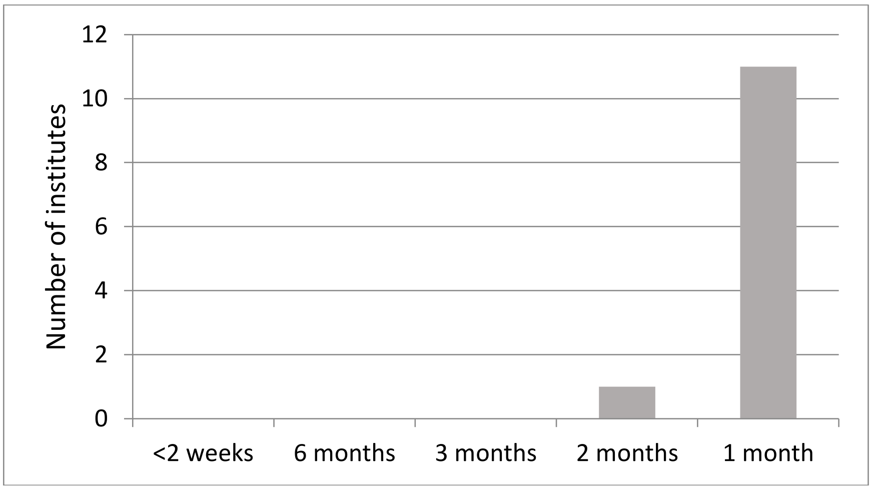


Figure 3.15 How long does it take to fill a security position on average

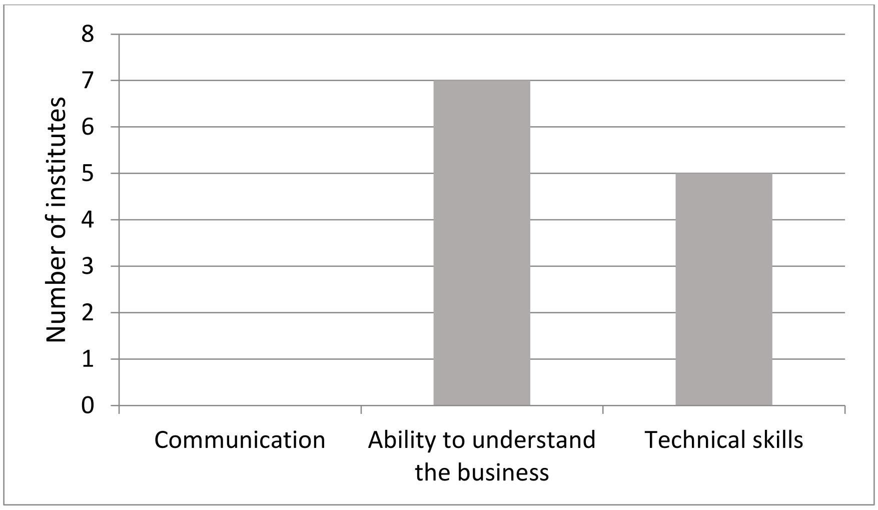


Figure 3.16 Biggest skill gap in today's security professionals

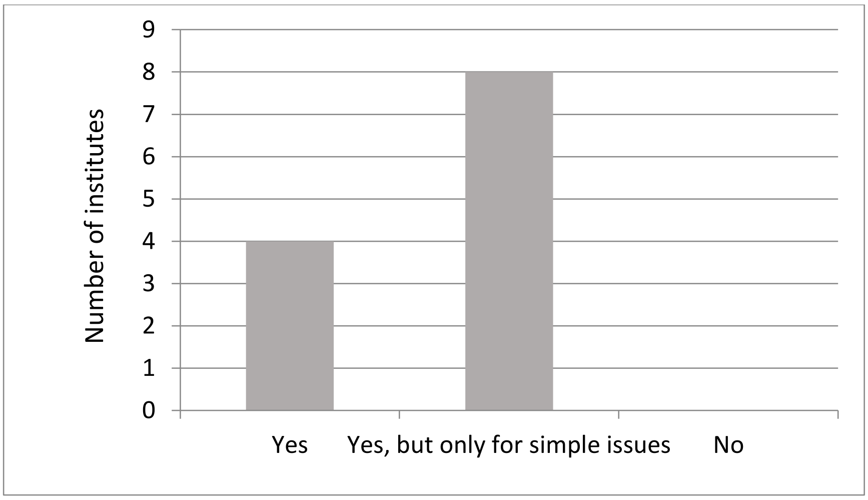


Figure 3.17 Satisfied with security team's ability to detect and respond to incidents?

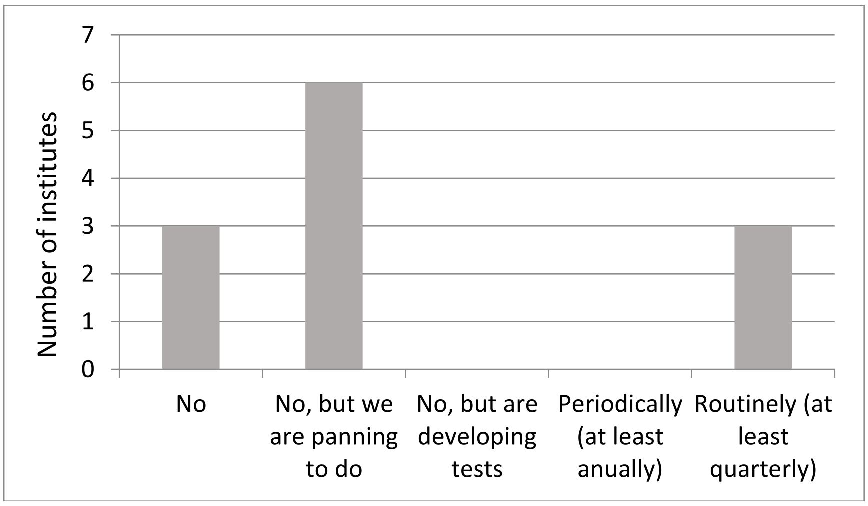


Figure 3.18 Are security controls tested?

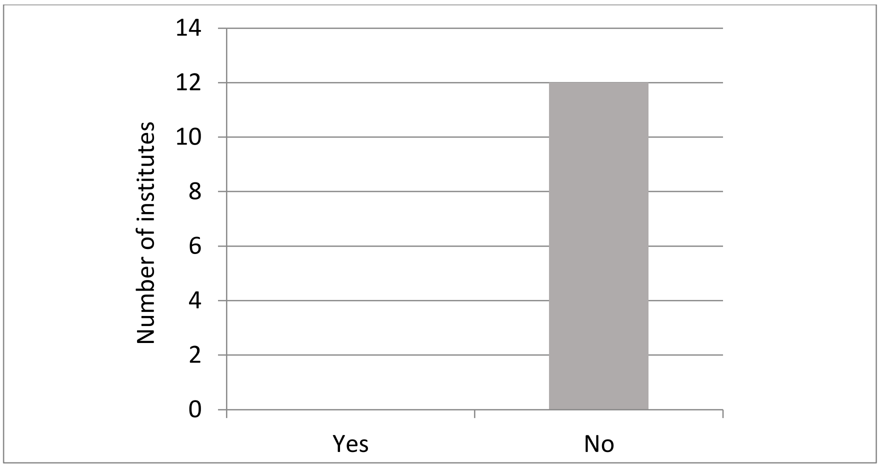


Figure 3.19 Any security awareness program in place?

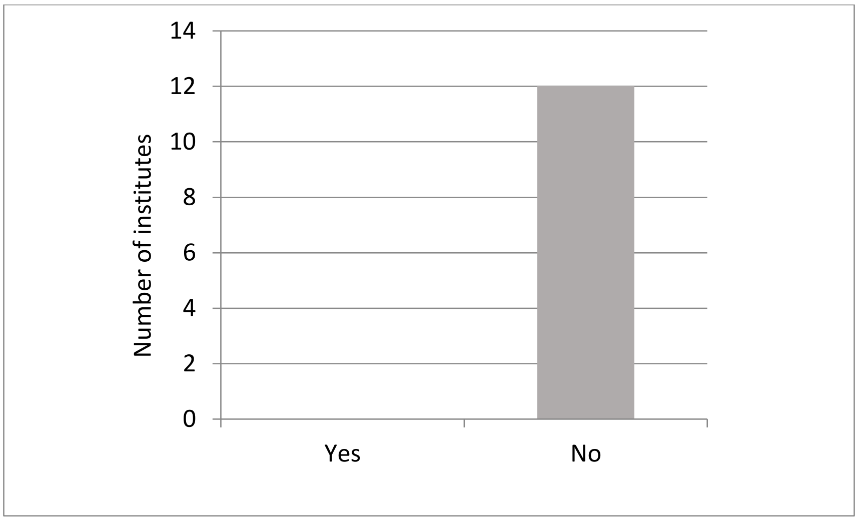


Figure 3.20 Any computer crime investigation cell in the institute?

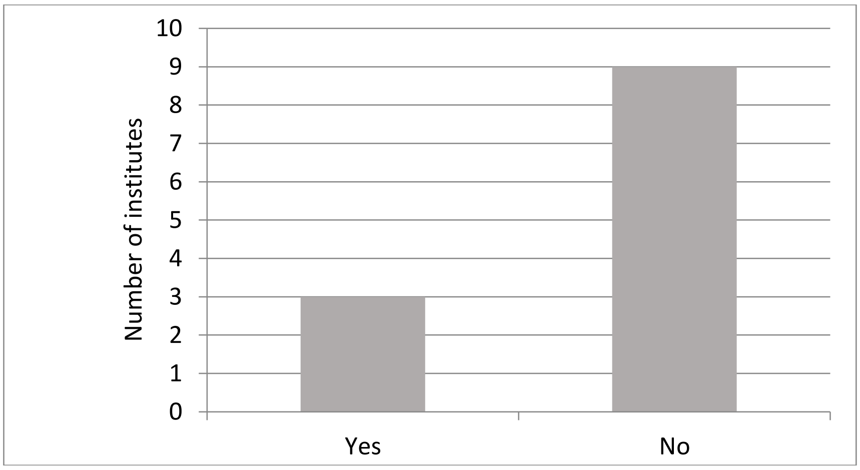


Figure 3.21 Any CSIRT (Computer security Incident response team) set up?

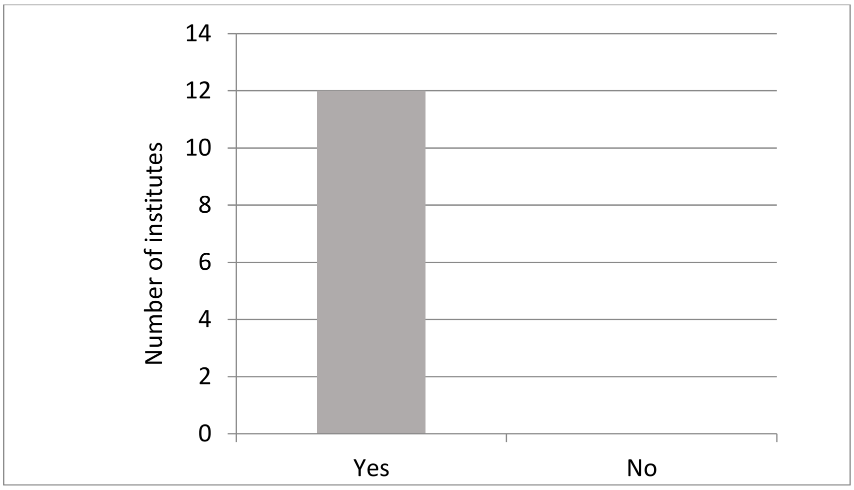


Figure 3.22 Senior management concerned with security

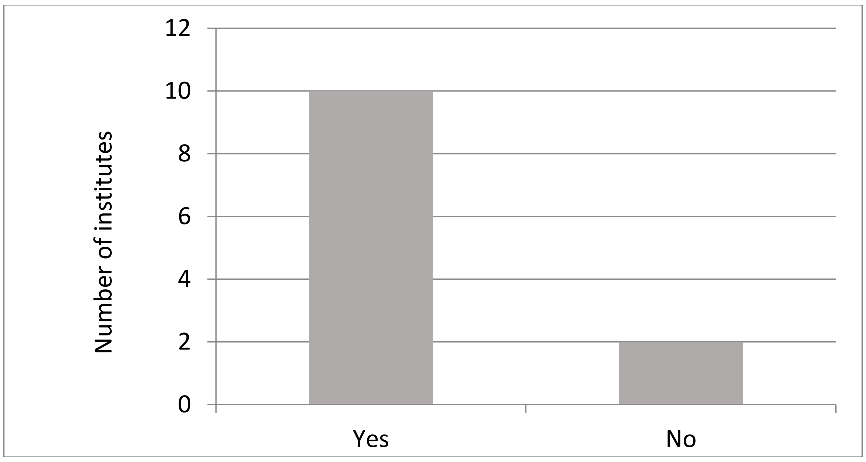


Figure 3.23 Restricted access to social media

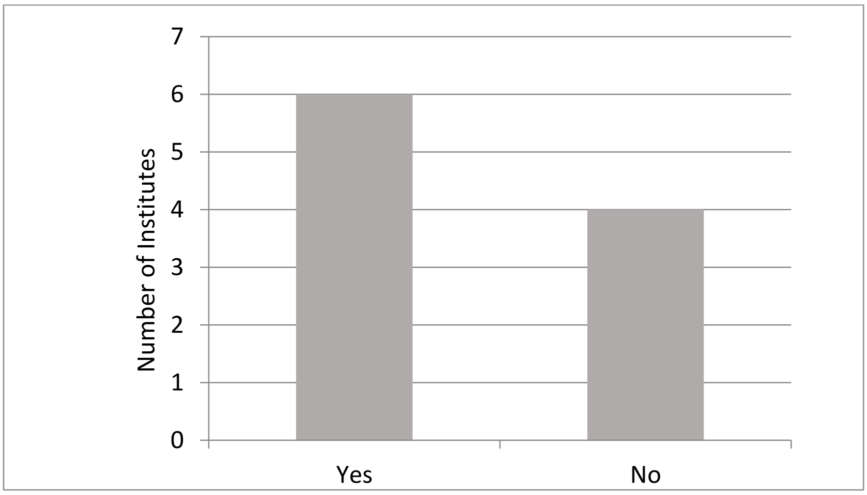


Figure 3.24 Are records kept of which employees have significant security responsibilities?

3.10 Physical security

This section aims at collecting information related to the measures taken by the institutes for the physical security of the IT assets. For instance, all the institutes surveyed claimed to have proper safeguarding of the server rooms. 11 claimed to give access of server rooms only to authorized people. All the institutes claimed of securing physical documents properly. None of the institutes provide separate badges to the authorized personnel for physical access to IT assets. None of the institutes were found to be maintaining password files in hard copy; they all claimed to be maintaining them in soft copies.

Table 3.2 Stats of physical security measures

Measures	**Number of institutes**		
	Yes	**No**	**N/A**
Are doors to the server rooms and computer spaces locked and guarded?	12	0	0
Do only authorized people have access to the server rooms?	11	1	0
How have you secured sensitive physical documents?	12	0	0
Have you provided the employees with separate badges to ensure authorization?	0	9	3
How have you maintained physical password files?	0	12	0

3.11 Digital security

This section aims at collecting information regarding measures for digital security of the IT assets. For instance, all the institutes claimed of proper installation and updating of the anti-virus solutions. Only 2 institutes incorporate policy of two-factor authentication.

Table 3.3 Stats of digital security measures

Measures	Number of institutes		
	Yes	No	N/A
Are anti-viruses installed on all systems?	12	0	0
Are they updated regularly?	12	0	0
Are anti-spyware installed on all systems?	2	7	3
Is logging activated on the systems?	3	6	3
Is Two-factor authentication enabled?	2	8	2

3.12 Assets and Threats

Figure 3.25 and 4.26 shows the stats of responses shared by the institutes regarding assets and threats according to their assessment. Institute's official website and learning management systems are most critical assets according to most institutes and security unawareness is the most critical threat.

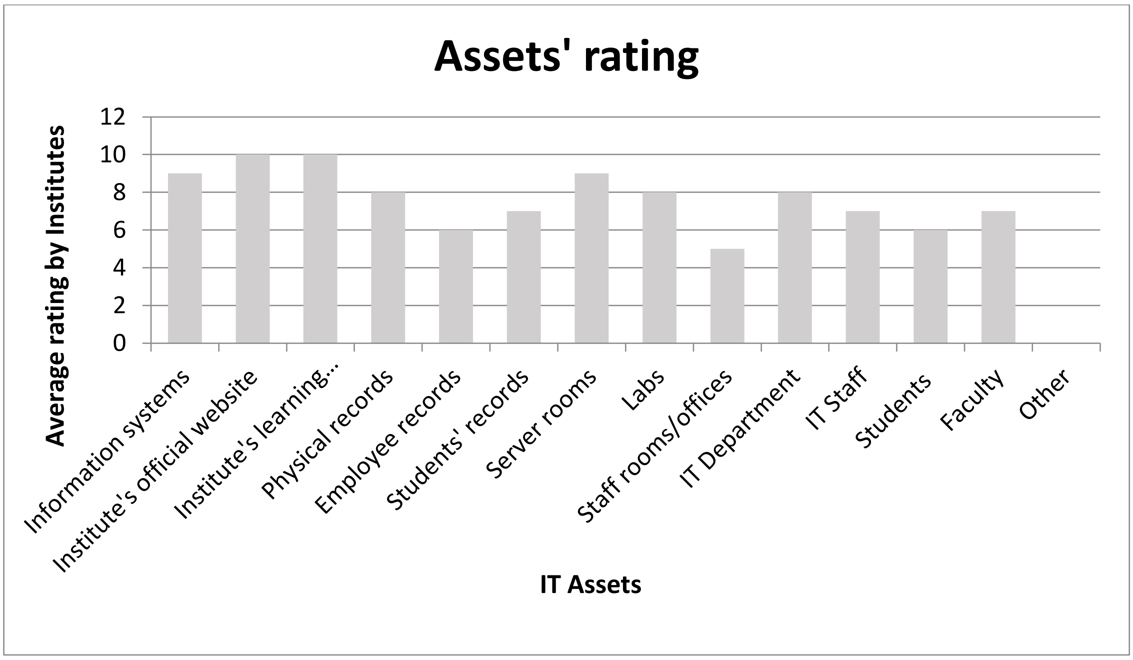


Figure 3.25 Rating of critical assets of the institute

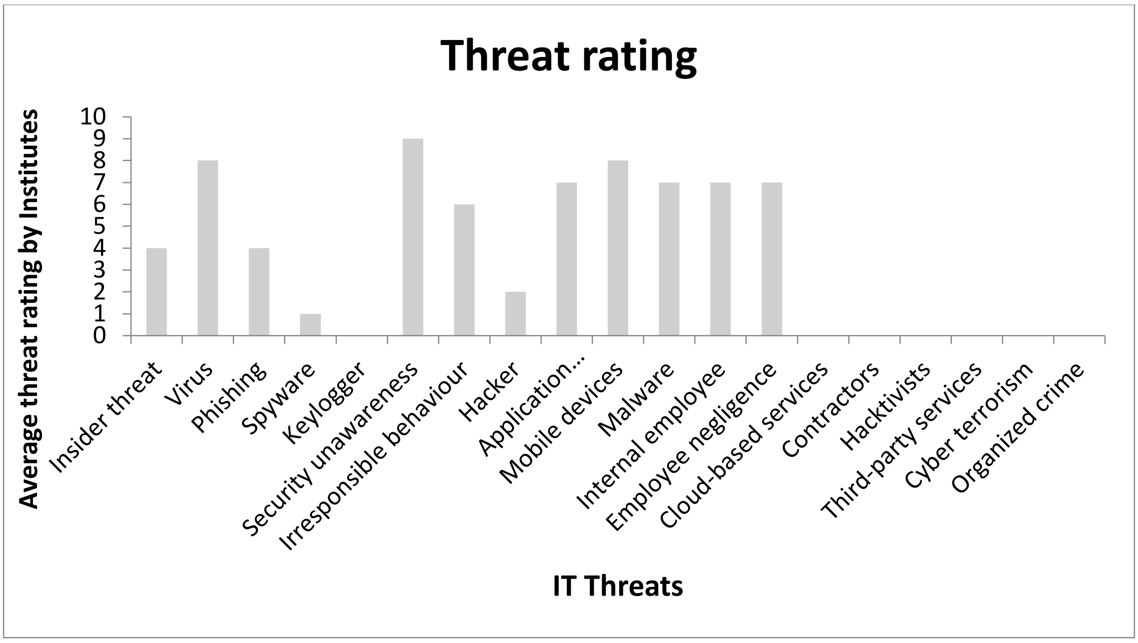


Figure 3.26 Rating of major threats faced by the institutes

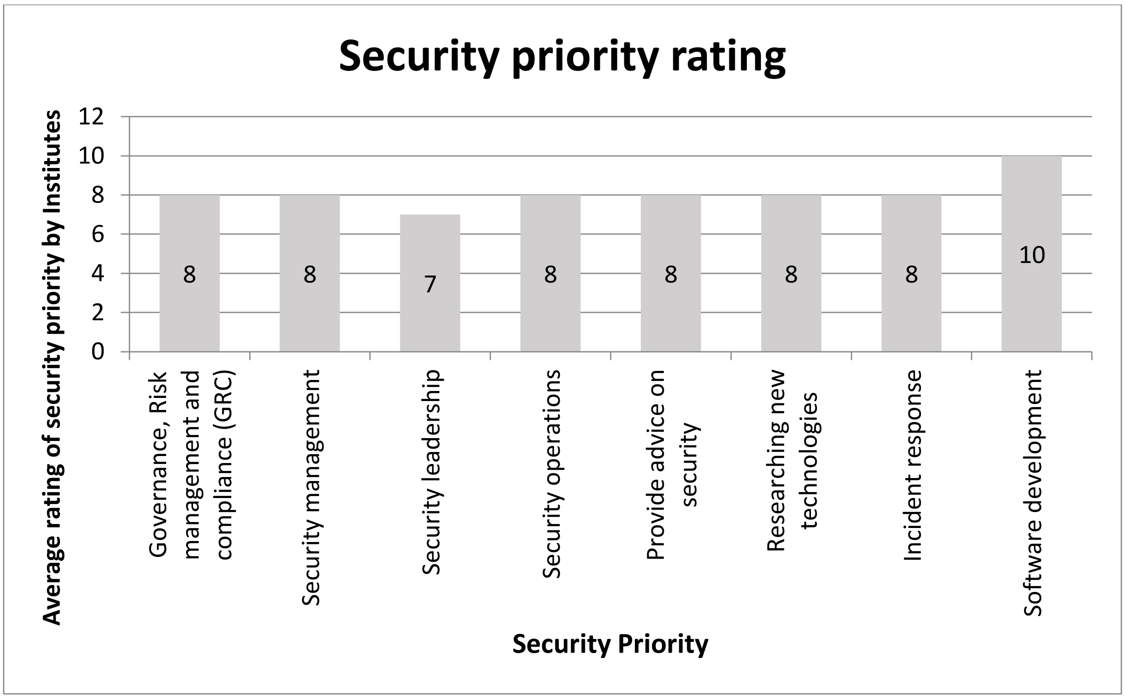


Figure 3.27 Rating of security priorities of the institute

3.13 Survey Analysis

The security posture for six security categories has been devised from the survey conducted, as shown in Table 3.4. The reasons behind the conclusion for each category are given as under:

(Note: The analysis below is presented as aggregate from the responses of total 12 institutes; the exact stats have been shared in Sections 3.6 - 3.11).

Security Policies: Weak security policies have been observed throughout, most institutes do not provide training/certifications to the employees, there is no policy of 'separation of duties', most institutes do not conduct risk and vulnerability assessments of their critical assets. The overall security posture has been found to be weak.

Hacks, attacks and flaws: The threat factors faced by the institutes include only malicious and non-malicious insiders. The attack types include malware, loss of mobile phones and social engineering. The overall security posture has been found to be medium.

Security Threats: Most institutes experienced fewer attacks as compared to the previous year. Loss of physical assets only included 'Mobile phones'. The overall security posture has been found to be medium.

Organizational security: Most institutes chose 'Ability to understand the business' and 'Technical skills' as the biggest skill gaps in information security. Security controls are not tested regularly by most institutes. There are no security awareness programs in place. None of the institutes have any crime cell. Only 2 institutes indicated that they have a CSIRT (Computer and Security Incident response team) in place. The overall security posture has been found to be weak.

Physical security: All institutes allow only authorized individuals into the server rooms. Physical documents are properly secured. None of the institutes have authorization badges for employees. No password files are maintained. The overall security posture has been found to be medium.

Digital security: All institutes indicated that they have updated anti- virus. Logging is not enabled on all the systems. Only 2 institutes have Two-factor authentication enabled. The overall security posture has been found to be Weak.

Table 3.4 Overall Security Posture

Security Category	**Security Posture**
Security Policies	Weak
Hacks, attacks and flaws	Medium
Security Threats	Medium
Organizational security	Weak
Physical security	Medium
Digital security	Weak

3.14 Conclusion

This chapter highlighted the overall security posture of the academic institutes in the country, the security measures that they have in place and the efforts being planned. The survey has been conducted keeping in mind all the dimensions of security including hacks, attacks and flaws faced by the institutes, security threats, security policies, physical security, digital security and organizational security. The overall security posture has been found to be weak and there still seems to be a long way to go in order to attain a better and acceptable state of security in these institutes.

Chapter 4

ANALYSIS OF CYBERSECURITY AWARENESS LEVEL OF GENERAL USERS IN THE ACADEMIC COMMUNITY OF PAKISTAN

4.1 Introduction

This chapter aims to assess the overall awareness level of the category ‘general users’ in ten different domains of cyber security. The awareness levels are assessed in these ten domains against three dimensions namely; ‘*knowledge*’, ‘*attitude*’ and ‘*behavior*’ (KAB Model). The purpose is to analyze the IT habits of the users, their level of security consciousness, their awareness level of the technology and its threats, their level of cautiousness while interacting with Internet and to assess their general attitude towards IT security. The survey has revealed some alarming facts which yet again strengthen the purpose of this research. The overall awareness level of the users has been found to be ‘Low’ and hence risk level ‘High’. This is the risk that comes in due to lack of awareness of the users regarding IT security in addition to the risk that is posed by the attacks and threats by the technology itself.

4.2 Survey methodology for general users

The survey for the general users i.e. students, faculty and staff members has been divided into ten cyber domains. The survey that includes questionnaires and interviews has been manually performed in six Pakistani universities that are all HEC (Higher Education Commission) recognized. The universities’ names have been kept anonymous for the privacy purpose. A total of over 1000 users from both technical and non-technical backgrounds were part of the survey. The survey has been analyzed on the basis of the assumption that the questionnaires were read carefully and the questions were answered with maximum accuracy possible. The results of the questionnaire based survey were justified by conducting interviews with the users randomly. The survey questionnaire is in Appendix B.

4.2.1 Cyber domains for survey

The ten cyber domains that were used to analyze normal IT habits of the users and their awareness in the corresponding area are as under. These domains are chosen according to SANS standard of Users Information Security Training ‘Securing the Human’. These domains are an outline to broadly cover the awareness level and IT habits of the users from all angles.

- General awareness
- Attacks and threats
- Email and communication
- General security
- Mobile devices
- Privacy
- Safe browsing
- Software and applications
- Social networking
- Internet Usage

4.2.2 Dimensions of assessment – Knowledge, Attitude and Behavior (KAB) Model

In a dynamic learning environment, different users with different levels of knowledge behave differently and possess different attitudes. The concept that the complex aspects of teaching or learning does not directly corresponds to a single outcome measure is not a new one. Bloom started the development instructional objectives' taxonomy in three domains—the cognitive, affective, and psychomotor back in 1956, indicating the old age of this concept. Alexander then found strong relation between the cognitive and affective attributes of the learner and their relative impact on the comprehension and absorption of information [48]. Owing to these old, successful and still in practice theories, thus survey has incorporated KAB model in order to assess the users' awareness in all three dimensions. The awareness levels were measured against all ten areas in three dimensions; knowledge, attitude and behavior.

1) **Knowledge:** This dimension corresponds to 'what a person knows'. E.g. In the area 'Attacks and threats', to assess the user's knowledge included questions like 'How much do you know about USB threats' and users shared responses with 'Low', 'Medium' and 'High' in terms of awareness. The answer 'Low' corresponds to low awareness level.

2) **Attitude**: Attitude refers to 'how does the user feel about something'. E.g. In the category 'Email and Communication', the questions like 'How important do you think scanning the document is before downloading'. The responses were converted into corresponding Low, Medium and High awareness levels. The answer 'High' (very important) corresponds to 'High awareness level and vice versa.

3) **Behavior:** This dimension refers to 'how does the user behave towards a particular situation'. E.g. In the category 'General security', questions like 'How often do you connect to Public Wi-Fi network' were included. The responses were converted into corresponding awareness levels. The answer 'low' corresponds to 'High' awareness level and vice versa.

TABLE 4.1 SAMPLE QUESTIONS

Dimension	**Category**	**Sample question**
Knowledge	Attacks and threats'	How much do you know about online frauds?
Attitude	Email and Communication	How cautious are you of revealing personal information in email.
Behavior	General Security	How often do you back up your data?

4.2.3 Awareness rating scale

The three point scale *'Low'*, *'Medium'*, *'High'* has been chosen to rate the levels of awareness in all the domains individually.

Table 4.2 Scale conventions for Risk analysis

Rating	**In terms of use**	**In terms of awareness**
Low	No or rarely	Not aware at all
Medium	Sometimes or often	Aware to some extent
High	Very often or always	Total aware

4.3 Survey results for the general users

This section consists of the survey results for the general users. Each of the ten domains has been broken down into different questions and concerns related to security knowledge, attitude and behavior. The users' daily IT habits and level of security consciousness/awareness has been assessed on the basis of these results.

(Note: N/A corresponds to 'Not attempted')

4.3.1 General awareness

This section aims to assess the overall general awareness of the users regarding cyber security and how eager they are to know about and get trained on cyber security. More interest of users in cyber security is considered proportional to more security consciousness in everyday life. The assessment has been made in three dimensions; knowledge, attitude and behavior.

4.3.1.1 Dimension: Knowledge

The results in this dimension are somewhat alarming. A total of 2% of the users chose ‘High’ scale to grade general awareness level on cyber security, 80% chose low and 18% chose ‘Medium’. The users who chose ‘High’ were found to be from IT backgrounds and showed their keen interest in the field.

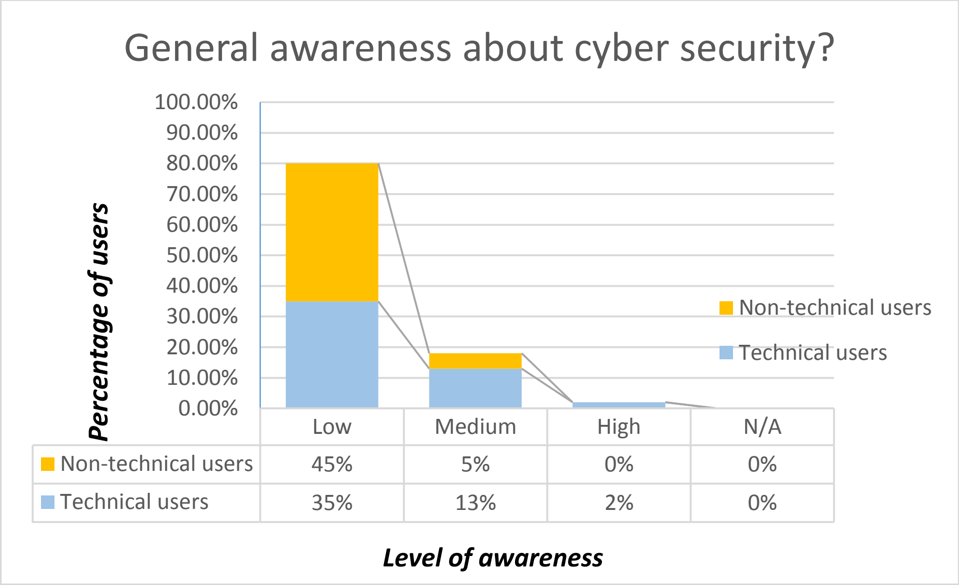
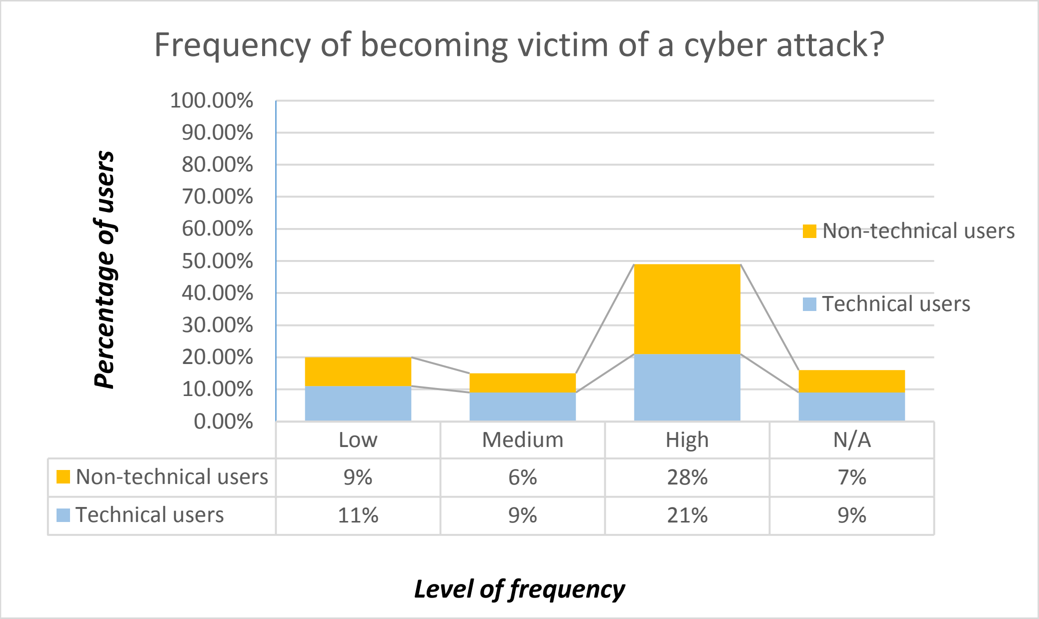


Figure 4.1: General awareness level of cyber security awareness of users

The users were asked how often they had become victim to a cyber-attack which includes malware infection, system compromise and account hacking etc. 49% of the users chose ‘High’ scale meaning that their frequency of facing a cyber-attack had been high. 20% chose ‘Low’ meaning that they had very rarely become a victim of cyber-attack. 15% chose ‘Medium’ and 16% users chose not to attempt this question (N/A).

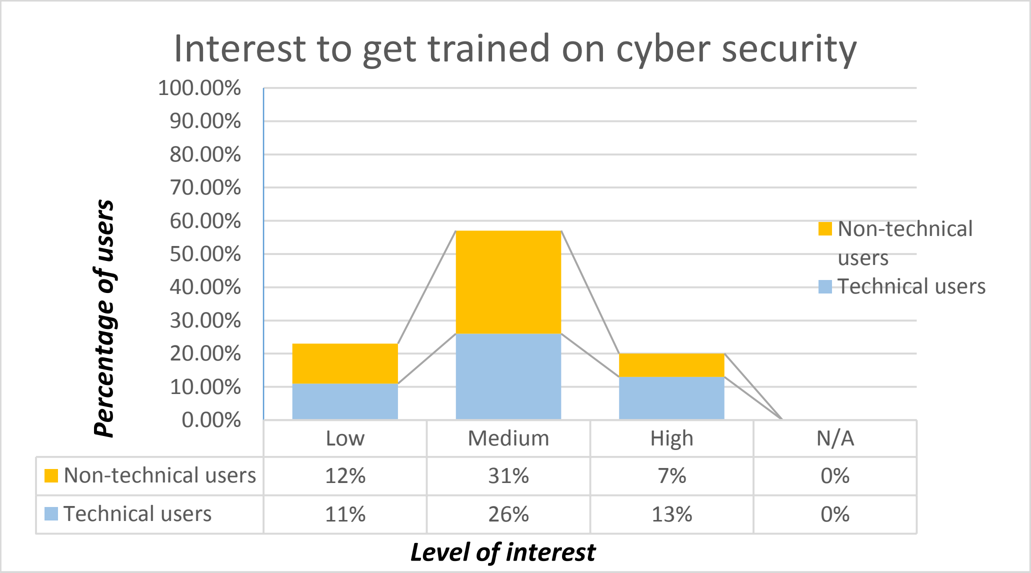


	Low	Medium	High	N/A
Non-technical users	9%	6%	28%	7%
Technical users	11%	9%	21%	9%

Figure 4.2: Frequency level of cyber-attacks in users

4.3.1.2 Dimension: Attitude

Figure 4.4 shows the stats showing the level of interest of the users to get trained on cyber security i.e. their attitude towards security. 23% of the users honestly showing ‘Low’ level of interest here in this regard show that they do not realize the threats that the daily use of technology brings to them.



	Low	Medium	High	N/A
Non-technical users	12%	31%	7%	0%
Technical users	11%	26%	13%	0%

Figure 4.3: Level of interest of users in cyber security

4.3.1.3 Dimension: Behavior

23% users chose ‘Low’ level of security consciousness, 59% chose ‘Medium’ and 18% chose ‘High’ level of security consciousness. Security consciousness here refers to the level of cautiousness and carefulness the users show while interacting with technology.

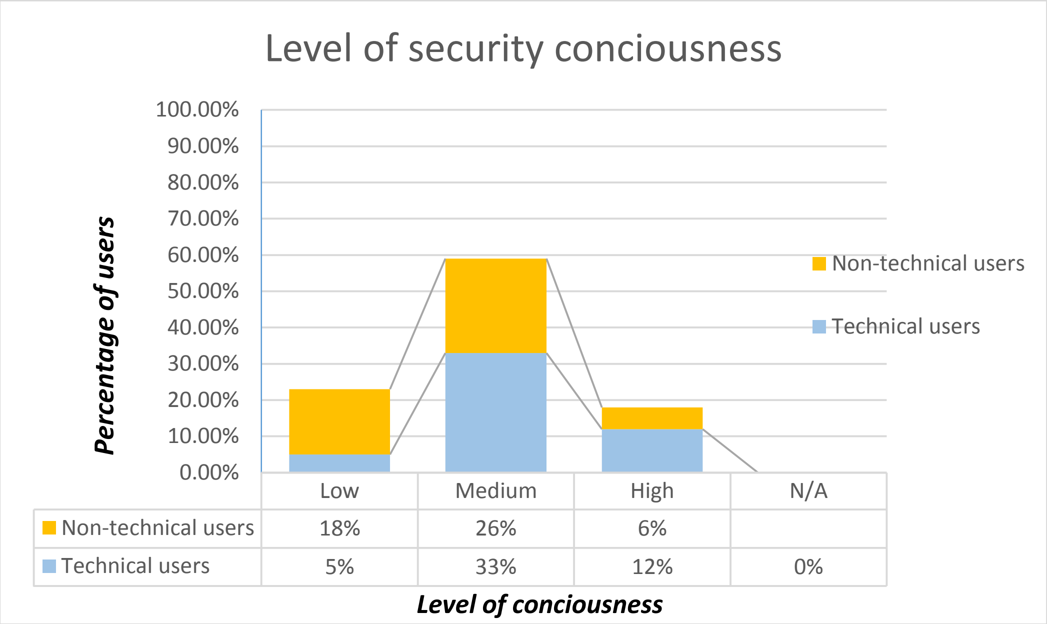


Figure 4.4: Level of security consciousness of users

4.3.2 Attacks and threats

This section focuses on the questions and concerns related to the threats and attacks of the use of technology. It includes the handling of software and its updating, safe browsing, safe file downloading, social engineering, knowledge of system security settings etc. The aim is to assess the average awareness level of the users in all these areas against the three dimensions under analysis.

4.3.2.1 Dimension: Knowledge

Stats in Fig. 4.5 show awareness level of users regarding the threats of USB drives. A total of 52% users choosing ‘High’ level of awareness of USB threats is indeed encouraging.

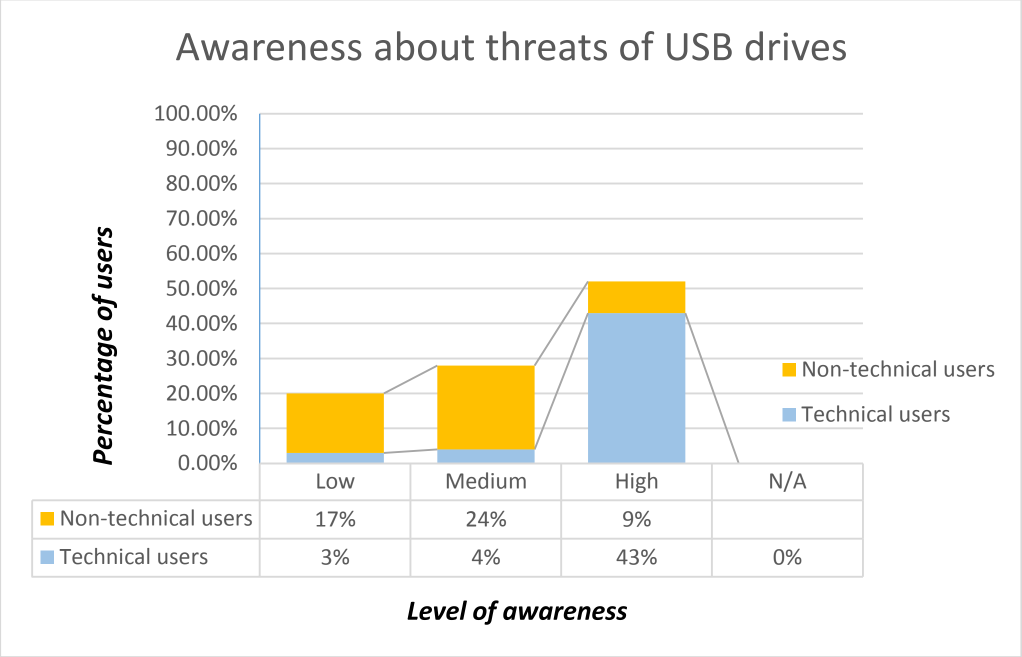


Figure 4.5: Level of awareness of USB drive threats

44% users chose 'Low' scale when asked if they used licensed software, meaning that they never used licensed software. 39% chose 'Medium' meaning that they use licensed software but not always. 17% users choosing 'High' scale means that they (always) used licensed software.

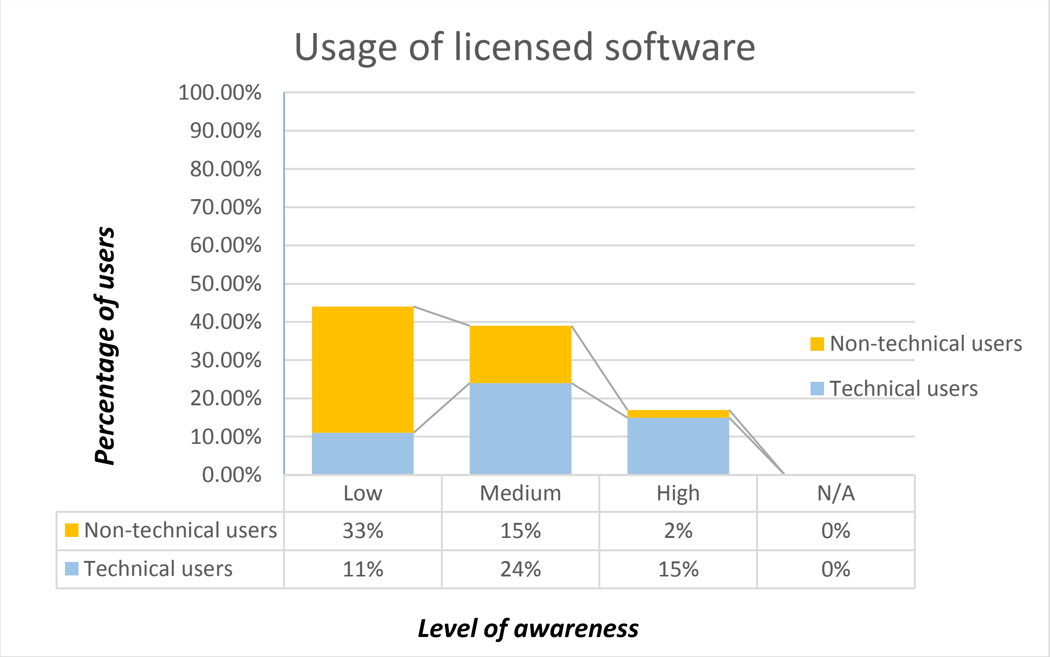
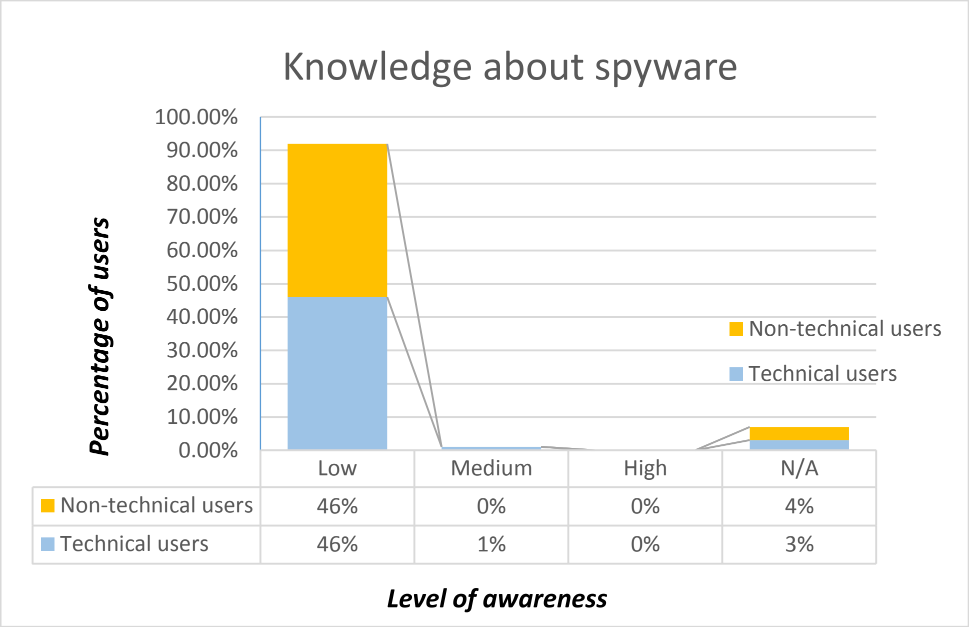


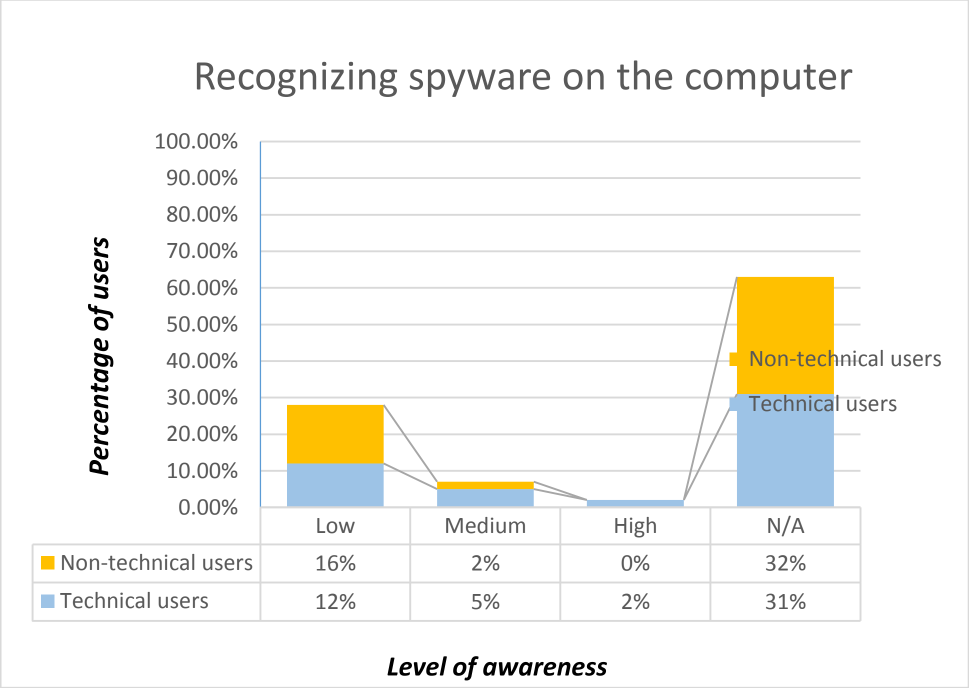
Figure 4.6: Level of awareness of users regarding licensed software

The survey revealed alarming results when users were asked to share their knowledge about spyware. 92% users chose 'Low' level of awareness about spyware, 28% indicated that they cannot recognize spyware on the computer; however most of the users chose N/A against questions related to spyware.



	Low	Medium	High	N/A
Non-technical users	46%	0%	0%	4%
Technical users	46%	1%	0%	3%

Figure 4.7: Level of awareness of Spyware



	Low	Medium	High	N/A
Non-technical users	16%	2%	0%	32%
Technical users	12%	5%	2%	31%

Figure 4.8: Level of awareness of Spyware recognition on computer

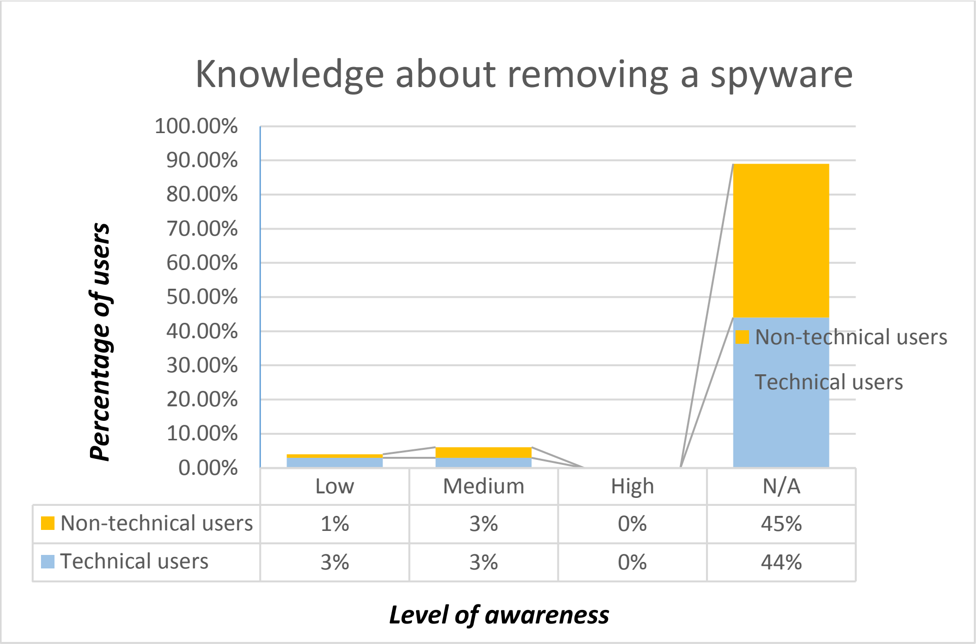


Figure 4.9: Level of awareness about Spyware removal

Another striking result was against online frauds where 25% of users chose ‘Low’ level of awareness. 54% chose ‘Medium’ level of awareness. 21% users with ‘High’ level of awareness about online frauds is still encouraging.

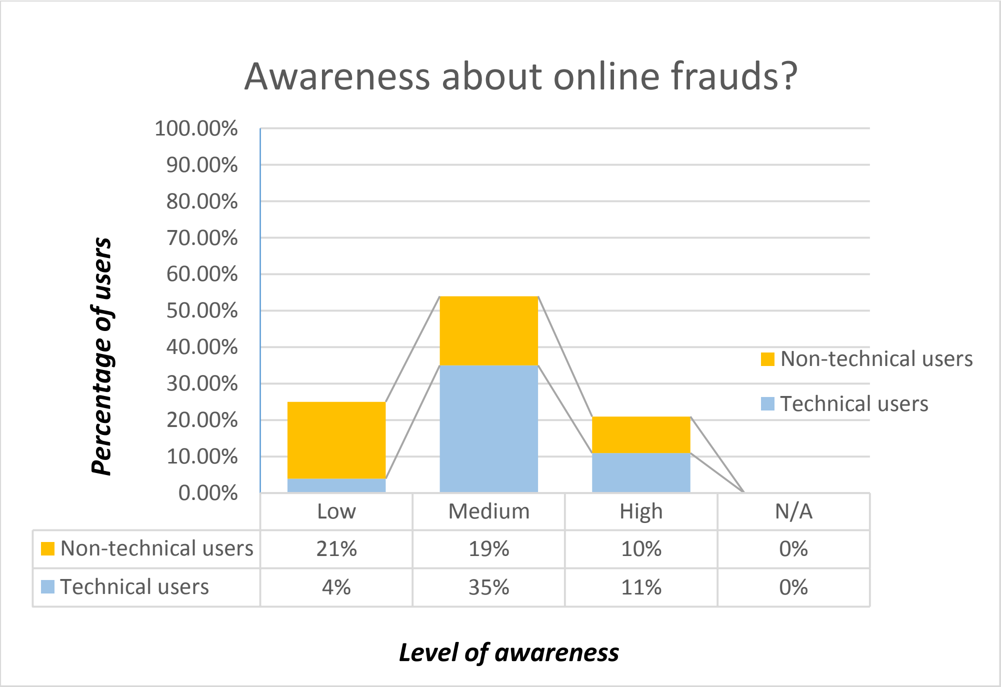


Figure 4.10: Level of awareness of Online Frauds

4.3.2.2 Dimension: Attitude

34% of the users indicated that they were not cautious about downloading files from the internet (showing low awareness level), 44% chose 'Medium' and 22% users indicated that they were highly cautious of downloading files from the internet.

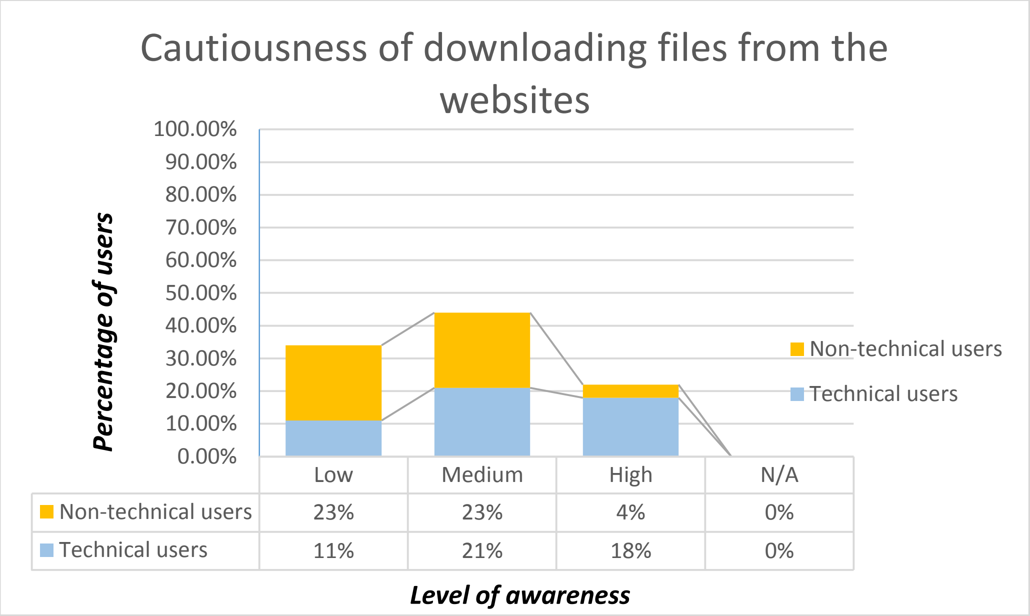


Figure 4.11: Level of awareness of safe file download

80% users indicated that they were highly cautious about providing personal information on the telephone. 2% indicated they were least cautious. The figures 4.12 shares stats about the cautiousness about revealing personal/financial information in email.

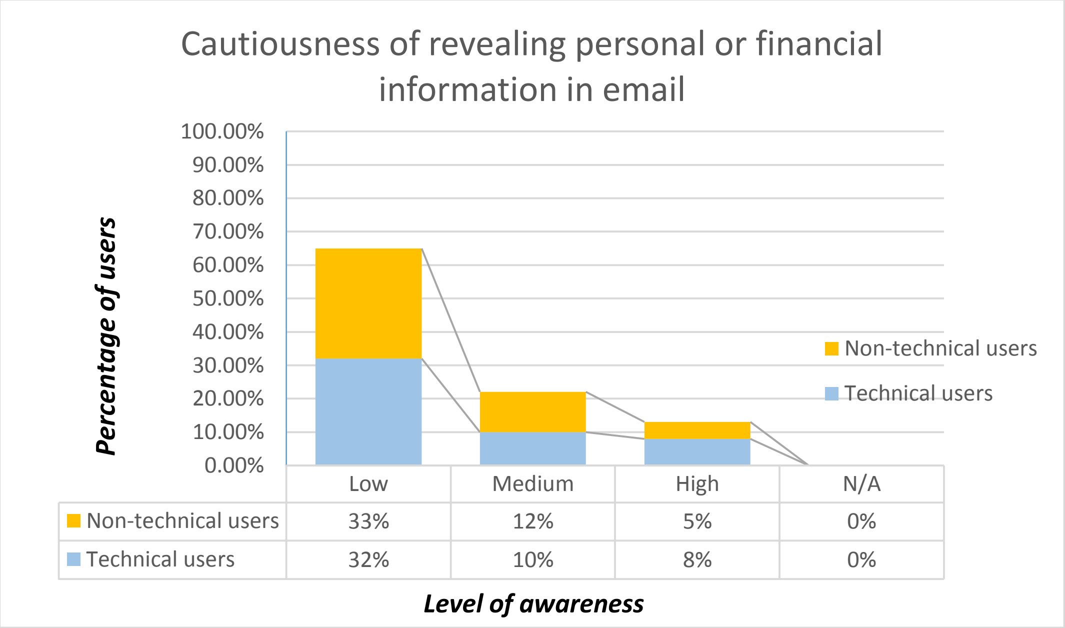


Figure 4.12: Level of cautiousness of sharing personal information in Email

4.3.2.3 Dimension: Behavior

53% users claimed that they always keep their software updated. Alarmingly, 14% chose ‘Low’ indicating that they never updated their software, another channel of inviting attacks and threats to the system.

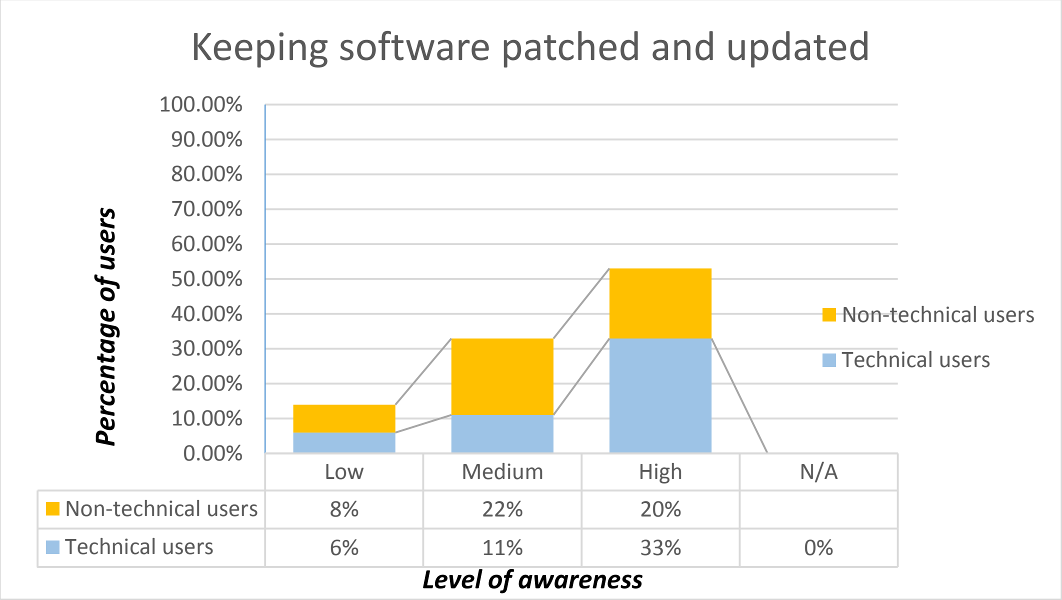


Figure 4.13: Level of awareness of users regarding software update

When asked if they always visited the genuine vendor sites directly to purchase or renew the software, following are the results that came out. ‘Low’ means never, ‘Medium’ means sometimes and ‘High’ means always or very often. 19% users chose N/A i.e. did not choose to answer this question.

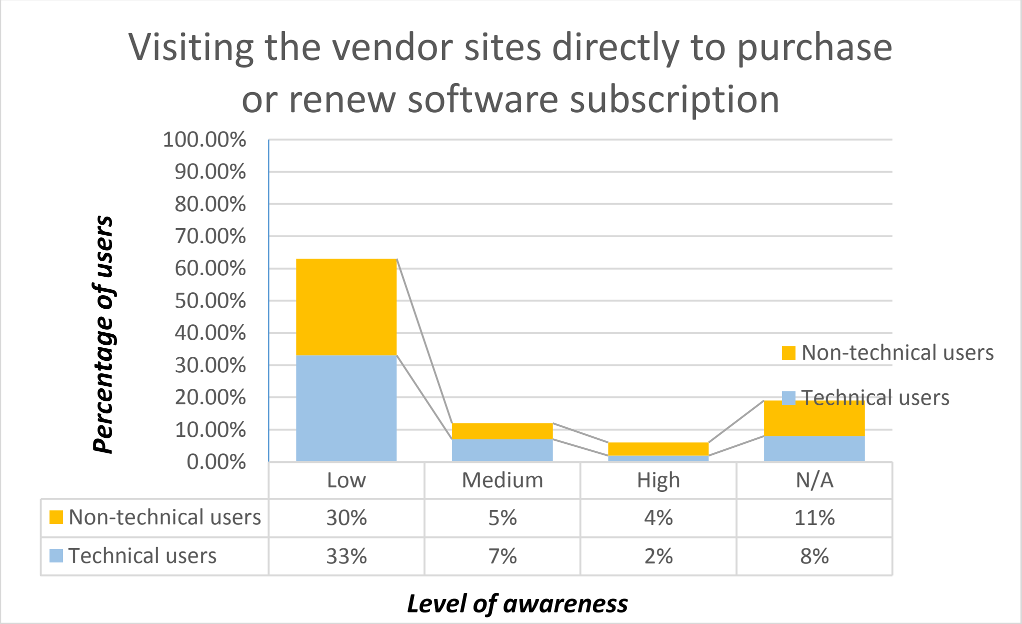


Figure 4.14: Level of awareness of users regarding software purchase/renewal

Stats in fig. 4.15 show the number of users making use of the system security settings where ‘Low’ means never, ‘Medium’ means often and ‘High’ means very often or always. 47% score of users making use of system security setting often is not too bad. 14% choosing ‘Low’ i.e. never making use of PC security settings is still questionable. 11% users chose not to answer.

Point to be noted here is that out of total users who chose ‘High’ scale, 38% were from technical backgrounds, indicating that clearly the users from technical or engineering educational backgrounds have better level of awareness in the IT security domain. The people from non-technical background however lag here.

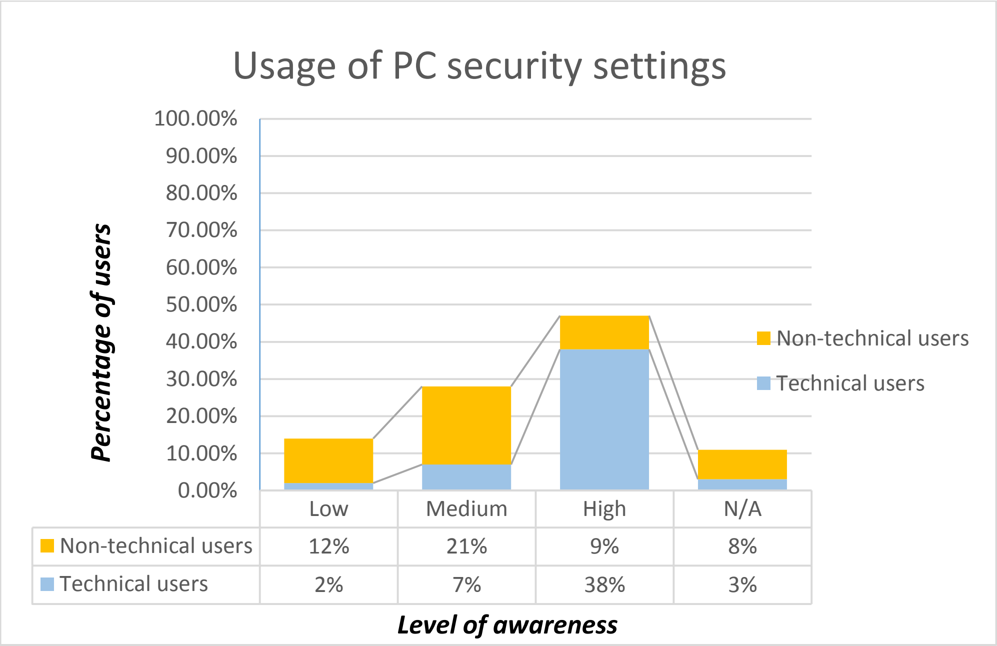
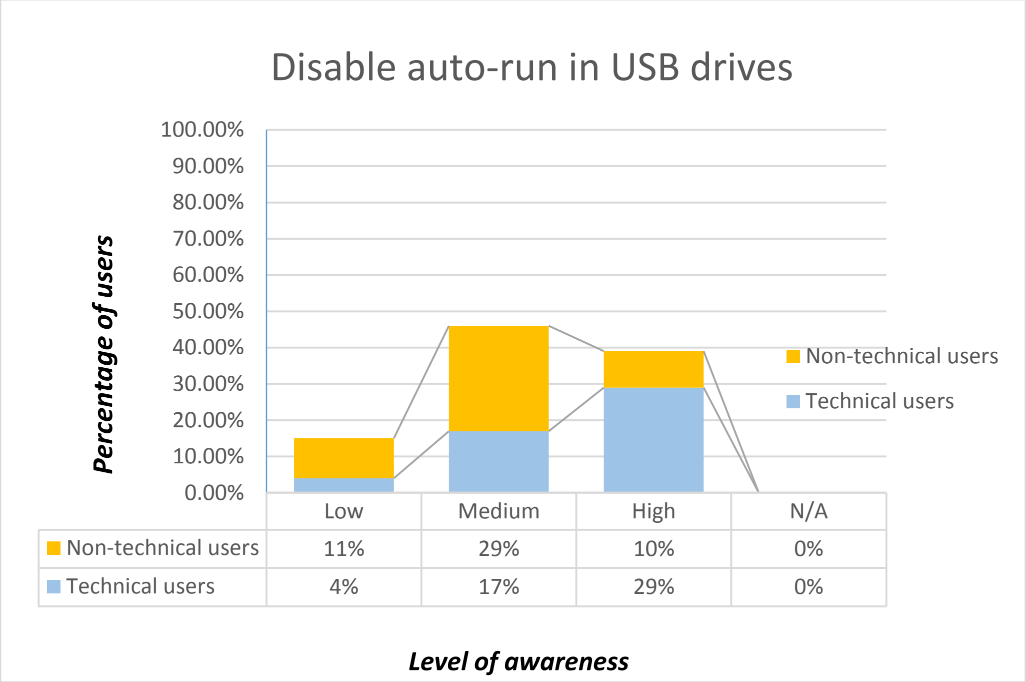


Figure 4.15: Level of awareness of PC security settings

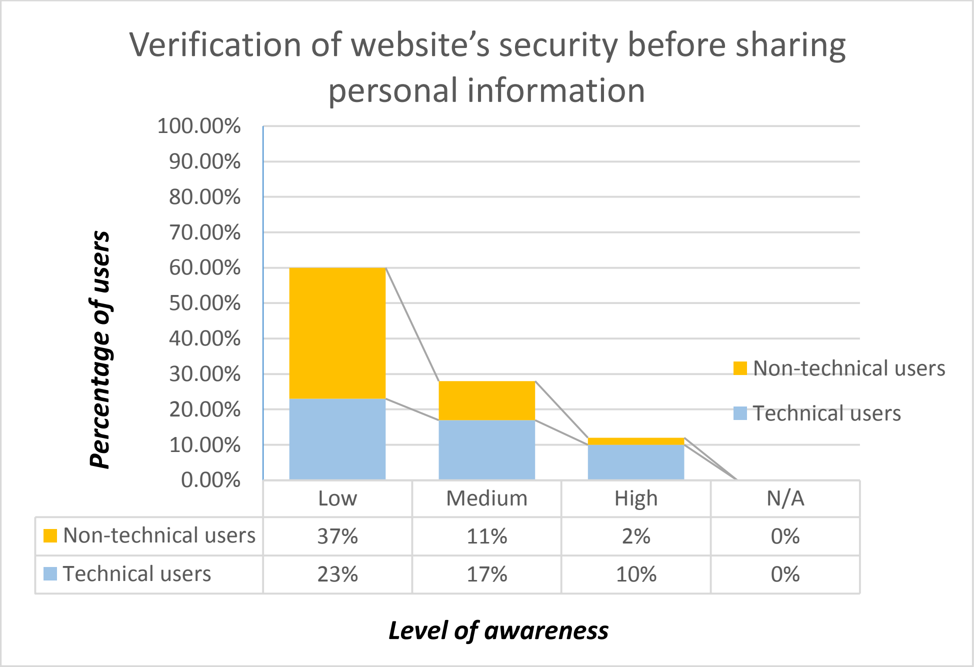
15% of the total users do not disable auto-run in USB drives. 46% do it sometimes and 39% users claimed that they always disabled auto-run in USB drives.



	Low	Medium	High	N/A
🟨 Non-technical users	11%	29%	10%	0%
🟦 Technical users	4%	17%	29%	0%

Figure 4.16: Level of awareness regarding disabling auto-run of USB drives

Survey results also reveal that 60% users never verify website's security before sharing personal information (low awareness level). Detailed stats are shown in Fig. 4.17.



	Low	Medium	High	N/A
🟨 Non-technical users	37%	11%	2%	0%
🟦 Technical users	23%	17%	10%	0%

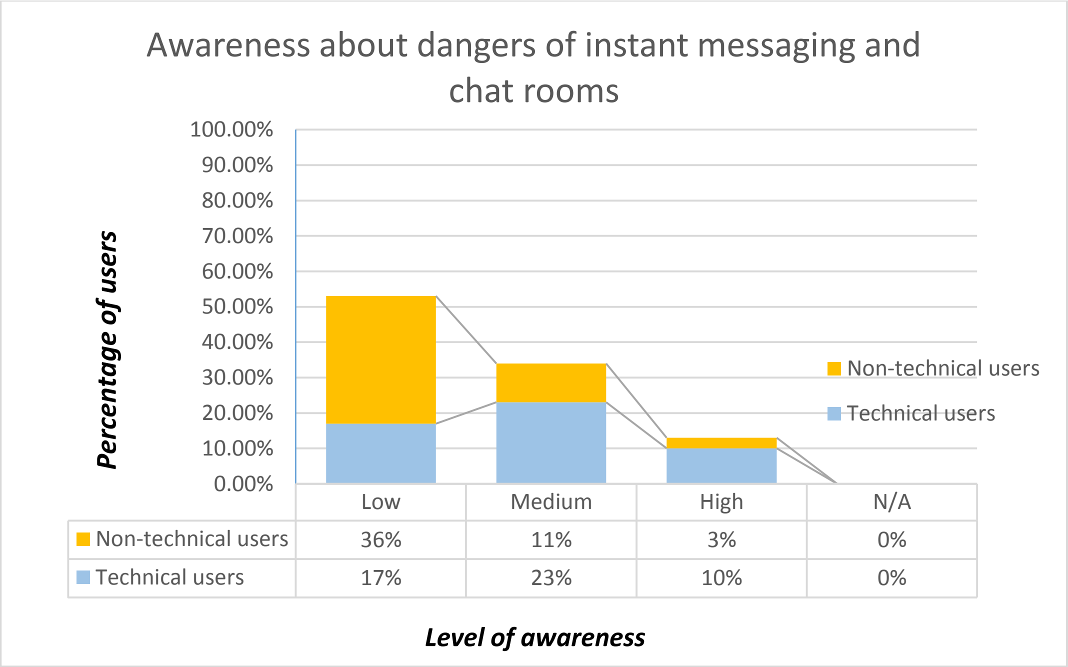
Figure 4.17: Level of awareness about checking Website's security

4.3.3 Email and communication

This section aims at collecting information about users' sense of IT security while using Email, Instant messaging and other online communication media.

4.3.3.1 Dimension: Knowledge

The results show that only 13% of total users have 'High' i.e. reasonable awareness level of dangers of instant messaging and chat rooms, 5% of the people indicated that they reveal personal information in chat rooms and email.



	Low	Medium	High	N/A
Non-technical users	36%	11%	3%	0%
Technical users	17%	23%	10%	0%

Figure 4.18: Level of awareness of threats of instant messaging

4.3.3.2 Dimension: Attitude

Survey revealed that 13% users admitted that they are not cautious about opening unsolicited attachments directly, 65% chose high level (very cautious).

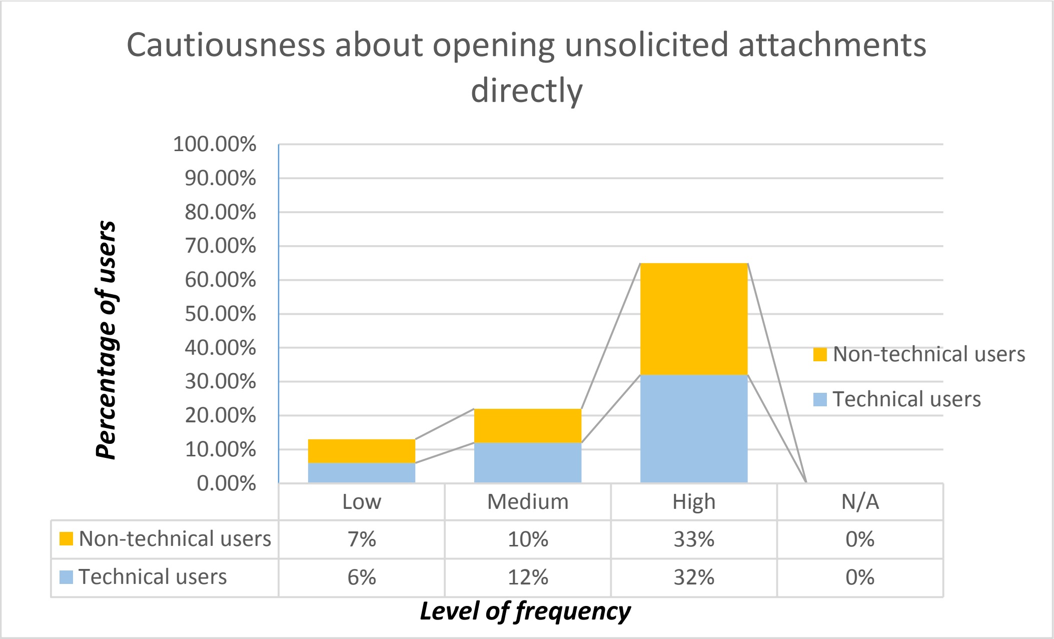


Figure 4.19: Verifying unsolicited attachments

4.3.3.3 Dimension: Behavior

83% users admitted they never reveal personal information in chat rooms, 5% chose that they do reveal personal information in chat rooms.

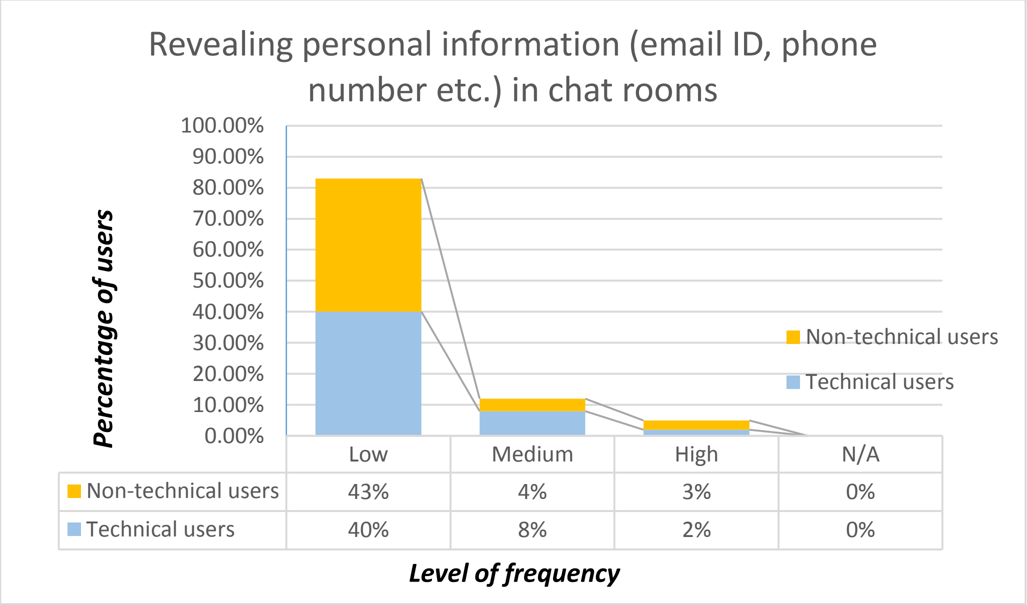
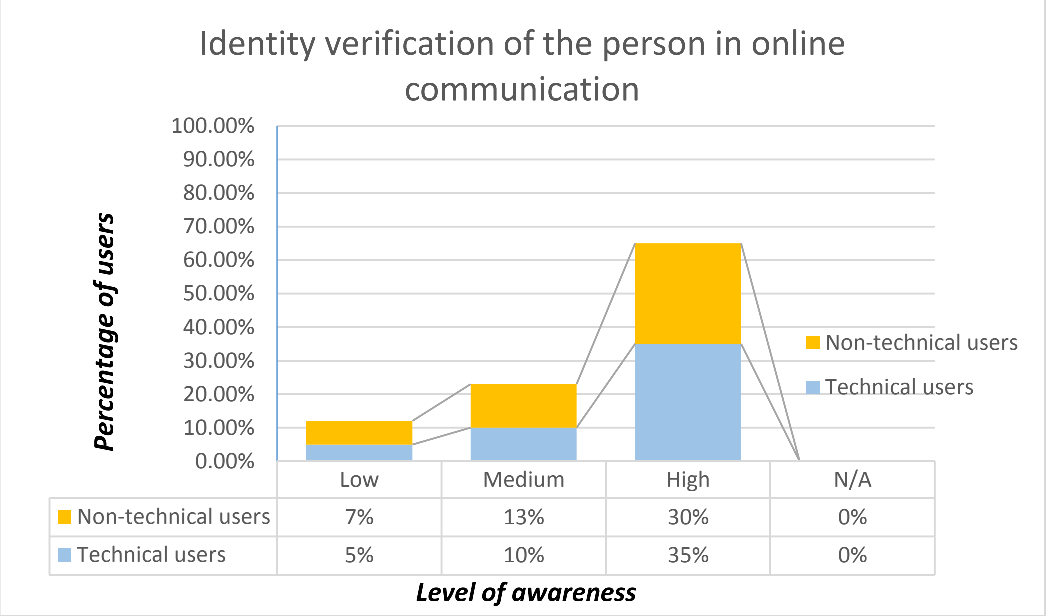


Figure 4.20: Level of frequency of revealing personal information in chat rooms

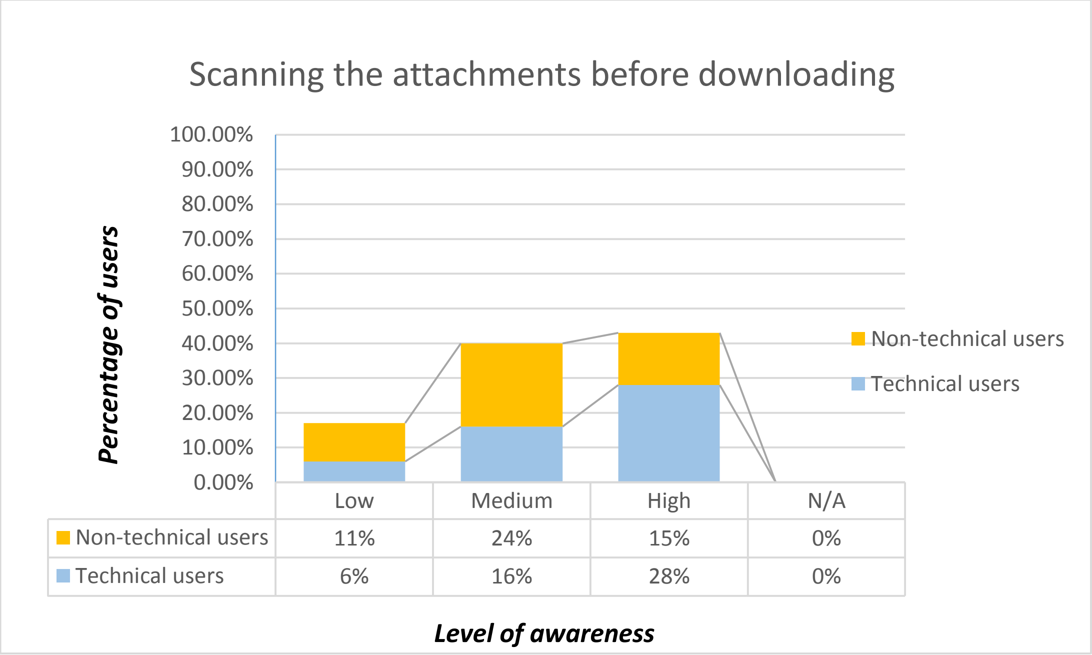
65% users claimed that they verify the identity of the person they communicate with online, 12% indicated they do not do so. 65% users claimed that they are highly cautious about opening the unsolicited (uninvited/suspicious) attachments directly, 13% chose ‘Low’ indicating that they are least cautious in this regard.



	Low	Medium	High	N/A
🟨 Non-technical users	7%	13%	30%	0%
🟦 Technical users	5%	10%	35%	0%

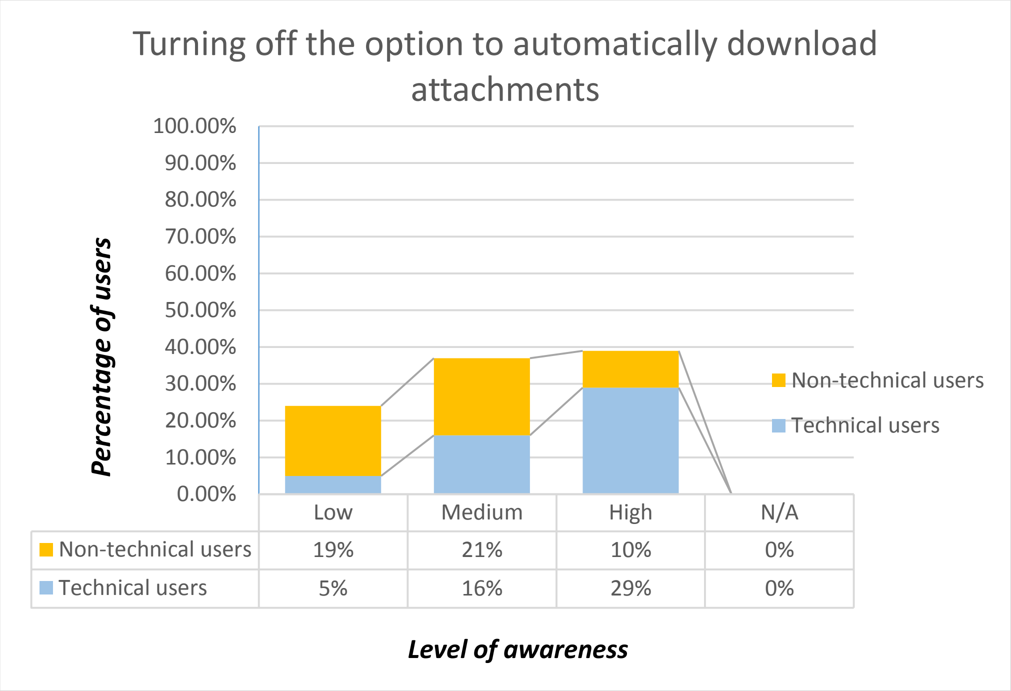
Figure 4.21: Verifying person’s authenticity

17% users do not scan the attachments before downloading (Low), 40% do it sometimes (Medium) and 43% do it every time (‘High’). 24% of the users never turn off the option to automatically download the attachments (Low) and 39% claimed that they always do (High). Details stats are in Fig. 22 and Fig. 23.



	Low	Medium	High	N/A
🟨 Non-technical users	11%	24%	15%	0%
🟦 Technical users	6%	16%	28%	0%

Figure 4.22: Level of awareness of document scanning



	Low	Medium	High	N/A
Non-technical users	19%	21%	10%	0%
Technical users	5%	16%	29%	0%

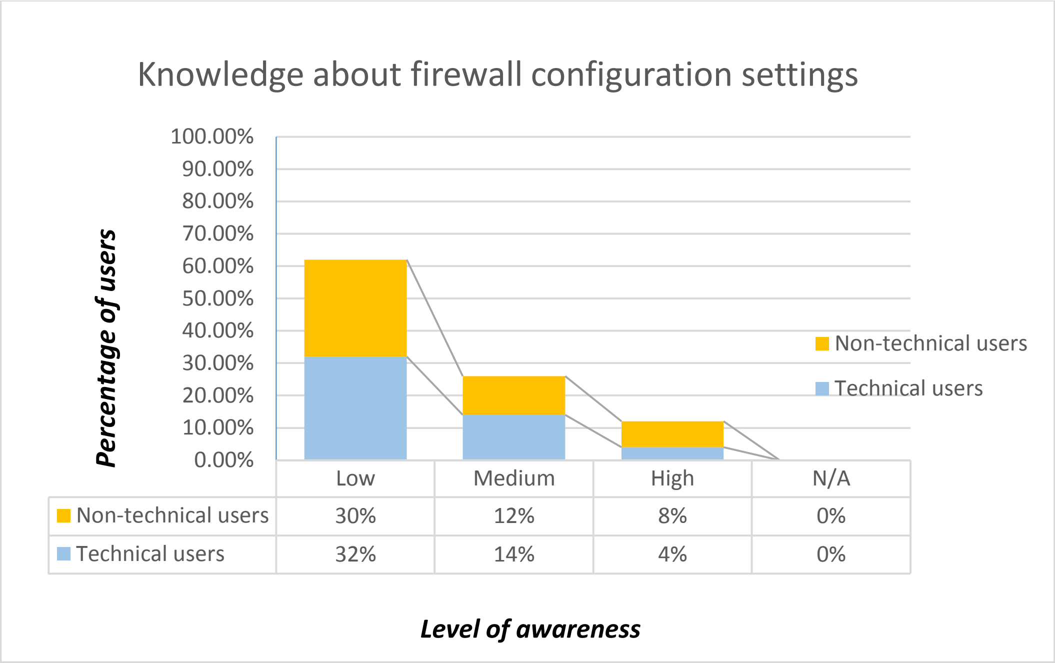
Figure 4.23: Level of awareness of safe document download

4.3.4 General Security

This section is focused on collection information about awareness on general security of IT devices like knowledge of security software configuration on computer, use of strong password, locking computer when away, disconnecting computer from internet when not needed etc.

4.3.4.1 Dimension: Knowledge

Fig. 4.24 shows that 62% of the survey participants do not know much about firewall configuration settings. The random interviews revealed that most of the non-technical participants did not even know about firewall and its functionality and usage. 12% of the users chose ‘High’ indicating their good knowledge in this domain.

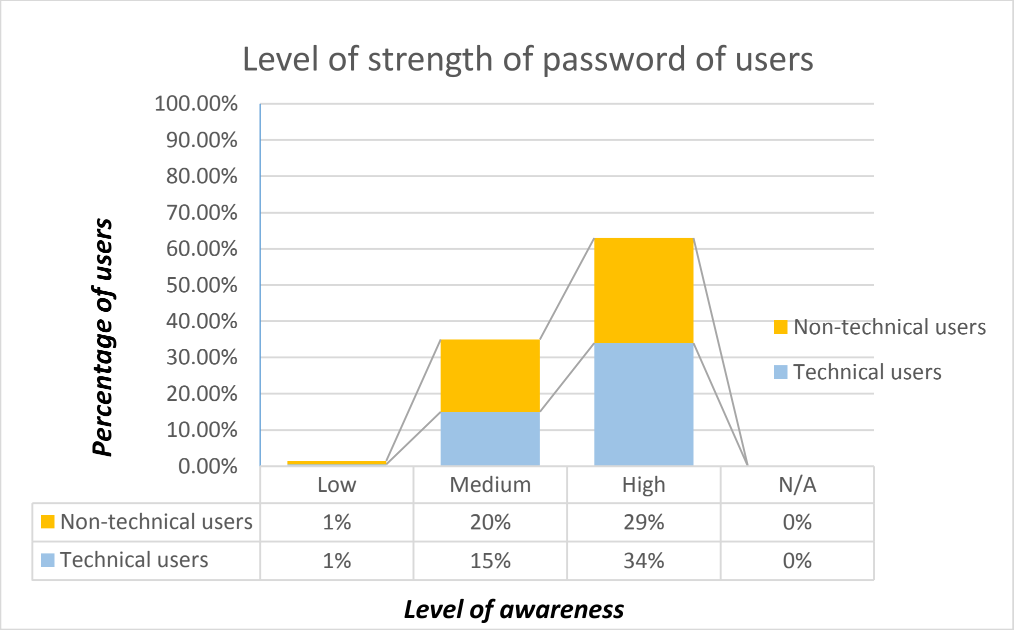


	Low	Medium	High	N/A
🟨 Non-technical users	30%	12%	8%	0%
🟦 Technical users	32%	14%	4%	0%

Figure 4.24: Level of awareness of Firewall configuration

4.3.4.2 Dimension: Attitude

65% users indicated that they used strong passwords i.e. passwords with combination of capital and small letters and numbers (explained to users verbally). 2% admitted that they use very weak passwords (low). Stats reveal that the attitude of users in this domain is somehow better.



	Low	Medium	High	N/A
🟨 Non-technical users	1%	20%	29%	0%
🟦 Technical users	1%	15%	34%	0%

Figure 4.25: Strong password usage

4.3.4.3 Dimension: Behavior

Fig. 4.26 shares stats on how many users lock their computers when away. 50% users never lock their computers when away (low) and 24% users indicated that they always locked computer when they are way.

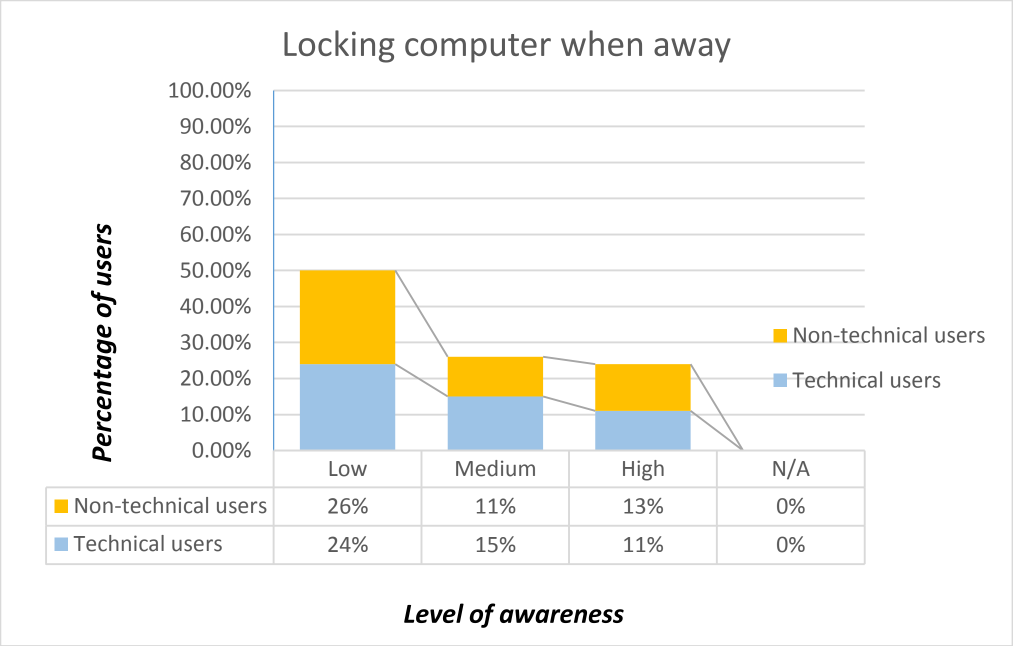


Figure 4.26: Level of awareness of safe computer use

Fig. 4.27 shows that 62% users admitted that they do not disconnect their devices from the internet when away (low), however 13% indicated that they always did (High).

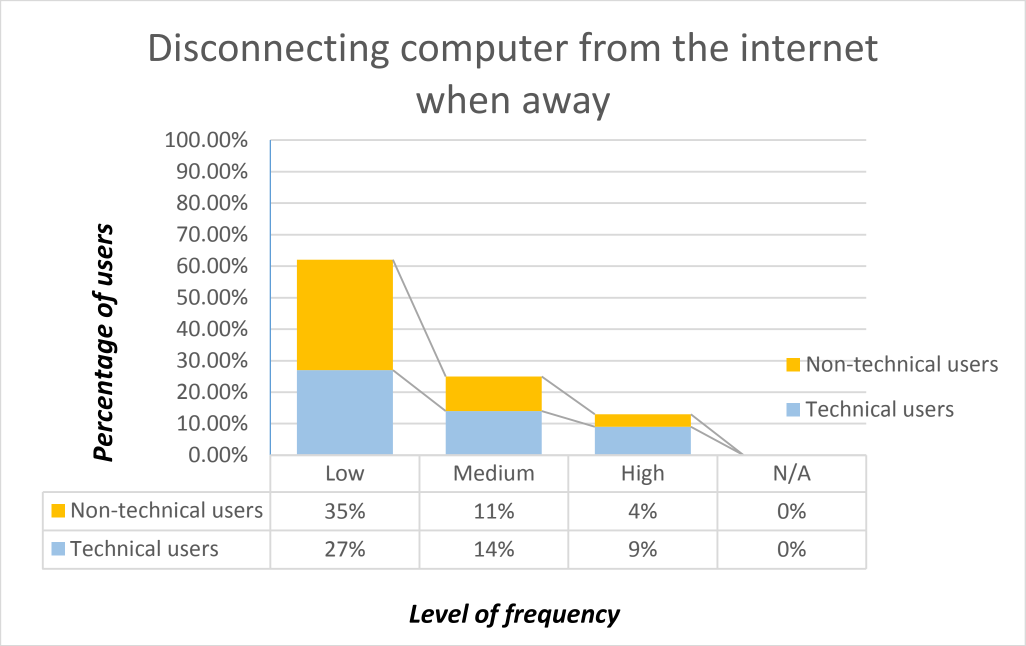
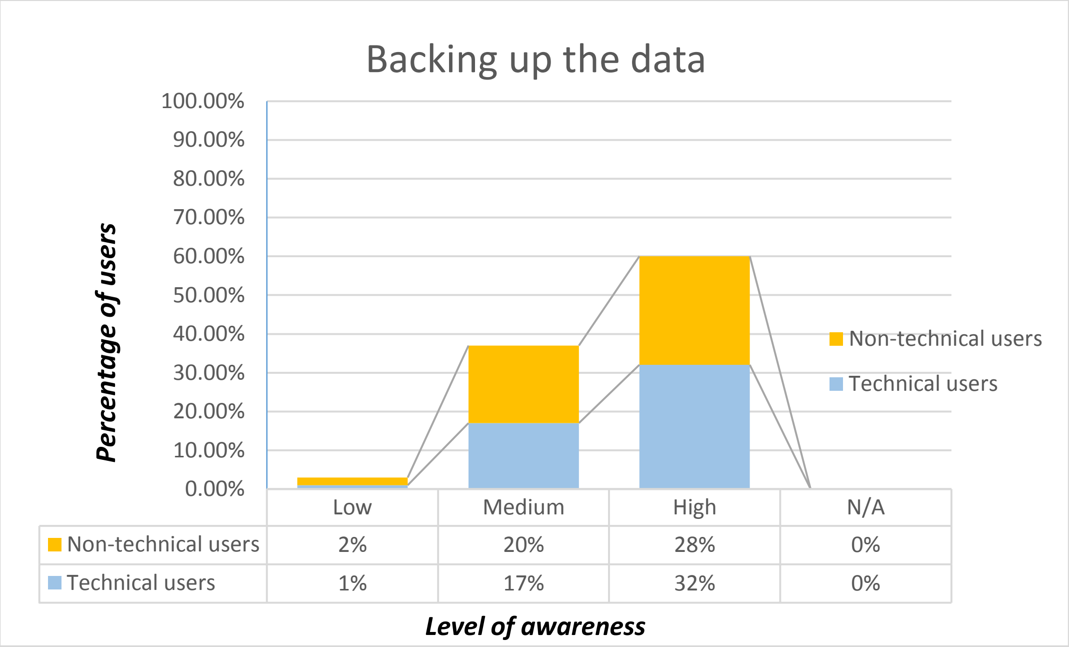


Figure 4.27: Level of frequency of disconnecting computer when away

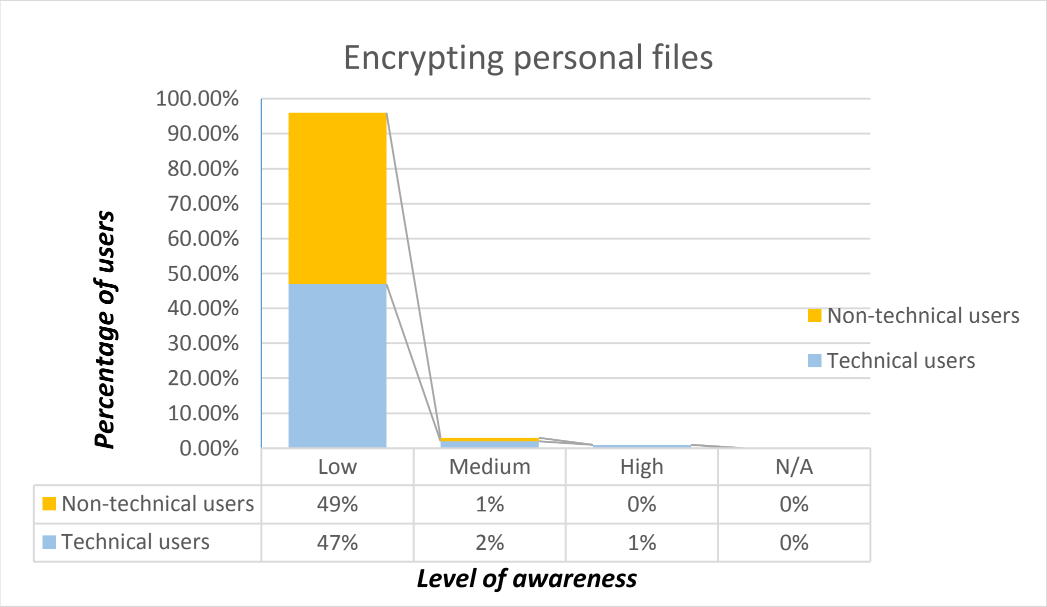
Fig. 4.28 shows stats about users backing up their data. Survey reveals that 3% users never back up their data (low), 60% users always back up their data (high) and 37% users sometimes do (medium).



	Low	Medium	High	N/A
🟨 Non-technical users	2%	20%	28%	0%
🟦 Technical users	1%	17%	32%	0%

Figure 4.28: Level of awareness of data backup

Fig. 29 reveals alarming results about users' behavior towards privacy. 96% of the users never encrypted their files. This indicates that the users do not have enough awareness about encryption and how it can protect their privacy.



	Low	Medium	High	N/A
🟨 Non-technical users	49%	1%	0%	0%
🟦 Technical users	47%	2%	1%	0%

Figure 4.29: Level of awareness of encryption

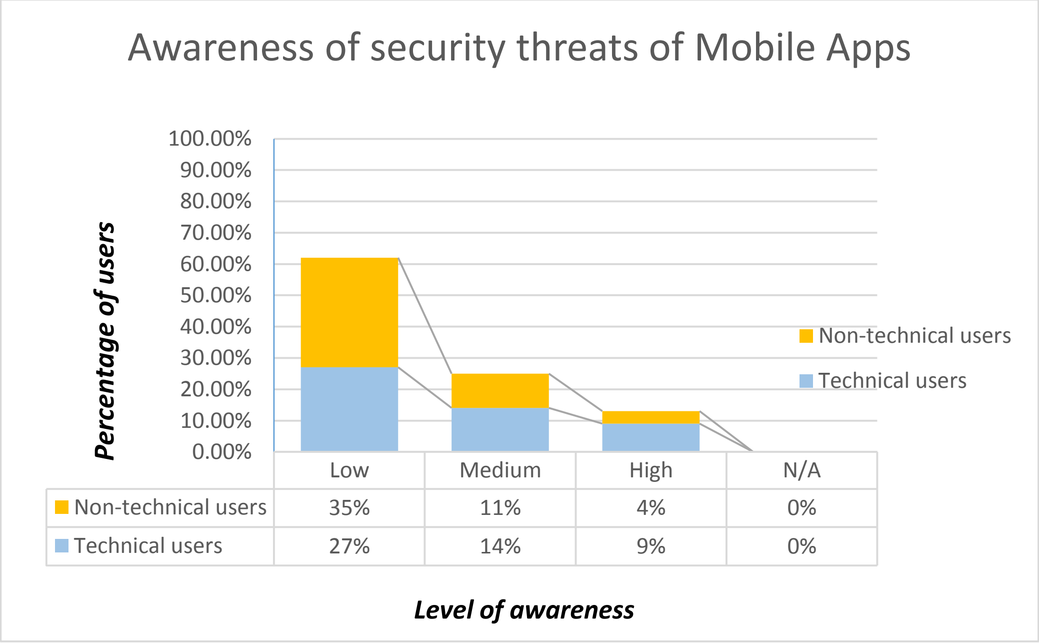
4.3.5 Mobile Devices

This section aims to collect information on the users' awareness and security consciousness regarding their mobile device i.e. number of users who password protect their device, number of users who use public Wi-Fi and numbers of users who turn off Bluetooth when not in use.

Out of all the cyber domains for which the survey was conducted, the level of awareness has been found to be highest in 'Mobile devices' (at least in terms of physical security). This shows that users have their most personal data in their mobiles and they realize the threats of security attacks more in Mobile devices as compared to their PCs.

4.3.5.1 Dimension: Knowledge

Fig. 4.30 shows awareness levels of users about threats related to mobile apps. 62% users have low awareness level and 13% users indicated that they have good (high) awareness level in this regard.



	Low	Medium	High	N/A
🟨 Non-technical users	35%	11%	4%	0%
🟦 Technical users	27%	14%	9%	0%

Figure 4.30: Awareness of security threats of mobile apps

4.3.5.2 Dimension: Attitude

66% users always password protect their Mobile device, 3% indicated that they never do. Awareness level in this area has been found to be pretty high.

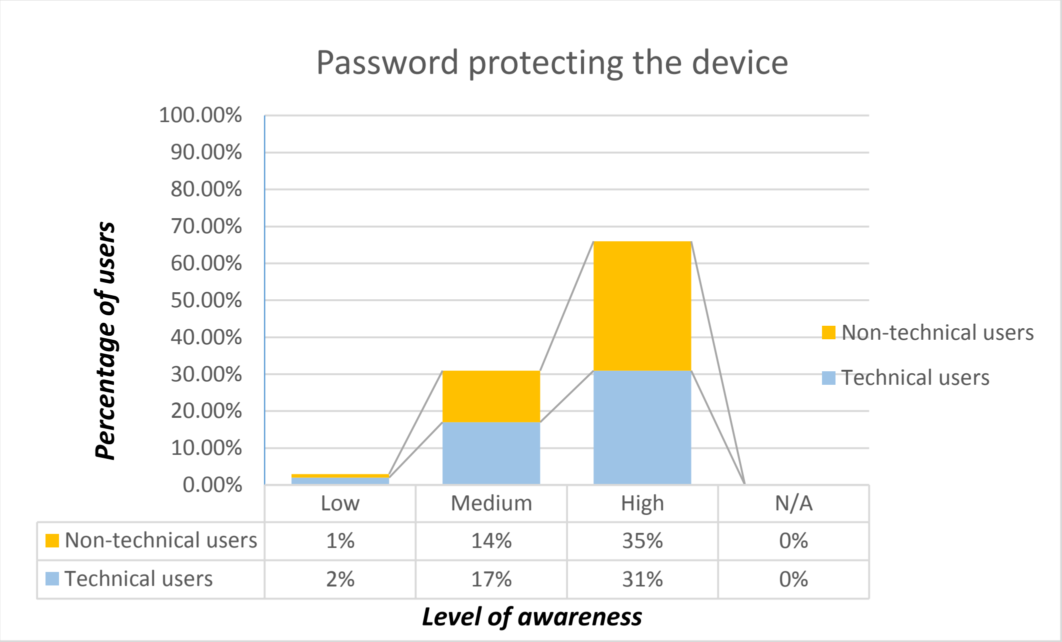


Figure 4.31: Users password protecting the device

4.3.5.3 Dimension: Behavior

85% users admitted their frequent use of Public Wi-Fi networks i.e. low awareness in terms of behavior. Survey also revealed that 87% users disconnect from the Bluetooth when not in use (high awareness level). Detailed stats are shown in Fig. 4.32 and Fig. 4.33 respectively.

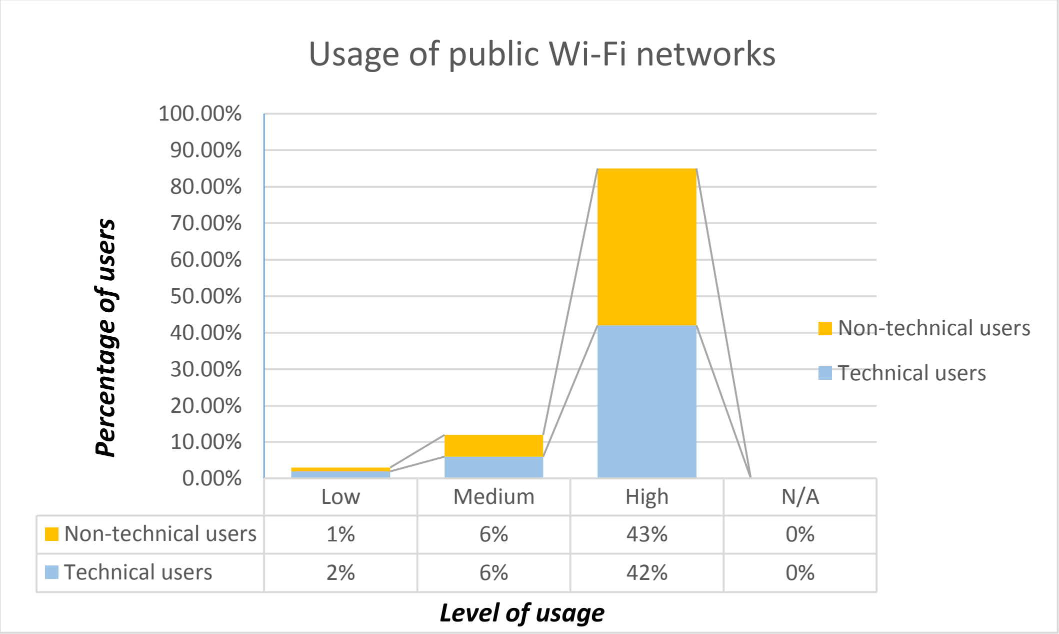
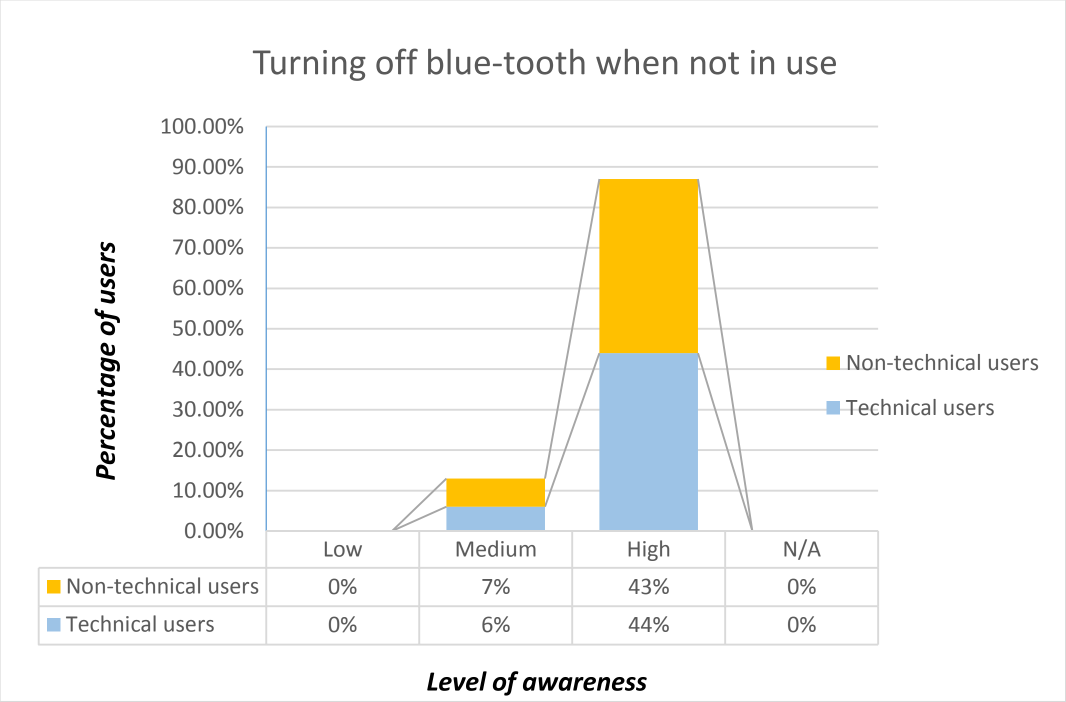


Figure 4.32: Level of usage of Public Wi-Fi



	Low	Medium	High	N/A
Non-technical users	0%	7%	43%	0%
Technical users	0%	6%	44%	0%

Figure 4.33: Safe Bluetooth usage

4.3.6 Privacy

The aim of this category is to determine how aware the users are when it comes to dealing and protecting their personal on IT devices.

4.3.6.1 Dimension: Knowledge

Fig 4.34 stats show the number of users who have least knowledge about how to securely erase the data from the device (Low), the users who know this to some extent (Medium) and the number of users who are well aware of securely erasing the data.

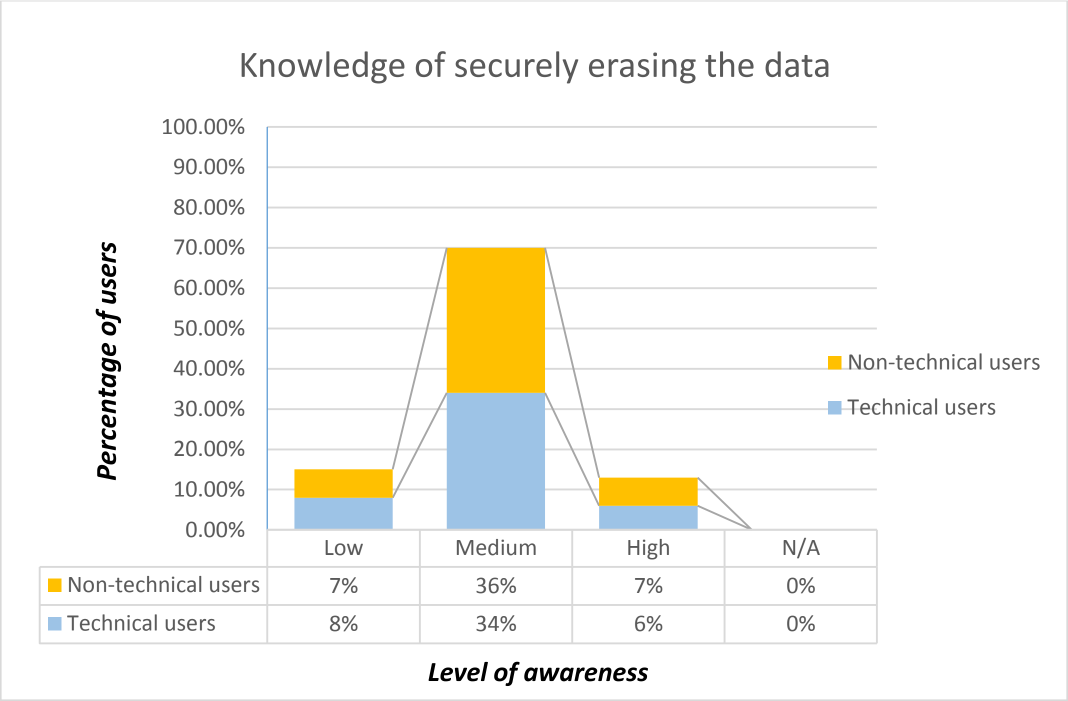


Figure 4.34: Securely erasing the data

Fig 4.35 shares stats on the awareness level of users on the security implications of use of cookies. Sadly 53% of the users admitted that they are least awareness of the implications the use of cookies brings to them.

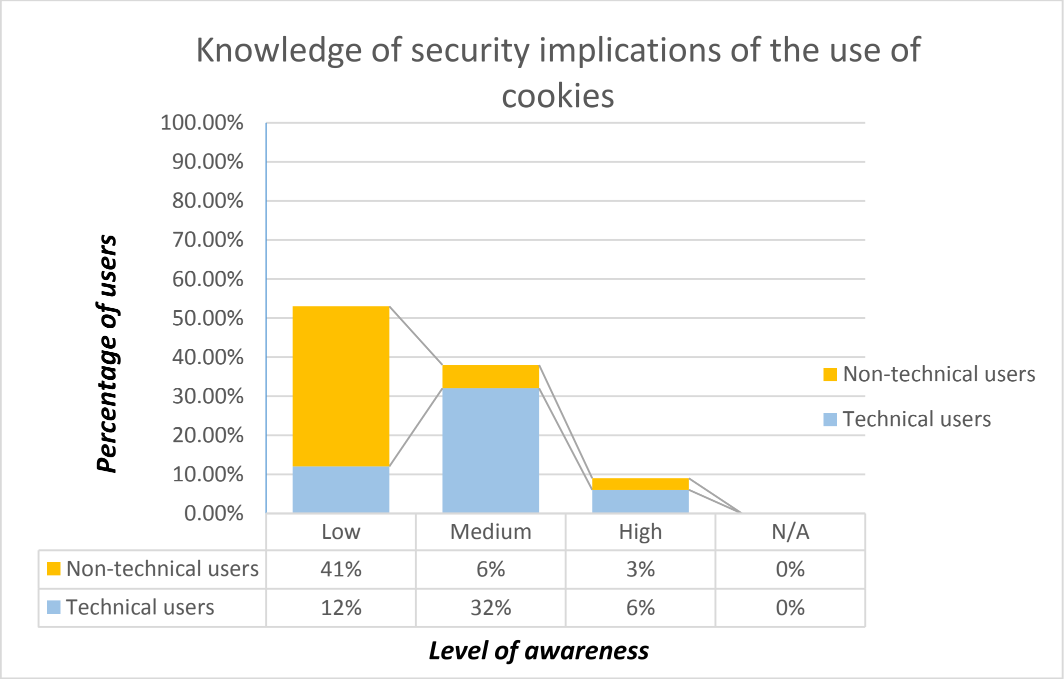


Figure 4.35: Level of awareness of cookies

Fig. 4.36 highlights on awareness levels on understanding about encryption. 50% of the users were found to be least aware (Low). However 33% of the users (that mostly includes the technical users) claimed that they had good idea about the concept of encryption (High).

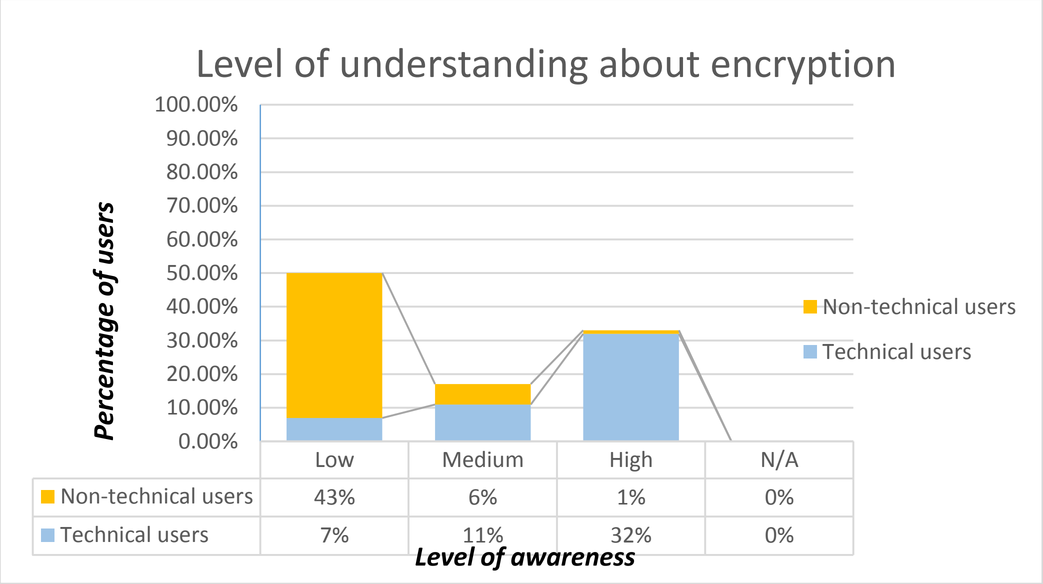


Figure 4.36: Level of awareness of encryption

4.3.6.2 Dimension: Attitude

80% users indicated that they are very cautious about providing personal information on Telephone (high), 2% indicated that they are least cautious (Low).

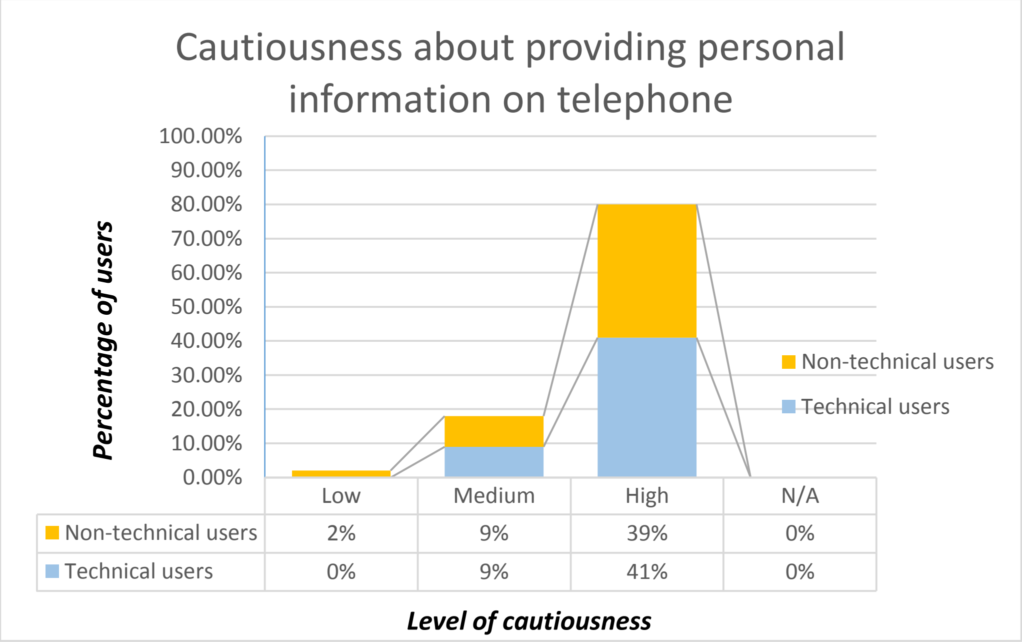
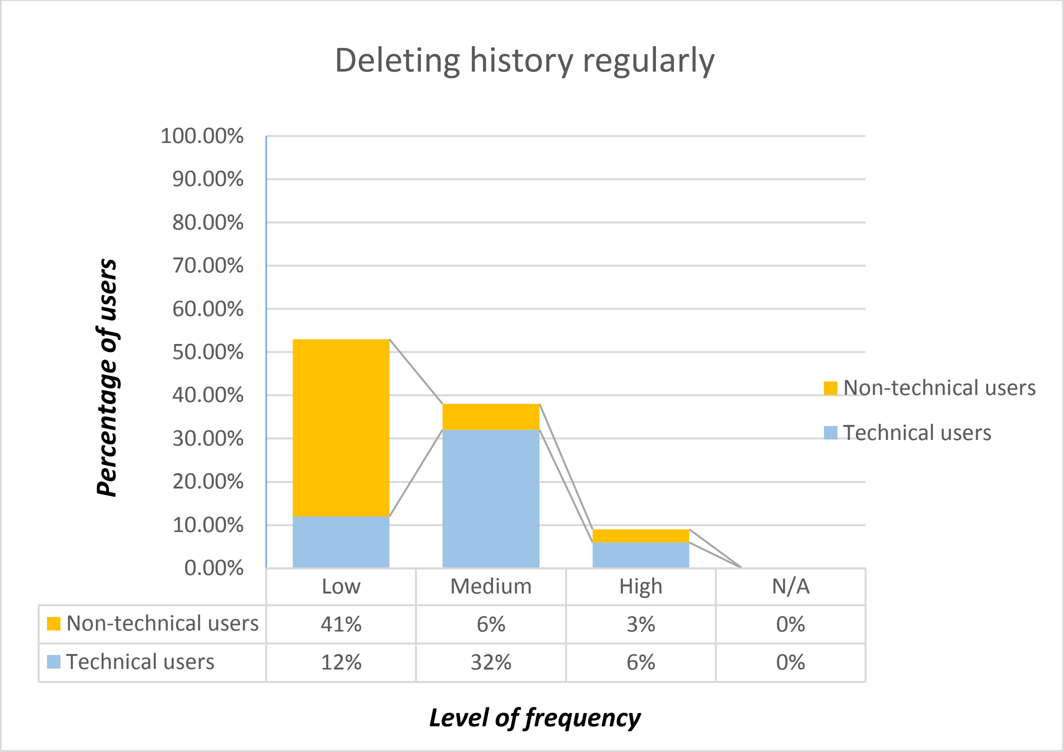


Figure 4.37: Level of cautiousness of sharing personal information on Telephone

4.3.6.3 Dimension: Behavior

Fig. 4.38 shows stats about history deletion. Only 9% users indicated that they delete history on regular basis for privacy purpose.



	Low	Medium	High	N/A
Non-technical users	41%	6%	3%	0%
Technical users	12%	32%	6%	0%

Fig. 4.38 Frequency of deleting history regularly

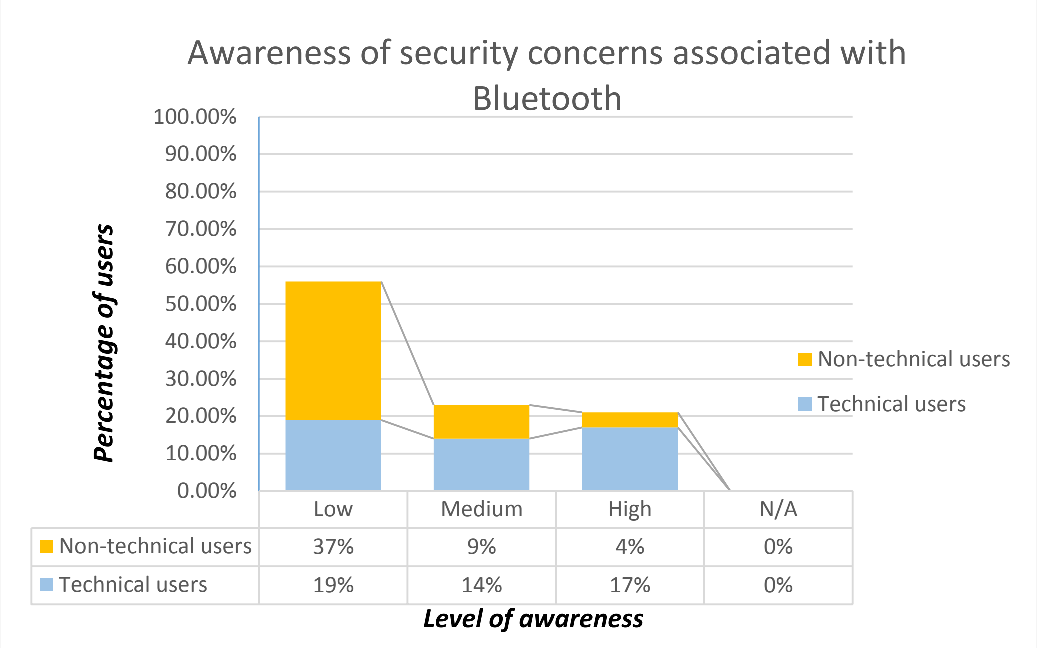
4.3.7 Safe Browsing

This section highlights the awareness level of the users on safe and secure browsing. The results show that hardly 21% of the users are comfortable with their knowledge on safe browsing (High). Stats for Medium and Low rating are shown below.

4.3.7.1 Dimension: Knowledge

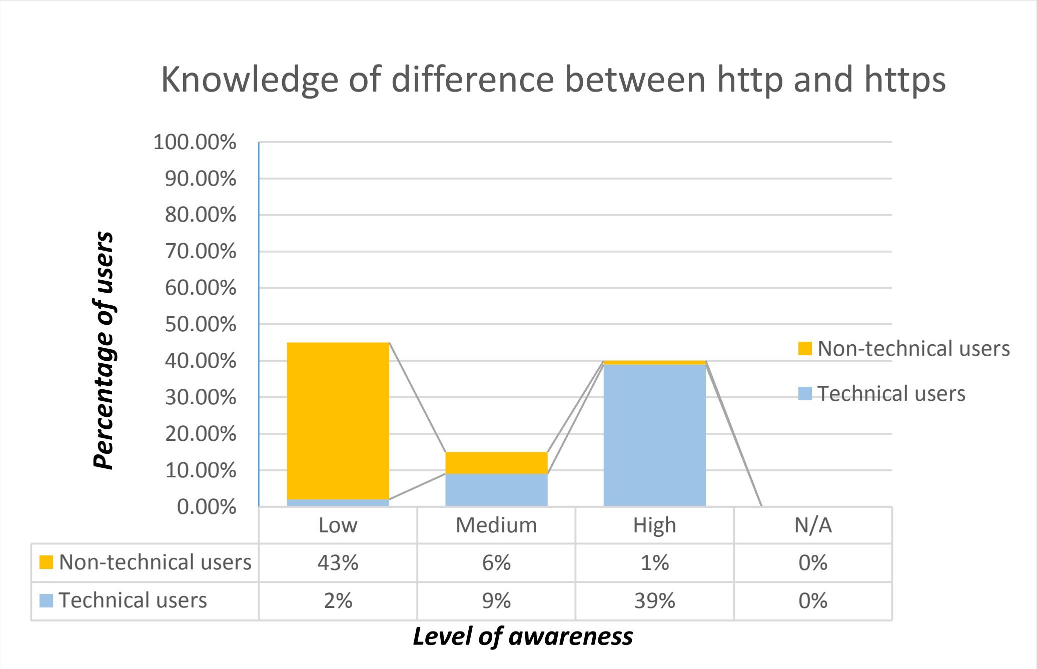
Survey revealed that 21% users are well aware of the security concerns associated Bluetooth and 56% are least aware. Detailed stats are shown in Fig. 39.

Fig. 4.40 shows stats about awareness level of difference between http and https. Survey revealed that 40% users know this difference and 45% users do not know the difference at all. (Low awareness level).



	Low	Medium	High	N/A
Non-technical users	37%	9%	4%	0%
Technical users	19%	14%	17%	0%

Figure 4.39: Level of awareness of Bluetooth security concerns

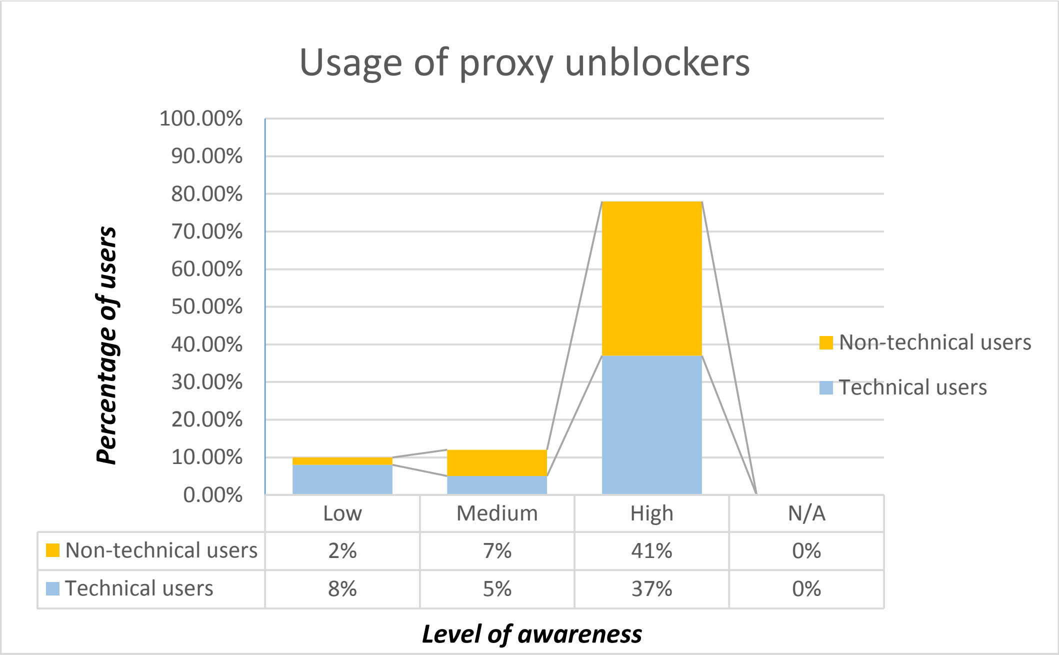


	Low	Medium	High	N/A
Non-technical users	43%	6%	1%	0%
Technical users	2%	9%	39%	0%

Figure 4.40: Level of awareness of https and https

4.3.7.2 Dimension: Behavior

A pretty high number of users (78%) were found to be regular users of proxy unblockers (e.g. Hotspot shield).



	Low	Medium	High	N/A
🟨 Non-technical users	2%	7%	41%	0%
🟦 Technical users	8%	5%	37%	0%

Figure 4.41: Usage of proxy unblockers

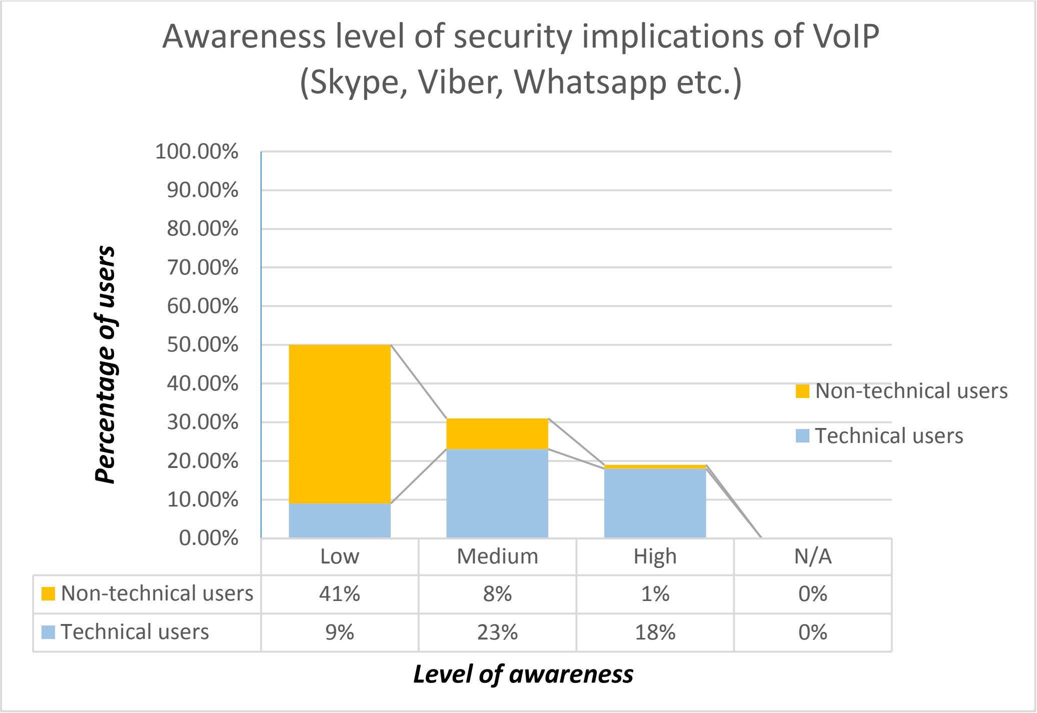
4.3.8 Software and Applications

This section throws light on awareness levels on security implications of VoIP, File sharing technology and privacy policies of the apps.

4.3.8.1 Dimension: Knowledge

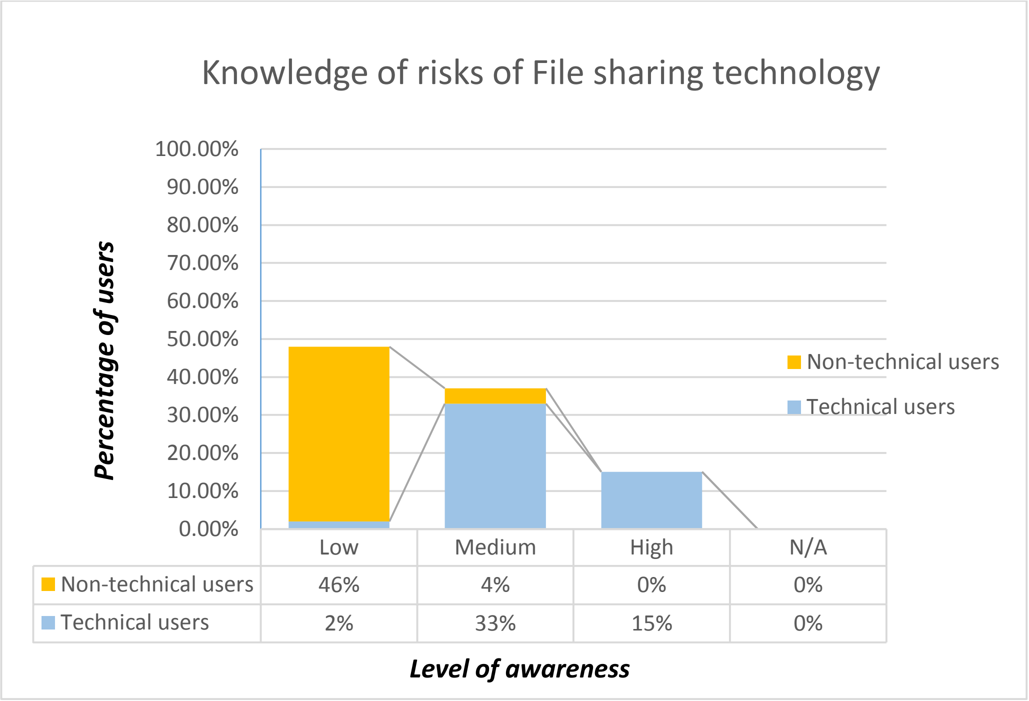
Fig. 4.42 shares stats about awareness level of users regarding security implications of VoIP. Only 19% users were found to be well-aware (High awareness level).

Fig. 4.43 shows stats about awareness of risks associated with File sharing technology. Only 15% users were found to be well-aware .



	Low	Medium	High	N/A
🟨 Non-technical users	41%	8%	1%	0%
🟦 Technical users	9%	23%	18%	0%

Figure 4.42: Level of awareness VoIP Security implications



	Low	Medium	High	N/A
🟨 Non-technical users	46%	4%	0%	0%
🟦 Technical users	2%	33%	15%	0%

Figure 4.43: Level of awareness of File sharing risks

4.3.8.2 Dimension: Attitude

Survey revealed that 81% users never check privacy policies of the apps before downloading i.e. poor attitude towards security.

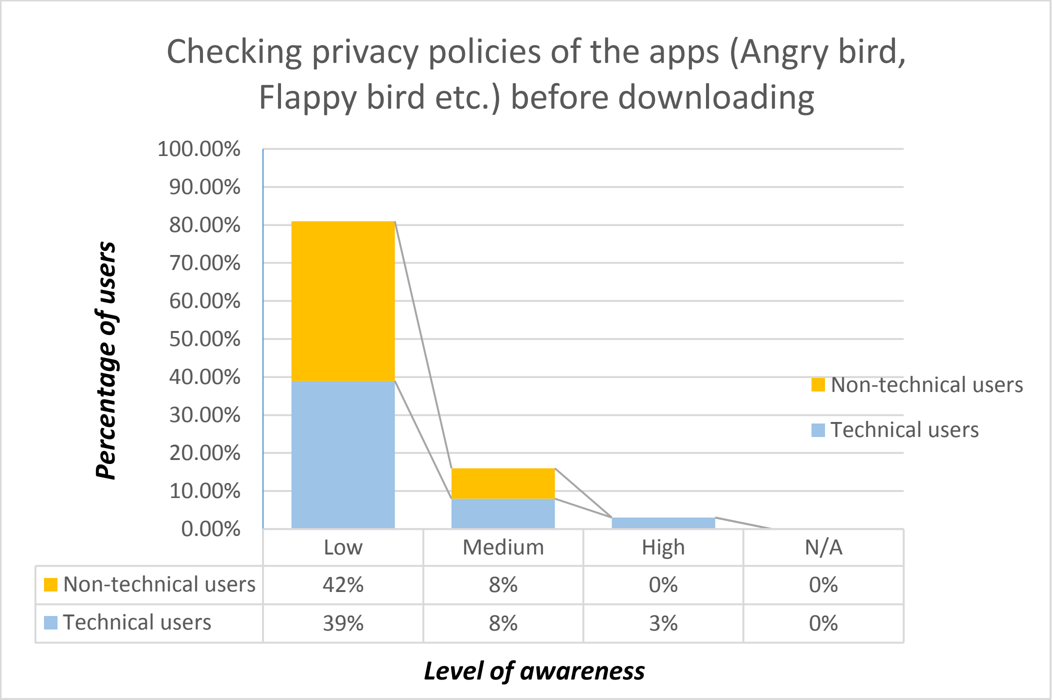


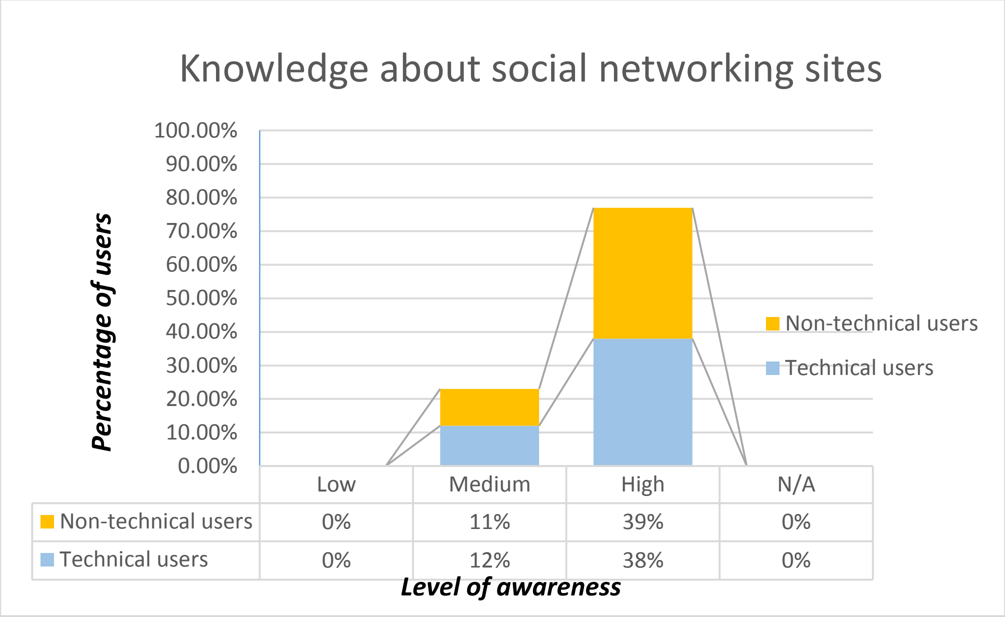
Figure 4.44: Privacy policies of apps

4.3.9 Social Networking

Social Networking has become a common trend worldwide today. The threats and risks associated with the social networking sites are inevitable.

4.3.9.1 Dimension: Knowledge

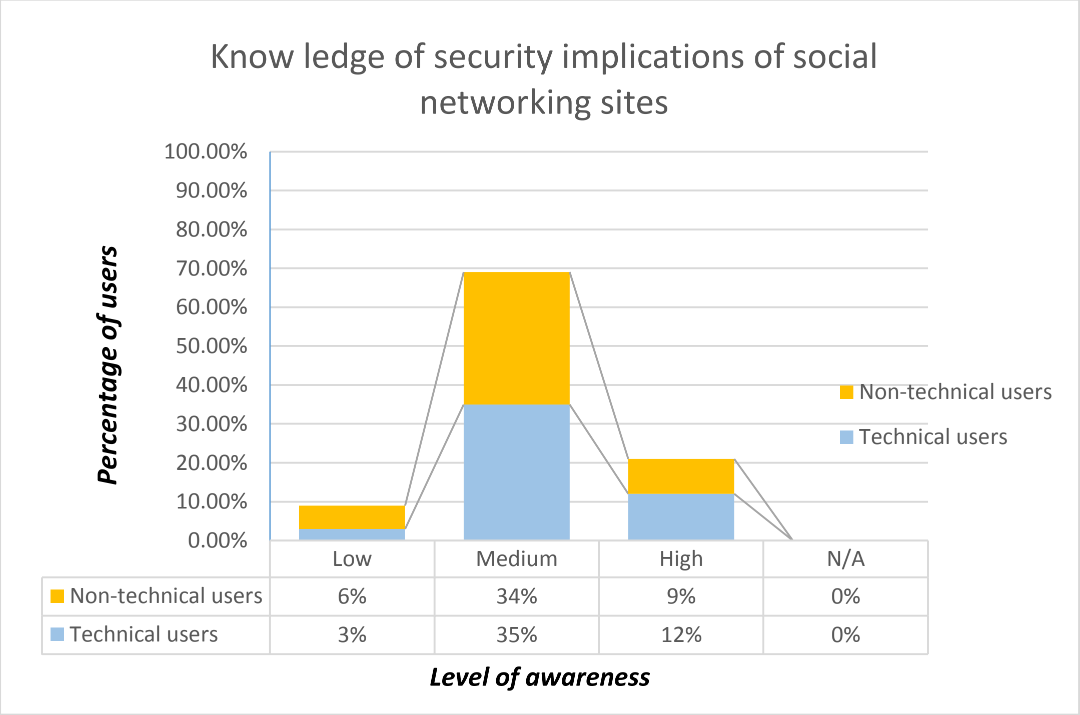
Most of the users who were part of the survey were found to have good knowledge of the social networking sites like Twitter, Facebook etc.



	Low	Medium	High	N/A
🟨 Non-technical users	0%	11%	39%	0%
🟦 Technical users	0%	12%	38%	0%

Figure 4.45: Level of awareness of social networking sites

Most of the users (69%) however indicated medium level of awareness regarding the social implications of the social networking sites (Fig 4.45).



	Low	Medium	High	N/A
🟨 Non-technical users	6%	34%	9%	0%
🟦 Technical users	3%	35%	12%	0%

Figure 4.46: Level of awareness of security implications of social networking sites

4.3.9.2 Dimension: Attitude

Alarmingly only 1% users indicated that they check privacy policies of social networking sites. This poor attitude presents a big hurdle in safe and secure Internet usage.

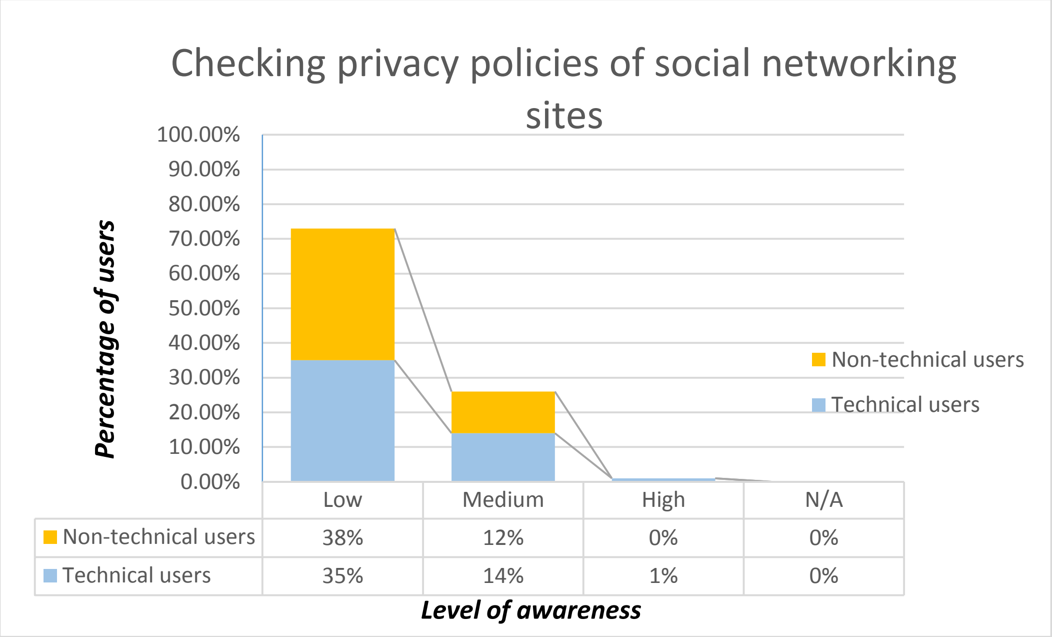


Figure 4.47: Checking privacy policies of social networking sites

5% users indicated that the average number of users whom they share personal information with online is ‘High’, 24% chose it to be low and remaining chose ‘Medium’ average number of users who they share personal information with.

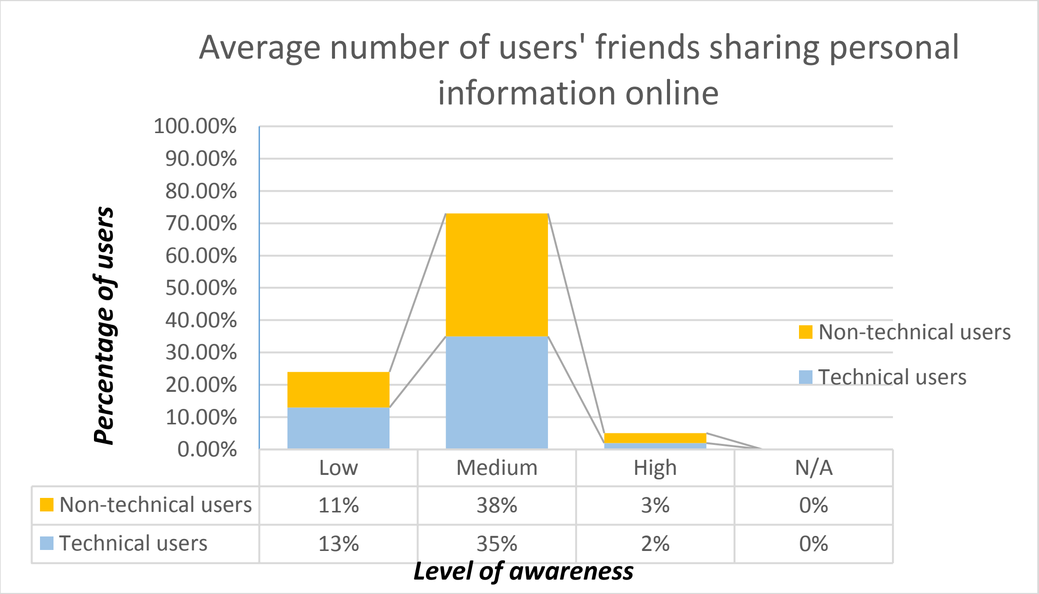


Figure 4.48: Sharing personal information online

4.3.9.3 Dimension: Behavior

Fig. 4.49 shows stats of frequency of leaving account unattended. Only 2% users indicated that they very often leave their account unattended (High) and 73% said that they never left their account unattended (Low).

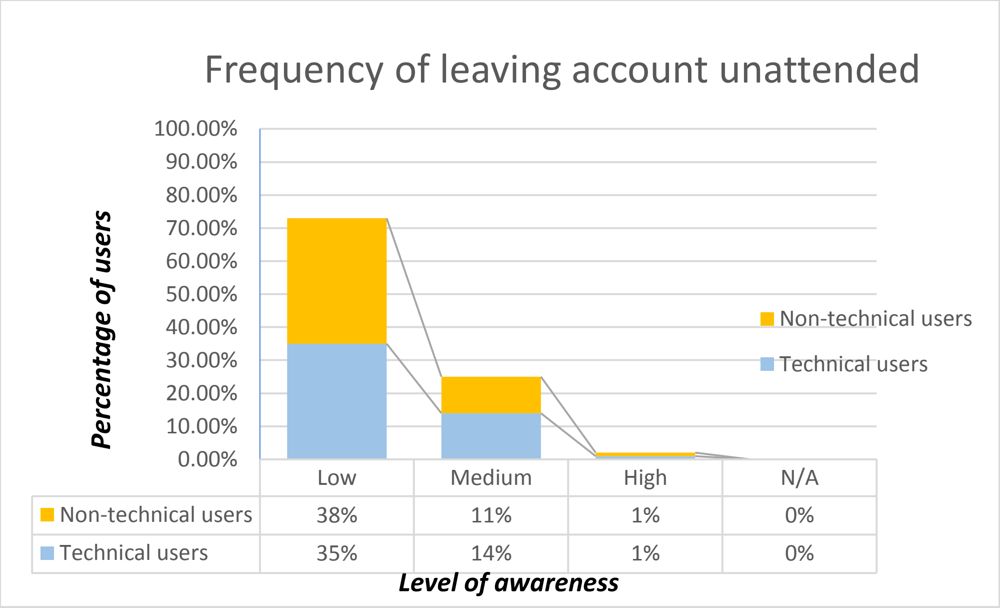


Figure 4.49: Frequency of leaving account unattended

4.3.10 Internet Usage

This section throws light on the daily internet usage of the users. The more the duration of internet usage, the more the threats the users are exposed to.

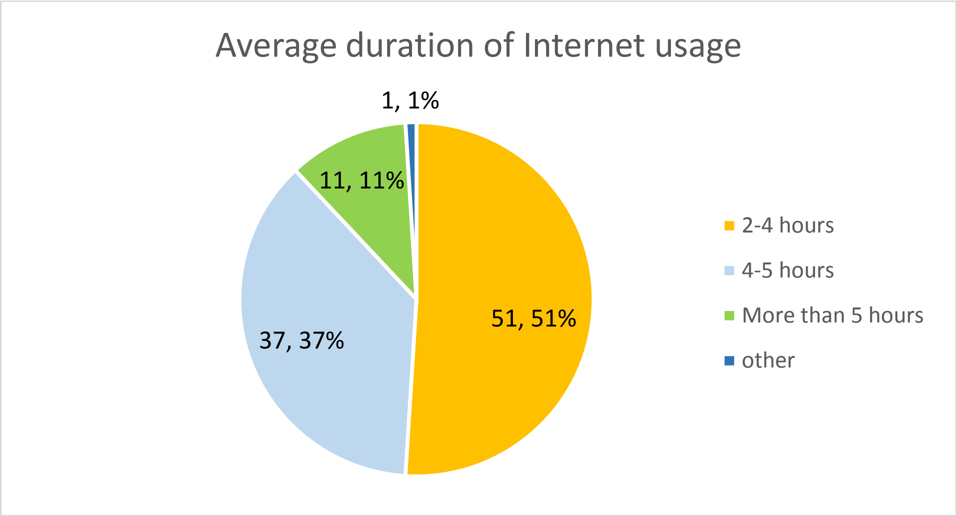


Figure 4.50: Average duration of Internet usage

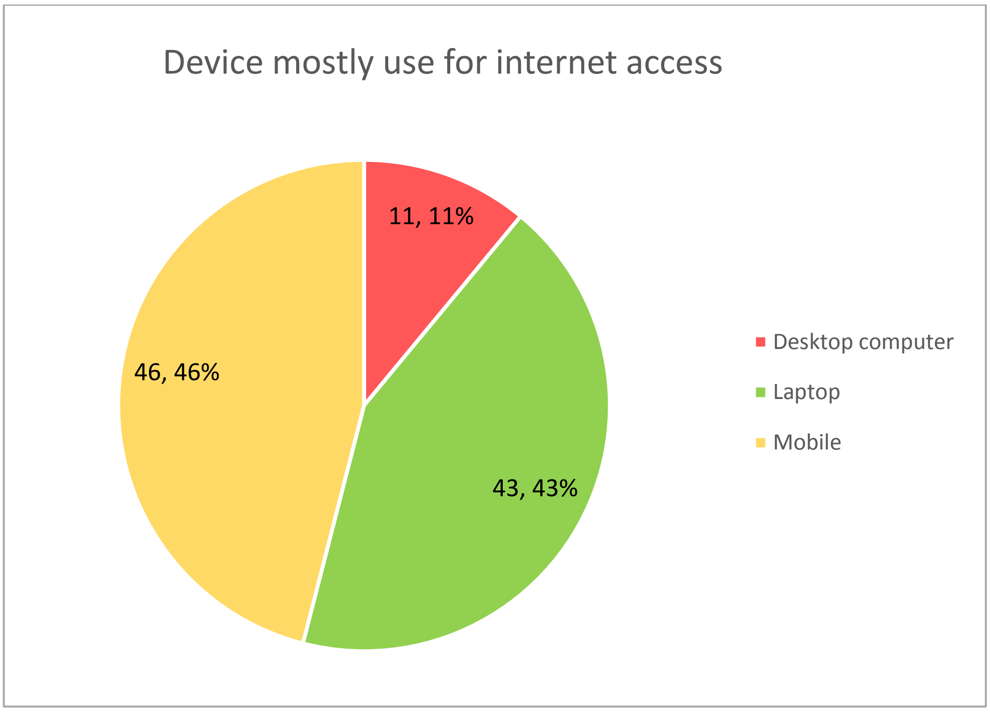


Figure 4.51: Stats of devices used for internet access

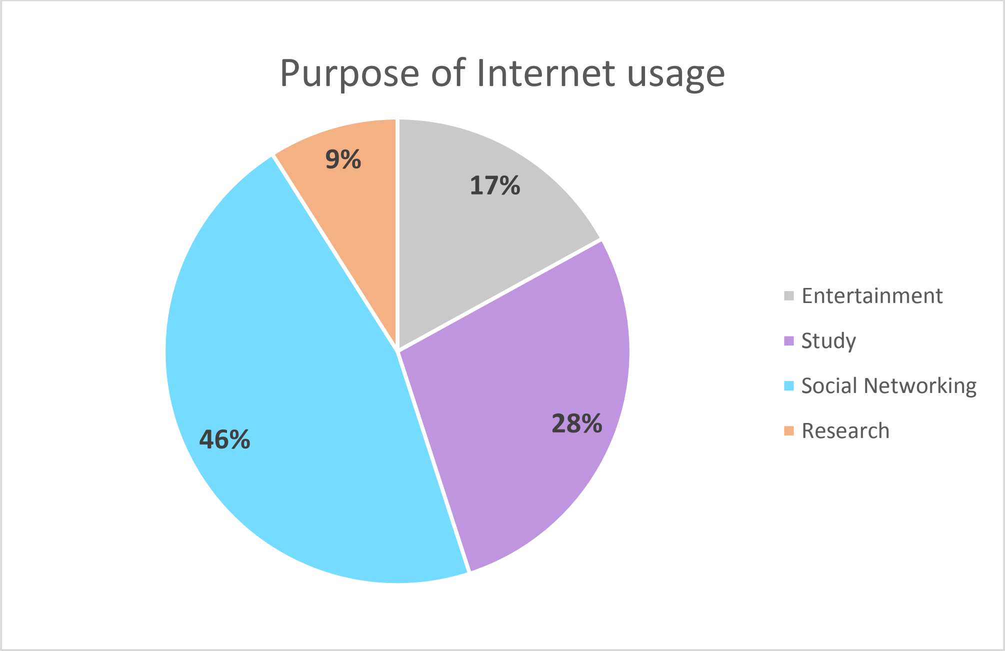


Figure 4.52: Internet usage purposes

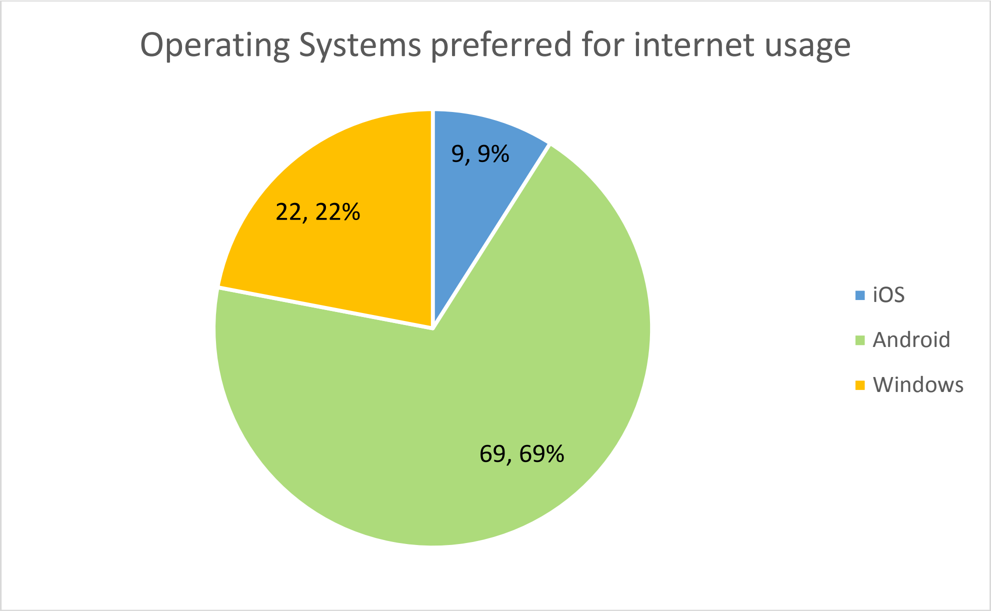


Figure 4.53: Operating Systems preferred for internet usage

The users were also asked to rate the social media in accordance with their usage which is shown in following graph. Facebook and Whatsapp are found to be most commonly used social media networks. ‘Other’ refers to any other social medium that the users use e.g. Line or Viber. None of the users however chose ‘Other’.

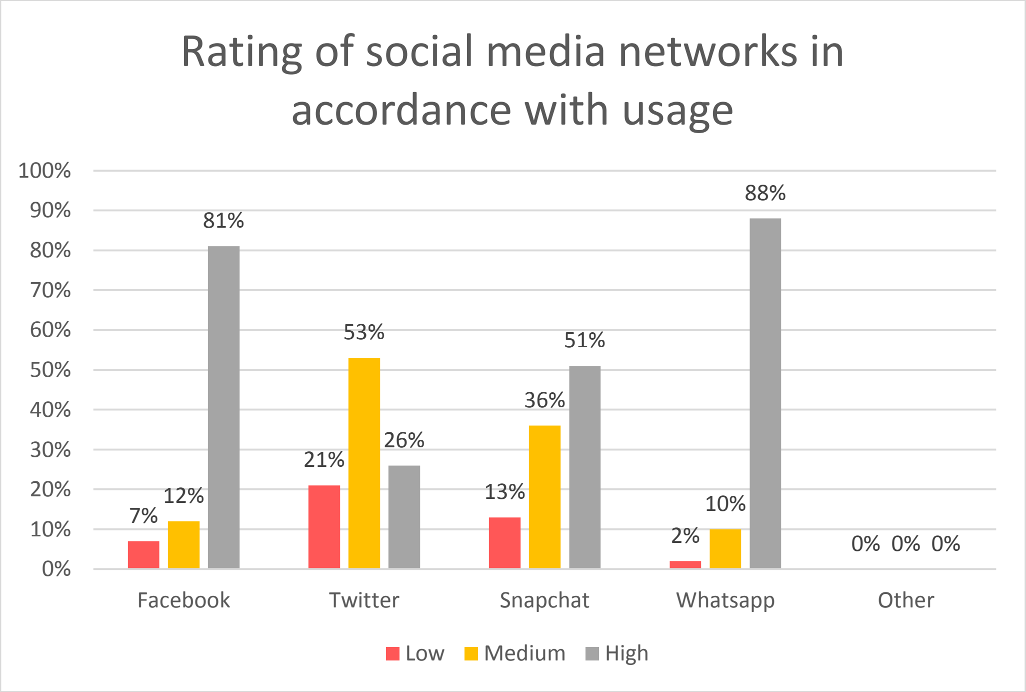


Figure 4.54: Stats of social networks usage

The users were also asked to rate the social media networks in accordance with the threats and attacks that they pose according to the users. The results show that most of the users found Facebook to be the most vulnerable networking site. Whatsapp stands second, Twitter third and Snapchat was rated to be least vulnerable according to the users. The 'Other' (any other social networking site) was left unanswered by all the users.

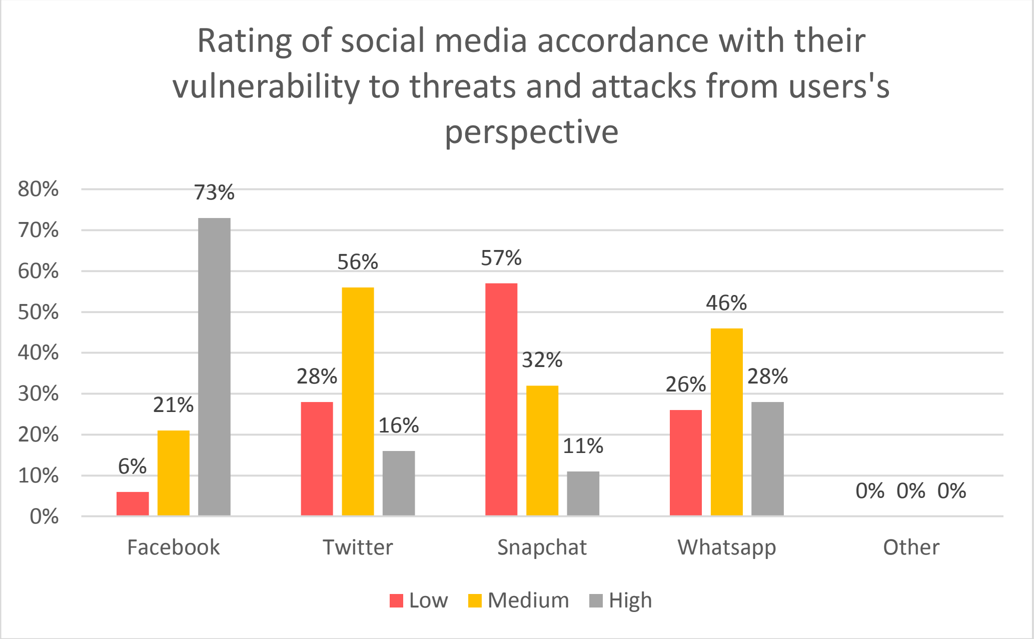


Figure 4.55: Stats of vulnerability of social networks from users' perspective

4.4 Survey Analysis

The survey conducted with the purpose of finding out the current state of awareness among the individuals basically provides the results of the risk assessment. Low awareness corresponds to High risk and vice versa. The final risk level was calculated as aggregate response of all the users. E.g. If 80% users showed 'High' awareness level in category 'Mobile devices' against the dimension 'knowledge, then the risk level in this particular category and dimension was concluded to be Low.

The term Risk here implies risk due to non-awareness to the users' privacy, confidentiality, security of computer systems, exposure to online frauds etc. Also the lack of awareness of one user brings the entire network he is connected to at risk. For instance, the user who is not very cautious of downloading files from the Internet can very well click on a legitimate looking malware. The malware after being executed can start lateral movement (hopping to other systems in the network) bringing entire network and IT assets to huge risk.

The final risk levels have been deduced against all three dimensions. There have been cases observed that in some categories, the user had reasonable knowledge about the area but his attitude (e.g. not considering security important) brings huge risk.

In all the areas except ‘Mobile devices’ the risk factor has been found to be high i.e. awareness level is below the reasonable threshold. In the ‘Mobile devices’ domain, the users have been comparatively found to be more cautious. The reason has been found to be high usage of Mobile phone. This also reflects that most users keep their personal information in their mobile phones.

Table 4.2 summarizes the overall risk associated with the ten cyber domains in all three dimensions. (Grey boxes represent dimensions for which exact awareness level could not be measured).

TABLE 4.3 RISK PROFILE DUE TO NON-AWARENESS

Cyber domains	Assessment Dimensions		
	Knowledge	Attitude	Behavior
General Awareness	Medium	High	High
Attacks and Threats	High	Medium	Medium
Email and Communication	High	High	Medium
General Security	Medium	High	Medium
Mobile Devices	Low	Low	Low
Privacy	Medium	High	Medium
Safe Browsing	Medium	Unknown	Low
Software Applications	High	High	Unknown
Social Networking	Low	Medium	Low

4.5 Conclusion

This chapter has compiled the results achieved from the survey conducted for the general users. The survey was categorized for both technical and non-technical users. The purpose of the survey was to assess the security consciousness of the users, their daily IT habits and their cautiousness towards the use of technology and the threats it brings. The survey has revealed some of the alarming facts about the current awareness level of the users in the domain of cyber/IT security. Following are the most striking observations:

- 47% of the survey participants indicated that they do not keep their software updated regularly.
- 53% of the users do not make use of the security settings on their computers
- 78% of the users are not very cautious of downloading files from the websites.
- 48% users are not well aware of the threats of USB drives.
- 92% of the users do not know what a spyware is i.e. they are not able to detect any software spying on their systems.
- 79% users do not know much about online frauds. In today's world where online frauds are more common than physical robbery, this level of negligence is pretty worrisome.
- 65% of the users are least cautious on providing personal information on Email.
- 55% of the users open the unsolicited attachments directly.
- 85% of the users make frequent use of public Wi-Fi.
- 46% of the users use internet mostly for social networking.
- According to the users, 'Facebook' is the most vulnerable social networking site.
- The risk factor for category 'Mobile devices' has been found to be low against all three dimensions. The awareness levels in all other domains are low enough to put users at risk. This risk needs to be addressed by providing enough awareness to the users in all the domains.

Chapter 5

CYBER SECURITY TRAINING PROGRAM FOR THE GENERAL USERS

5.1 Introduction

This cyber security training program contains the modules that provide learning to the general users who have interaction with the technology on daily basis. This program simply lays down the foundation of providing training to the technology users. This has been developed on the basis of the gaps in security awareness that have been identified in the survey. One cannot wholly depend on these modules to be completely cyber safe and secure. Security awareness is a continuous process. The requirements of the awareness/ awareness programs change with the everyday advancements in technology. However, this training program is capable of providing a good starting point to an individual.

5.2 Training program structure

The training program structure has been designed to map against the KAB model in order to address the awareness needs in all three dimensions. The training program structure starts with the basic introduction of the cyber domain under discussion to strengthen the dimension 'Knowledge'. The second component of the program is the background of the threats related to the particular cyber domain in order to strengthen the dimension 'Attitude'. The third component is the tips for the users to protect themselves, in order to mold their behaviors to security conscious behaviors.

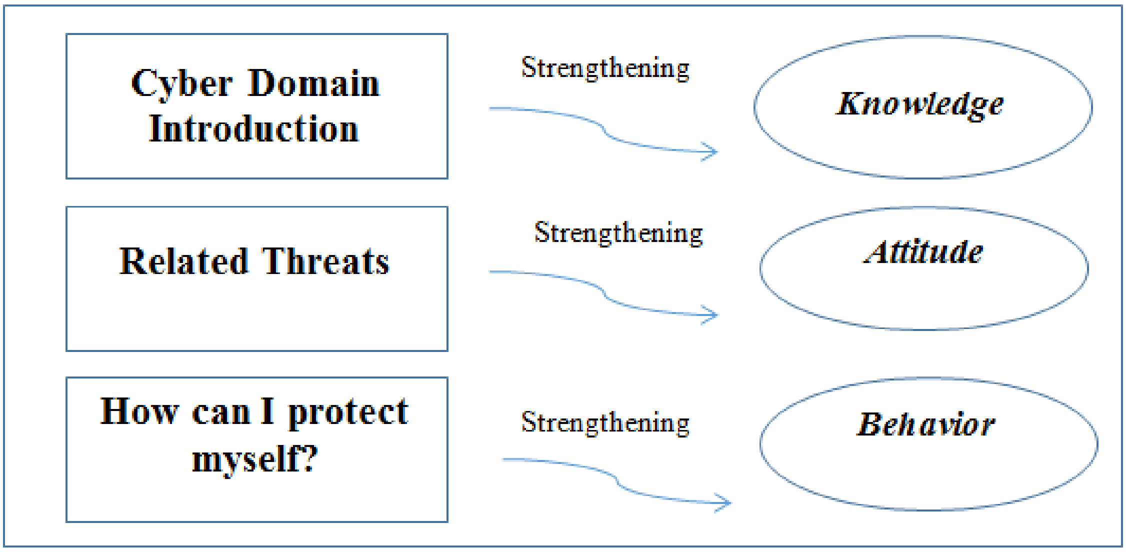


Figure 5.1 How Training Program is designed

Cyber domain introduction introduces the chosen area of cyber security awareness. It highlights the background of the particular area. The goal of this section is to introduce the users to the cyber domain before educating them on it i.e. strengthening their 'Knowledge' *Threats* section throws light on the threats and risks associated with the cyber domain under discussion. This section aims to make the users aware of the threats brought to them by the IT assets they daily interact with. This will tend to enhance their 'Attitude' towards security.

How can I protect myself is the main component of the training program. It focuses on tips and tricks for the users to help them stay conscious, safe and secure while using the technology. This will introduce more security conscious behaviors.

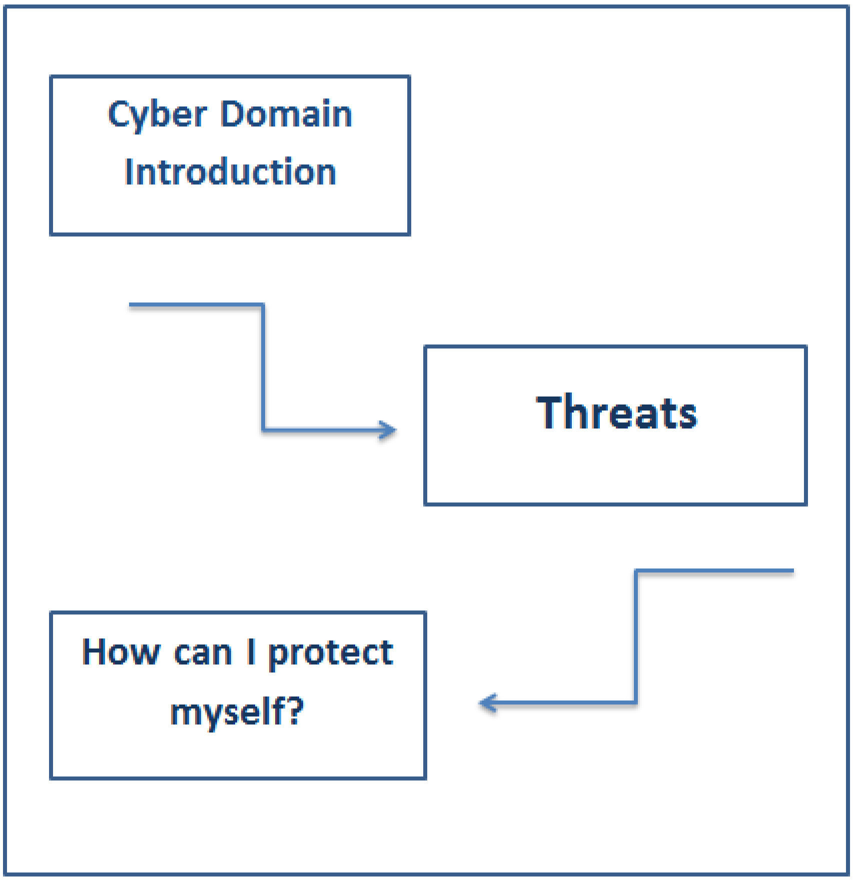


Fig 5.2 Training program structure

5.3 Training modules

Fig. 5.2 shows the ten basic components that the training program needs to be made up of according to the survey results. These ten components thoroughly cover all the aspects of security awareness. Educating the general IT users in all these areas will help them always stay safe and secure online. This program covers the introduction of the threats and attacks associated with technology, the details of safe email communication, prevention from account hacking, securing the home networks, use of strong passwords and securing personal user accounts, the ever rising concept of social engineering, backing up the data, safe online shopping, mobile devices and free security check-up and tools. Every area starts with the introduction followed by its associated threats and closes with the tips and tricks to prevent from the expected threats and attacks.

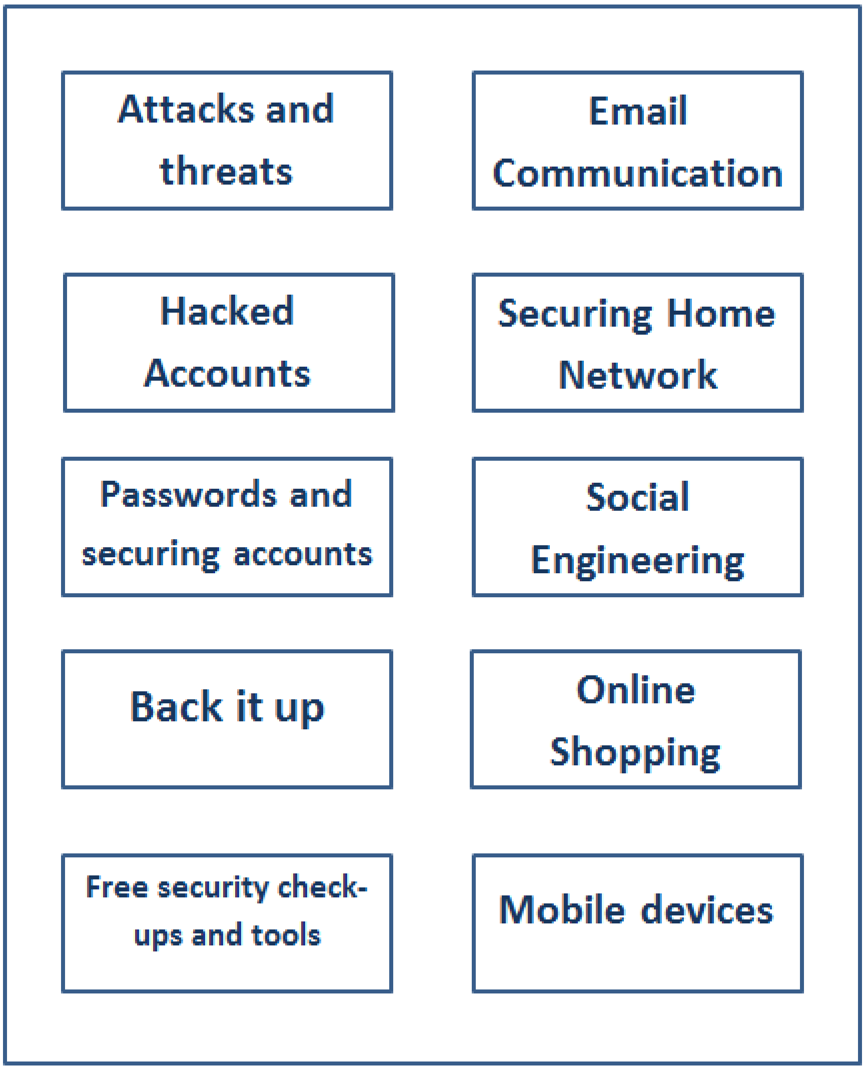


Fig. 5.3 Training modules

5.4 Attacks and threats

Internet is a powerful tool, but it’s not recommended to venture online without taking the important precautions. Following are the basic building blocks of the cyber threat environment.

5.4.1 A word about malware

The term malware comes from malicious software, any software that can infect your computer and gain unauthorized access to your personal information for nefarious purposes. Virus, worm, spyware etc. all are forms of malware.

5.4.2 Virus

Viruses are the harmful computer programs that can be made to propagate to other systems in various different ways. They are different in several ways, yet they all are crafted in such a way so as to enable them to propagate from one system to another Via the Internet causing harm to these systems. Above all, almost off of them are designed to help the criminals in accessing the infected computers.

5.4.3 Spyware

The terms "adware" and "spyware" refer to different technologies. Most noticeable things about these malicious software are:

- They have the ability to download themselves on victim’s computer without their permission (usually via an attachment or visit on an illegitimate website)
- They are able to make the victim’s computer perform the activities that they don’t want. They can be as simple as opening an ad/online commercial that one might not want to see, or even worse; the spyware has ability to spy on personal user activities, compromise their accounts and steal their passwords.

5.4.4 Key loggers

Key logging is the act of recording or monitoring the keys struck by a person on a keyboard usually covertly to keep the victim unaware. Numerous methods are available for this; both hardware or software. The key loggers are used by the cyber criminals to monitor the activities of a person mostly for the purpose of retrieving sensitive information which can be used for financial gains.

5.4.5 Botnets

Botnets are the malware infected networks of computers (Key loggers, virus, or some other malware) and remotely controlled by hackers, usually for purpose of financial theft or to launch cyber attacks against networks etc.

- If a computer gets infected with the botnet malware, it starts receiving the instructions about its course of action from the "command and control" servers that can be located anywhere across the world. The computer then acts in accordance with what the cyber criminals want to gain.
- Most botnets are crafted to exfiltrate sensitive data, like telephone numbers, passwords, addresses, social security numbers or credit card numbers, and other personal information. This data is then used for crime purposes or financial gain, such as credit card fraud, identity theft, website attacks, spamming (sending junk email), and malware distribution.

5.4.6 DoS attack

A **denial-of-service** (**DoS**) **attack** is an attempt to make a network resource or a machine authorized/unavailable to its intended users, such as to indefinitely or temporarily suspend or interrupt services of a host connected to the Internet. Denial of service is typically done by flooding the victim machine or resource with superfluous requests in an attempt to exhaust the resources or overload the systems and prevent the all legitimate users from availing the resources.

5.4.7 How can I protect myself?

- **Keep your security software updated:** To have the latest security software, OS (operating system) e.g. window and web browser is usually the most preferred defense against malware and other threats.

- **Whenever in doubt, throw it out:** The web links received in email, posts, tweets and the online advertisements are most common ways the cybercriminals adopt to steal your sensitive/personal data. If something looks unusual or suspicious, delete it, even if you recognize the source.

- **Protect the devices that are connected to the Internet:** In addition to computers, mobile devices, the gaming systems and other gadgets that are web-enabled need complete and thorough protection against malware.

- **Plug and scan:** Flash drives and other removable media can also be infected by worm, malware, viruses. Use updated security tool or anti-virus to scan them.

5.5 Safe Email communication

Email has become a common medium for attackers/hackers to steal the users' personal data. By sending spam emails and getting their responses, the hackers can compromise users' confidentiality.

5.5.1 Spam

Spam can be defined as the electronic junk mail. It is basically unsolicited/uninvited email.

5.5.2 How can I protect myself?

Here are some tips to defend against spam:

- **Enable filters on the email programs:** Most email providers and ISPs offer this service of spam filters. Depending on the level you set, you can always filter the emails you want usually categorized as 'Important and Unread', 'Everything' etc. It's a strongly recommended to frequently check the junk folder to make sure that the filters are properly working as expected.
- **Own your online presence:** Prefer not to share your personal or official email address on the online profiles, the social networks websites and allow only selective people to view the personal information you put there.
- **Reporting spam:** Mostly email programs offer this service of marking an electronic mail as spam or report the indicators if observed. This reporting will also help in preventing the emails from directly being delivered to you.

5.6 Social engineering

Cybercriminals have now become very mature in their attempts to trick or lure people and have them click on an illegitimate link or open any suspicious attachment. The email that

they send looks just like it came from a legitimate source like some relevant business organization, some government agency, or some other related service.
It mostly provokes you into responding immediately, since the account has now been compromised, the request cannot be served.

5.6.1 How can I protect myself?

If you need to verify the authenticity of an email, do the following:

- Contact concerned organization directly.
- In case of a financial matter, contact the concerned organization using the information provided by them on an account statement or on the back of the credit card.
- Search for the organization using their official website online –and not with the information provided to you in the suspicious or unsolicited email.

5.6.2 Phishing

Phishing is type of a social engineering attack. Phishing attacks exploitation ways like email or malicious websites (clicking on a link) to collect sensitive financial and personal information to infect your machine with viruses and malware.

5.6.3 Spear Phishing

Spear phishing is type of a highly specialized attack that is launched against a particular target to collect sensitive data in order attain access to critical IT assets.

For instance, a cybercriminal may launch a spear phishing attack for a health care center to gain access to sensitive patients' records. From this attack, they can launch another phishing attack against those patients by sending them information in the email that they will be familiar with along with a legitimate looking malicious link which they will tend to trust and click and ultimately getting hacked.

The cybercriminals can take even more dangerous social engineering steps such as offering a fake service online and luring victims into sharing their very personal information themselves.

5.6.4 Spam & Phishing on Social Networks

Social engineering attacks like phishing, spam and other kinds of scam are not only limited to email but these threats are applicable to social network websites too. The rule: "When in doubt, throw it out" is applicable to social networking websites too and also applicable to the links in tweets, online ads and forums and other posts.

Here are links to report and fight spam on social network sites:

- Reporting phishing and spam on Facebook https://www.facebook.com/help/205730929485170
- Reporting spam on Twitter https://support.twitter.com/groups/33-report-a-violation/topics/122-reporting-violations/articles/64986-how-to-report-spam-on-twitter
- Reporting spam and phishing on YouTube https://www.youtube.com/yt/policyandsafety/?hl=en&rd=1

How can I protect myself?

- **Don't ever reveal personal/financial information in an email**. Avoid responding to unsolicited emails that ask for any personal information. Before sharing or sending sensitive information on the Internet, **verify the security of the website**.

- **Always pay attention to website's URL.** There is less difference between the look of malicious websites and legitimate sites, but the URLs may help. It may have a change in spellings or a may have a not so similar domain.
- **Try to verify the doubtful email by contacting the relevant company directly** if you are uncertain whether an email is legitimate. Do not contact the company using information provided in the email, instead use the information provided on an account statement.

Following are some useful links that provide information about known phishing attacks:

Anti-Phishing Working Group.
http://www.apwg.org/

Report phishing to the Anti-Phishing Working Group (APWG)
http://apwg.org/report-phishing/

- **Keep your machine clean.** Having the latest security software, operating system e.g. window and web browser is usually the best defense against malware, worm, viruses and other online threats.

5.6.5 How should I respond if I Think I am a Victim?

- **Report it to the appropriate people** in the enterprise that include systems and network administrators. These people can be notified about any unusual, anomalous or malicious activity.
- If you doubt that your financial accounts are compromised, c**ontact your financial organization immediately** and get the account(s) closed.
- **Watch for the unauthorized charges** to your account if any.
- **Consider reporting the attack** to and file a report with the Federal Intelligence Agency complaint center.

Additional Resources:

- Anti-Phishing Working Group
- United States Computer Emergency Readiness Team (US-CERT)
- OnGuardOnline.gov

How can I protect myself?

- **Make your password a sentence**: The strength of the password depends on mainly length. It should be a sentence with length of 12 characters at the very least. Prefer positive phrases or sentences or that are easier or which you personally like to think about to (for example, “Nothing like home.”). You can even use spaces on many sites. It’s strongly recommended to include special characters as well. Also the ideal password is a combination of capital letters, small letters, numbers and special characters.

- **When in doubt, throw it out:** The links you receive in email, posts, tweets the and online advertisements are the most common ways the cybercriminals adopt to steal your sensitive/personal data. If something seems suspicious, delete it, even if the source is known.

- **Think before taking action:** Be conscious of the messages or emails that provoke you to respond instantly or anything that offers something sounding too good in your favor or something that asks for any personal level information.

- **Unique account, unique password:** A different password for every account assists in defeating hackers/attackers. At the very least, segregate your personal and work accounts and ensure that at least your sensitive account has the unbreakable password.

- **Go two steps ahead**: Most security focused sites today offer two-step or two-factor authentication. Turn on two-step authentication – also called multi-factor authentication or two-step verification wherever available. Two-factor verification can use anything from a biometric like fingerprint to a code sent in text message on your phone in order to provide enhanced account security.

5.7 Hacked accounts

If you suspect that your account has been hacked or compromised, here are some useful tips to get it recovered.

5.7.1 How to figure out if the social network account or email account has been compromised?

- There will be posts or updates that were never made by you on your profile. These updates/posts mostly trick your social network contacts to click on a particular malicious link or into downloading an App.

- A family member, an acquaintance or a work colleague might report about receiving an email which was not sent by you.

- Your personal information was lost through a stolen device, security breach or any other cyber attack.

If you suspect your account to be compromised, take the following steps:

- Inform your contacts about the spam messages that they may receive seem to originate from your account. Warm them about the consequences of opening these messages or about tapping on any connections from the record following by and cautioning them about the potential danger of this malicious software.

- If you suspect your computer to be malware infected, ensure that your security software is updated and scan the system for any potential malicious software. The security tools given at the end of this chapter may be used for this purpose.

- Change the passwords of the accounts that are suspected to be compromised with other important accounts as soon as possible. Remember, passwords should be a mixture of lower uppercase letters, and digits and special characters and must be long enough and strong. It’s highly recommended to have a different password for each account.

If you are not able to access your online account due to change in password by the hacker, contact the web service instantly and follow the steps given by them to recover the hacked account. Following table shares some useful links in this regard.

Table 5.1 Useful resources to prevent account hacking

eBay	Help with eBay mail violations http://pages.ebay.com/help/account/unwanted-email.html
	Help with a hacked account http://pages.ebay.com/help/account/securing-account.html
	Help with inappropriate trading http://pages.ebay.com/help/buy/report-trading.html
	eBay Security Center http://pages.ebay.com/securitycenter/index.html
PayPal	Help with suspicious emails https://www.paypal.com/us/webapps/mpp/security/suspicious-activity#email_from_paypal
	Help with a hacked account

	https://www.paypal.com/us/webapps/mpp/security/report-problem
	PayPal Security and Protection Center https://www.paypal.com/webapps/mpp/paypal-safety-and-security
Facebook	Help with cyber bullying and impostor profiles https://www.facebook.com/help/263149623790594
	Help with a compromised account https://www.facebook.com/help/149190625213449
	Facebook Help Center https://www.facebook.com/help/
Gmail/Google	Help with a hacked account https://support.google.com/mail/answer/50270?cbid=1uslv13hx7tyw&src=cb&lev=answer
	Help with an inaccessible account https://accounts.google.com/signin/recovery?hl=en&rd=1
	General safety tips https://support.google.com/mail/?hl=en#topic=7065107
Twitter	Help with a hacked account https://support.twitter.com/articles/185703
	Help with an inaccessible account https://support.twitter.com/groups/33-report-a-violation/topics/122-reporting-violations/articles/185703-my-account-is-compromised-hacked-and-i-can-t-log-in
	Twitter Safety Center: http://staysafeonline.org/_admin/pages/body/%20https:/support.twitter.com/groups/33-report-a-violation/topics/166-safety-center/articles/76036-safety-keeping-your-account-secure
Yahoo	Help with a hacked account https://help.yahoo.com/kb/SLN2090.html
	To-do steps to stop sending of spam https://help.yahoo.com/kb/account/SLN3417.html?impressions=true
	Help Center https://help.yahoo.com/kb/helpcentral
Outlook	Help with a hacked account

	https://www.microsoft.com/en-us/safety/online-privacy/hacked-account.aspx
	Hotmail Help Center http://hotmailhelp.co.uk/
YouTube	Help with cyberbullying https://support.google.com/youtube/answer/2802268?hl=en&rd=2
	Help with flagging a spam-based video https://support.google.com/youtube/answer/2802027?rd=1
	Help with a hacked account https://support.google.com/youtube/answer/76187?hl=en
	YouTube Safety Center https://www.youtube.com/yt/policyandsafety/?hl=en&rd=2

5.7.2 How can I protect myself?

- Keep your security software updated
- Make your password a sentence
- Use ‘unique account, unique password’ strategy
- When in doubt, throw it out

5.8 Securing the home network

A secured home network is about your family’s safe secure Internet use. Most houses have the networks of devices running that are connected to the Internet, that mainly include laptops, tablets, smartphones, computers, laptops and gaming devices that have access to wireless networks. For securing the home network and protect your people online, you must have knowledge of using the required tools and ensure that everyone can browse safely.

The foremost step is to keep a system clean from any infections and ensure that all of the Internet-enabled devices have the updated operating system, current software and updated web browsers. This also includes the mobile devices that have access to public network.

5.8.1 How can I secure my wireless router?

A wireless network is connection to an Internet AP (access point) – like a DSL modem or a cable. Going wireless is a very convenient way to let multiple devices connect to the

Internet remotely from different areas of your house. However, you remain vulnerable to the individuals accessing information on your computer, by using your free Internet service and using your network potentially to conduct cybercrime, unless you secure your router.

Here are some tips to secure your wireless router:

- **Change the name of your router:** The default router ID - called “extended service set identifier” (ESSID) or simply service set identifier” (SSID), is assigned by the router manufacturer. Change this SID to a name that is unique to you and is difficult for others to guess.

- **Change the password pre-set on your router:** When creating a new password, make sure it is strong. The strength of the password has been defined in the previous section.

- **Review security options:** When selecting the router’s security level, go for WPA2, if available, or else WPA. The WEP option is comparatively less secure.

- **Setup a guest network:** Some routers allow the use of network for guests using a separate password. It’s a recommended to set up a guest network if you have many visitors in your home.

- **Use a firewall:** Firewalls prevent hackers from using your computer to access your personal data without your permission. A firewall is just like a guard that watches for unauthorized attempts to your system and blocks communications with hosts you don't allow, just as the anti-virus software scans incoming files and email. Your security software or operating system mostly comes with a pre-configured firewall, but be certain that you turn on these features.

- **Keep the security software updated:** To have the updated security software, application or operating system e.g. window and web browser is the most preferred defense against any malware and all online threats.

- **Protect the devices that are connected to the Internet:** In addition to computers, mobile devices, the gaming systems and other gadgets that are web-enabled need complete and thorough protection against malware.

- **Plug and scan:** Flash drives and other removable media can also be infected by worm, malware, viruses. Use updated security tool or anti-virus to scan them.

- **Protect your money:** In shopping online and banking, make sure that the site is security enabled. Check the web addresses with "https://", which means the site is taking additional precautions in securing your data by encryption. "https://" provides security by encryption. "http://"does not encrypt the data hence it has no reliability in terms of security.

- **Back it up:** Protect your valuable data; photos, music, and other digital information by making an electronic copy and store it safely.

5.9 Passwords & accounts security:

Passwords are more like a key to one's personal briefcase. You must take necessary steps to prevent anyone from accessing your password. Furthermore, authentication methods can also be used for security of online accounts.

5.9.1 Passwords

Passwords might be inconvenient, but they're very important if you want to keep your information safe. Take necessary security measures, know the consequences of your actions online and use the Internet without worries. Following are some simple tips to protect your accounts through good password practices.

- **Strong password:** A strong password must be a combination of capital and small letters, numbers and symbols.

- **Unique account, unique password:** A different password for every account assists in defeating hackers/attackers. At the very least, segregate your personal and work accounts and ensure that at least your sensitive account has the unbreakable password.

- **Write it down and keep it safe**: It is normal forgetting a password. Prepare a list which is kept in a secure place and not close to the computer. Alternatively, the services like password manager can also be used in order to keep tracking the passwords.

5.9.2 More ways for account security

Typing your username plus password into a website is not the only method of your identification on web services used by you.

- **Go two steps ahead**: Most security focused sites today offer two-step or two-factor authentication. Turn on two-step authentication – also called multi-factor authentication or two-step verification wherever available. Two-factor verification can use anything from a biometric like fingerprint to a code sent in a message on your phone in order to provide enhanced account security.

5.10 Online shopping

It is extremely important to take precautions to protect yourself while shopping online. Anything that gets connected to the Internet including tablets and mobile devices like smartphones needs to be protected. Hackers, cybercriminals and scammers can target the online shoppers as well. Everyone must be conscious or on alert for the emails that lure us to act quickly and click on links to open the attachments. Beware of emails that discuss problems with your credit cards or the status of any online order. The hackers know that people are price sensitive when it comes to online shopping. Exercise caution when you see an ad or an offer where the price or the discount is unusual or is much below normal. Take necessary security measures, know the consequences of your actions online and use the Internet without worries while you shop online. Always remember these tips during all of your online purchases.

5.10.1 How can I shop online safely?

- **Do some research:** Whenever you use a website for first time for online purchases, must go through the reviews and check if other users have had a negative/positive, good or bad experience with that particular website.
- **Whenever in doubt, throw it out:** The links you receive in email, tweets the and online advertisements are most common methods the attackers adopt for reaching the sensitive/personal data. If something seems suspicious, delete it, even if the source is known.
- **Personal information is worthy: protect it and value it:** While making an online purchase, beware of the type of information being collected in order to complete the transaction. Be certain that it is mandatory and relevant for the vendor requesting that information.
- **Use safe payment options:** Mostly the safer option for payment is credit cards since they allow customers to seek credit from the issuer in case the product is not delivered or if does not match the order requirement.
- **Don’t be disappointed:** Do read return and other polices just so you know what to expect if the purchase does not go according to the plan.

5.10.2 Shopping On the Go:

- **Now you see me, now you don’t:** Most shops/stores and other locations scan the devices with Wi-Fi or Bluetooth switched on to track users’ whereabouts while they being within their range. Turn off Wi-Fi and Bluetooth when not in use.
- **Get savvier with Wi-Fi hotspots:** Restrict the business type conducted by you over the public Wi-Fi connections, including signing into key accounts, such as banking and email. Customize the security settings on your device to limit the access on your phone.

5.11 Back it up

Protection against the loss of data by making electronic copies of user’s important files is called Data backup. Our computers hold huge amounts of data, from music collection to family photos and financial records to personal contacts. Data can be lost in several ways:

hacking, theft, computer malfunctions, viruses, accidental deletion, spyware and natural disasters.

Data backup is a simple, three step process:

- Make copies of your personal data
- Select the suitable hardware to store your data
- Copy the data to the backup device and safely store it.

5.11.1 Make Copies of Your Data

Most computers come with a pre-installed backup software program. Check to see if you have one. Most of the backup software will allow you to make copies of every file and program present on your computer, or just the files you've updated since your last backup.

Here are some useful links to backup utilities in popular operating systems:

- Mac OS X Leopard
  http://www.apple.com/mac/#backup
- iCloud for Apple iOs devices (iPads, iPhones, iPod touch, etc.)
  https://support.apple.com/en-us/HT203977

- Windows 7
  https://support.microsoft.com/en-us/products/windows?os=windows-7
- Windows Vista
  https://support.microsoft.com/en-us/products/windows?os=windows-7

Hardware:

- Apple Time Capsule
  http://www.apple.com/airport-time-capsule/
- Windows Home Server 2011
  https://support.microsoft.com/en-us/allproducts

5.11.2 Select Hardware to Store Your Data

When you conduct the backup of your data, the files will have to be stored on a physical device - such as DVDs, CDs, or USB flash drives, an external hard drive, or on the web using cloud-based storage service.

- **CDs, DVDs and USBs:** These are most suitable for storing a small amount of data, music, picture and videos.
- **External hard drive:** If your computer acts as the family music library and photo album, it is recommended to get an external hard drive that can be plugged into your computer (preferably through a USB port). This way, you can have sufficient storage space for all the files. Also copying data will is faster with these devices.
- **Online backup services:** If you don't want to face hassle with new hardware, there are many online backup services available. You simply have to backup or copy your files to a secure server over the Internet. These services offer the advantage of storing your files on a remote location safely and the files can be accessed from anywhere as long as you have a connection to the Internet.

5.12 Mobile devices

The devices like your laptop, tablet or that smartphone in your pocket holds huge amount of personal information including but not limited to – photos, address book, location, documents etc. Your mobile devices also need to be protected. Take the following minimum security precautions and enjoy the taste of technology without having to worry for privacy issues.

- **Keep the security software updated on your mobile devices:** Having the latest security software, operating system e.g. window and web browser is usually the best defense against malware, worm, viruses and other online threats.

- **Delete it all when done:** We usually download apps for different purposes and then they're not needed anymore or we might have initially installed apps that are not needed anymore. It's a recommended practice to delete all the apps that are of no significant use to you anymore.

5.12.1 Protecting Personal Information

- **Secure your mobile devices:** Make use of strong passcodes, passwords and other security features like touch or face identification to lock your devices. Securing your device this way will help you protect your information in case your device is stolen or lost and will keep your data hidden from the prying eyes.
- **Personal information is worthy: protect it and value it:** While making an online purchase, beware of the type of information being collected in order to complete the transaction. Be certain that it is mandatory and relevant for the vendor requesting that information.
- **Own your online presence:** Make use of privacy and security settings on apps and websites to manage what information owned by you are available to whom.
- **Beware of getting tracked:** Most shops/stores and other locations scan the devices with Wi-Fi or Bluetooth switched on to track users' whereabouts while they being within their range. Turn off Wi-Fi and Bluetooth when not in use.

5.12.2 Connect with Care

- **Get savvier with WiFi hotspots:** Public wireless networks and hotspots have least security for users. This means that anyone's activities and locations can be tracked the moment they are connected to them. Best practice is to limit activity on public WiFi, and log in to key accounts on need basis. Usage of a private network (VPN) is the most preferred practice if there is any urgency of logging into any financial services.
- **Whenever in doubt, do not respond:** Online frauds are on the rise today. Fraud text messages, voicemails and calls have become common. Like the email, requests for personal information on mobiles are mostly scam.

5.13 Free security tools and check-ups

Many well-known computer security vendors offer free computer security check-ups for checking health of IT systems.

Following links can be visited for checking the computer for known malware, spyware, viruses, worms etc. to look for possible existence of any vulnerabilities.

- AOL Computer Checkup
- Audit My PC
- avast! Free Antivirus (for PCs)
- avast! Mobile Security (for Android)
- AVG AntiVirus FREE 2015
- BitDefender
- Cloudbric Comprehensive Website Protection Service (Free up to 4GB)
- ESET Online Scanner
- iScan Online Security Awareness Scan
- Kaspersky Virus Scanner
- McAfee Security Scan
- Microsoft Safety Scanner
- nCircle PureCloud Vulnerability Scanner
- Norton Security Scan
- OPSWAT Free Security Tools
- Panda Security Antivirus Scan
- Qualys Browser Check
- QualysGuard Malware Protection
- Secunia PSI
- Sophos Free Security Tools
- StopTheHacker Free Application Vulnerability Scan
- Symantec Security Scan
- Trend Micro HouseCall Virus Scan
- Trend Micro Security Assessment
- Vipre Internet Security 2013
- ZapFraud

5.14 Conclusion

This chapter has presented cyber security training program for the general users. The training program structure is divided into three components, namely 1) Cyber domain introduction', introducing the users to the area under discussion, 2) Threats, discussing the threats and attacks associated with that particular domain and 3) 'How can I protect myself', highlighting tips and techniques to prevent from these attacks and threats. The training program is divided into ten cyber domains that thoroughly address the security awareness needs from all angles.

These tips and techniques are not enough to call it a comprehensive and complete training program but they do provide a broad outline to kick start an effective training of users on safe use of technology.

Chapter 6

CYBER SECURITY ROLE-BASED TRAINING PROGRAM FOR THE IT STAFF

6.1 Introduction

This chapter presents the main component of this research i.e. the security training program for the IT community. The training program has been built according to the NIST training model (SP 800-16). The training modules have been customized according to the survey conducted for all necessary IT roles in different institutes. The main significance of this training program is the prevention from the hassle of training the individuals in the domains they do not hold significant responsibility in. The individuals can be trained only in the domain that is required for their particular job role. This prevents the individuals from over consumption of the material which is not of their interest and also prevents the individuals from being deprived of the training material that is necessary to be consumed by them. The survey and program methodology both have been discussed in detail. The training modules are made up of the knowledge units for four different functional perspectives namely; '*manage', 'design', 'implement'* and '*evaluate',* totally fit for the type of the job role an individual occupies.

6.2 IT Staff Survey methodology

The IT position holders from different universities were surveyed via questionnaires and interviews and data was collected in detail. The survey is based on following five components of employees:

- The roles they perform,
- The experience they have in that particular role
- Their minimum qualification
- The tasks related to their roles
- The skill set that they currently possess

The final training modules are built on all these parameters. The final results are aggregate of the responses from all the institutes. (Appendix-C)

6.3 Training program methodology

The program is based on “NIST model (SP 800-16) and NICE National cyber security workforce framework”, and contains three-tiers; namely *functional area*, *role area* and *roles*. The training modules are based on the tasks that are associated with each role and further the functional perspective i.e. the nature of each task; manage, design, implement and evaluate (explained later) for each role. The skill set with different IDs is customized for each functional perspective according to the need of the role. However, the modules can anytime be amended according to the change in the tasks associated with the role.

6.3.1 Functional area

The functional area is a special security area which further is categorized into role areas. This program is based on five functional areas that have been selected from a wide range based on the needs of the academic sector. The five functional areas that cover the roles related to the academic community are following:

- **Securely provision:**
  This includes the specialty areas that are responsible for conceptualizing, designing, and building secure information technology systems i.e. responsible for some aspect of systems development.
- **Protect and defend:**
  This includes functional areas responsible for identifying, analyzing and mitigating the threats to critical IT assets.
- **Operate and maintain:**
  This includes specialty areas responsible for providing support, administration and maintenance necessary to ensure efficient and effective IT systems security and performance.
- **Oversight and development:**
  This includes specialty areas responsible for providing leadership, direction, management, advocacy and development, so that the individuals and organization may perform the cyber security work effectively.
- **Investigate:**
  This includes specialty areas that are responsible for the investigating the cyber crimes and events relevant to IT assets, network and forensic evidence.

6.3.2 Role area

The role area basically identifies the roles that the specific area covers. Each functional area is further divided into related role areas.

6.3.3 Roles

All the positions that have some sort of IT related responsibility.

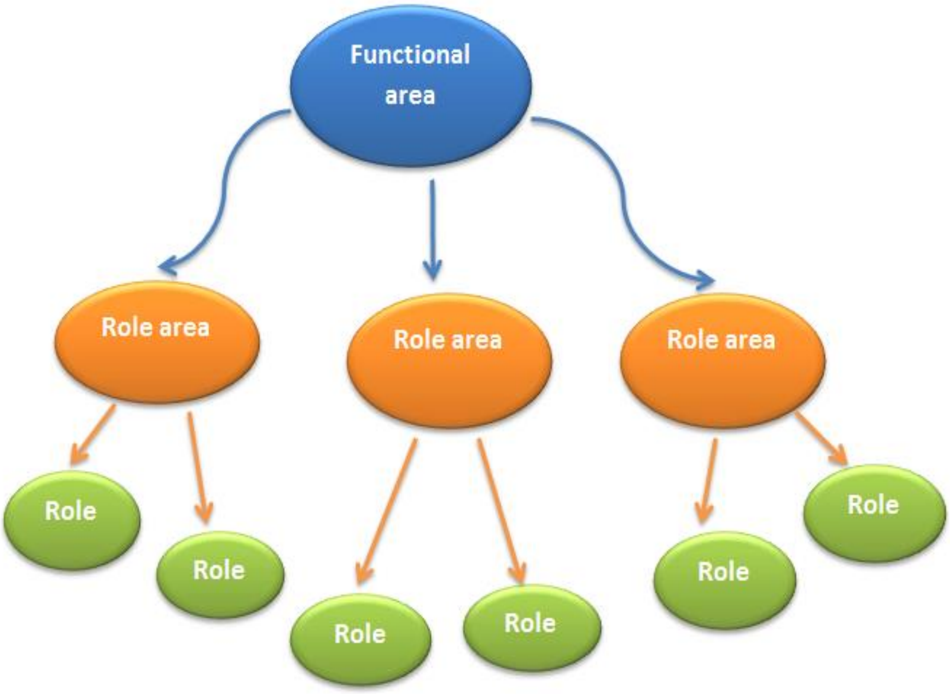


Fig. 6.1 Program hierarchy

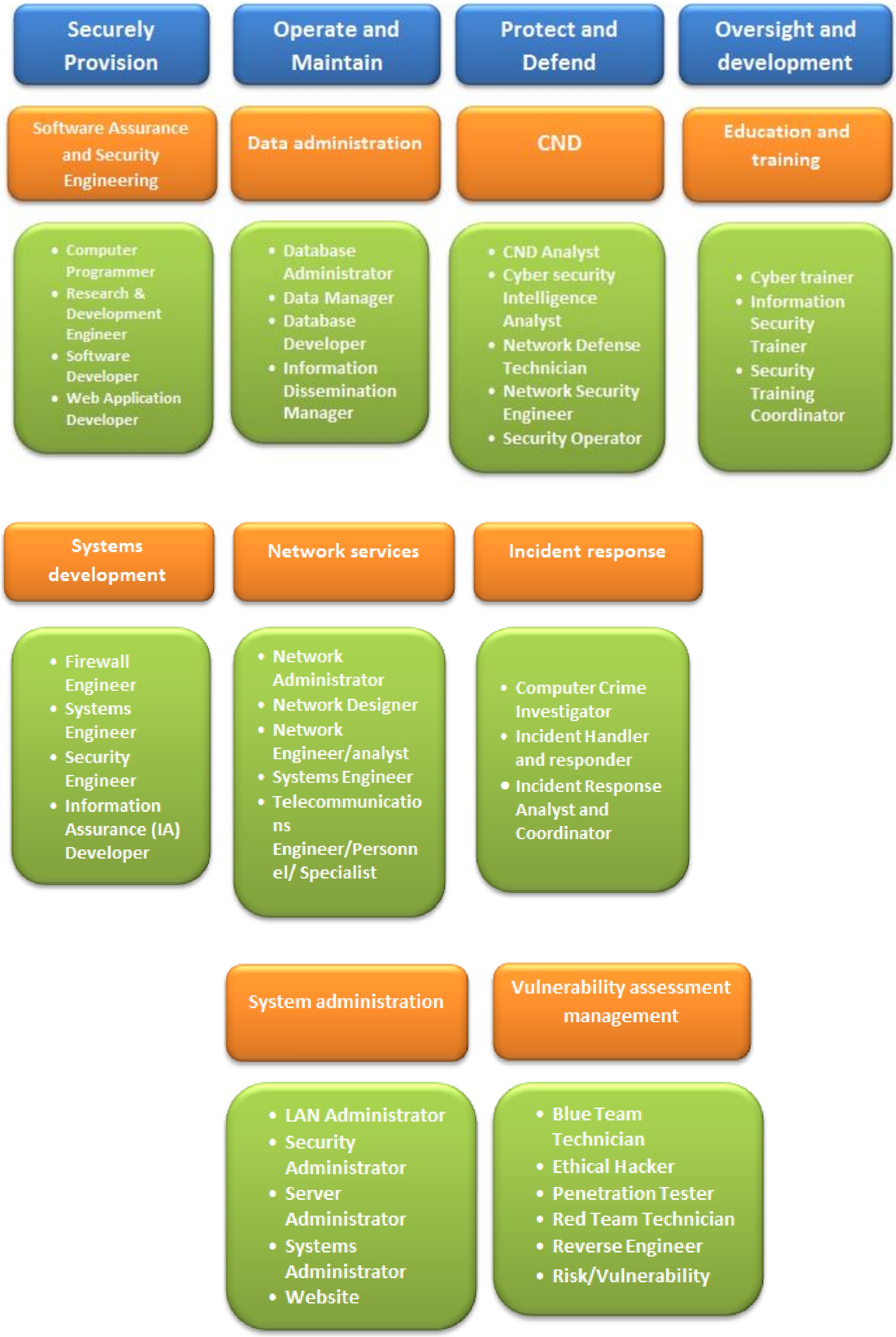
6.3.4 Three-tiered security training model

The first two functional areas; ‘Securely Provision’ and ‘Operate and maintain’ are currently functional in the academic institutes. The third and fourth functional areas are meant for the institutes that running CSIRTs, CERTs or some sort of security cells.

Tier 1 – Functional areas

Tier 2 – Role areas

Tier 3 – Roles



Securely Provision

Operate and Maintain

Protect and Defend

Oversight and development

Software Assurance and Security Engineering
- Computer Programmer
- Research & Development Engineer
- Software Developer
- Web Application Developer

Data administration
- Database Administrator
- Data Manager
- Database Developer
- Information Dissemination Manager

CND
- CND Analyst
- Cyber security Intelligence Analyst
- Network Defense Technician
- Network Security Engineer
- Security Operator

Education and training
- Cyber trainer
- Information Security Trainer
- Security Training Coordinator

Systems development
- Firewall Engineer
- Systems Engineer
- Security Engineer
- Information Assurance (IA) Developer

Network services
- Network Administrator
- Network Designer
- Network Engineer/analyst
- Systems Engineer
- Telecommunicatio ns Engineer/Personn el/ Specialist

Incident response
- Computer Crime Investigator
- Incident Handler and responder
- Incident Response Analyst and Coordinator

System administration
- LAN Administrator
- Security Administrator
- Server Administrator
- Systems Administrator
- Website

Vulnerability assessment management
- Blue Team Technician
- Ethical Hacker
- Penetration Tester
- Red Team Technician
- Reverse Engineer
- Risk/Vulnerability

Fig. 6.2 Three-tiered security training model

6.4 Program body

The training program body is composed of the role areas, roles, the tasks associated with a particular role, the knowledge unit and the functional perspectives. The relationship of all this components has been explained in detail below.

6.4.1 Tasks

The training of the IT staff depends on the tasks that they perform. The tasks have been listed down for every single role area. These tasks include the tasks that are actively performed for that particular role and the tasks that can be needed to be performed at any mature stage in the organization. The final training modules are customized according to these tasks.

6.4.2 Functional perspectives

Not every role in every institute has exactly the same nature or responsibility of job. Different individuals occupying the same may role have different mode and scope. Functional perspectives help in identifying and scoping the requirements for all these roles and help improve the training outcome. The knowledge units are customized for following functional perspectives.

- **Manage:** This includes functions which includes tasks that oversee the technical aspect of a security program at a high level, and ensure currency with changing risk and threat environments; including the management of person, program or operations;
- **Design:** This includes functions encompassing the development of processes/procedures, and the architectures that guide to executing the work at the program or system level; and development of systems, networks or applications.
- **Implement:** These are the functional areas that involve putting policies, procedures or processes in action in the enterprise; along with the maintenance and operation and of networks, applications or systems.
- **Evaluate:** These are the functional areas that involve the assessment of program, policy or process effectiveness and that of a security service in meeting its goals; also the evaluation of network or system or an application security state.

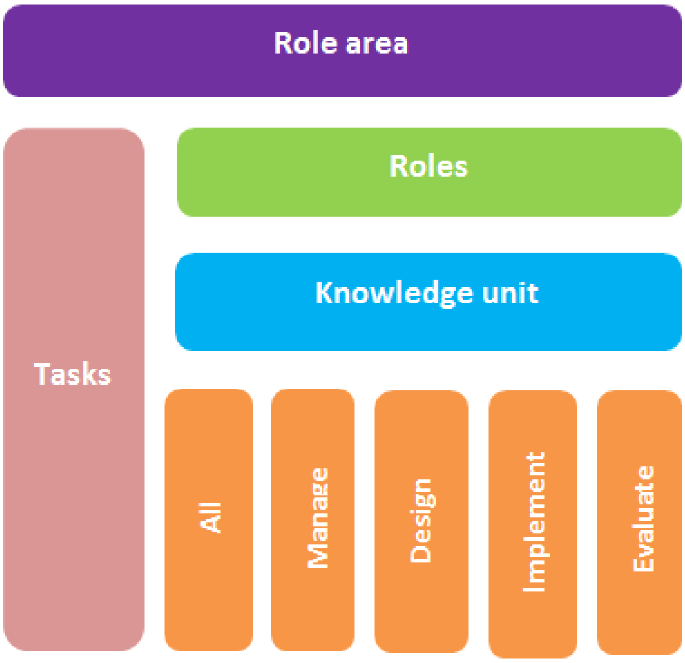


Fig. 6.3 Training module body

6.5 IT Staff Survey Results

The survey conducted for IT staff focuses on the five components as discussed earlier, namely; the *roles* they perform, the *experience* they have in that particular role, their *minimum qualification*, the *tasks* related to their roles and the *skill set* that they currently possess.

The results of the survey have been shared in section 6.6 with each role area separately followed by the training modules customized for that particular role area.

6.6 IT Staff Role-based Training Program

This section is the main component of this thesis, focusing on the survey conducted for the IT staff to gather information regarding their IT roles and security awareness and training requirements. The training program has been divided into the functional areas that are further broken down into role areas. Each role area has its own training module which has been designed on the basis of the requirement artifacts collected from the survey. Each training module has been broken down into following:

(Note: Following settings apply to all Role areas)

1. **Survey results:** This section includes the results gathered from the survey and compiled in tables. The results shared are the aggregate responses from all the institutes. It includes following details from the survey:

- Job details (Role name, minimum qualification and years of experience)
- Job tasks
- Skill set

2. **Training module:** This section presents the training modules for the role area under discussion. The training modules are built up of the knowledge units as discussed later for each of the functional perspectives individually. The knowledge units in the training modules have been customized according to the role needs and tasks selected by the users in the survey.

6.6.1 Knowledge Units

This section lists down all the knowledge units which the training modules are built up of. The knowledge units have been compiled from NIST training model 800-16. The list includes the knowledge units from a vast range of Information Technology domains. The *skill set ID* will be used to refer to a specific skill set or knowledge unit in the training modules. The complete set of modules with corresponding skill set IDs is attached in Appendix-D.

- Overall
- Architecture
- Computer Network Defense
- Cryptography and Encryption
- Database
- Emerging Technologies
- Identity Management/Privacy
- Web sec
- IT system and operations
- Modeling and Simulation
- Personnel Security
- Software
- Advanced Network Technology and Protocols
- Data Security

- Configuration Management
- Emerging Technologies
- Incident Management
- Information Systems
- IT Security Awareness And Training
- Security Risk Management
- Systems And Application Security

6.6.2 Functional Area: Securely Provision

This functional area covers following role areas:

- Software Assurance and Security Engineering
- Systems development

6.6.2.1 Role Area: Security Engineering and Software Assurance

Description: Developing plus writing/coding new (or modifying current) computer software, applications, or programs by following the best practices of software assurance.

Survey results (*Applies to all Role areas*):

The survey results reveal the following for the role area under discussion:

- **Job details**: All institutes have BS as their minimum qualification. The minimum experience of IT employees is 1 year and maximum years of experience were found to be 5 years.
- **Job tasks:** The table 'Job tasks' list down all the tasks associated with the role according to NICE framework. The status 'Yes' or 'No' shows whether the employee has that particular task for that role (yes) or not (no).
- **Skill set:** The tables named 'Skill set' list down all the competencies possessed by the employee under a particular job role.

Table 6.1 Job details - Software Assurance and Security Engineering

Roles/Job titles	Minimum Qualification	Years of experience
Computer Programmer	BS	Min 1 Max 5
Research & Development Engineer	BS	Min 1 Max 5
Software Developer	BS	Min 1 Max 5
Web Application Developer	BS	Min 1 Max 5

Table 6.2 Job tasks - Software Assurance and Security Engineering

Sr. No.	Tasks	Status	
		Yes	No
1	Analyze the related information to find, provide recommendation and modify an existing application or plan development of a new application.	✓	□
2	Assess the needs of the user and the software requirements to identify if the design is suitable for the cost and time constraints.	✓	□
3	Apply the testing and coding policies and standards, apply the security testing techniques and tools.	✓	□
4	Application of the ‘secure code documentation’.	✓	□
5	List the controls that were used in requirements gathering phase to combine security with the processes, figure out the main objectives, and above all to enhance software/app security while reducing hindrance in schedules and plans.	□	✓
6	Finalize the program development documentation and the following revised versions.	□	✓
7	Perform the trial runs of applications and programs to ensure they return the required information and ensure the correct instructions given.	✓	□
8	Coordinate with relevant individuals i.e. programmer, engineers etc. for the applications development and to get the required information on project capabilities and limitations, interfaces and performance measurements.	□	✓
9	Make the security threat model aligned with users’ input by conducting the interviews.	□	✓

10	Confer the engineering and IT personnel to assess interfacing between software and hardware.	✓	□
11	Error correction by incorporating the required changes and then re-evaluating the program to get the desired results.	✓	□
12	Design, create and amend the software systems, by using mathematical models for the measurement of the design outcome.	□	✓
13	Create the system testing and the validation procedures, coding and documentation and direct them.	✓	□
14	Development of the secure code and address the related (error) messages.	✓	□
15	Assess the concerned factors like cost, load and time constraints, reporting formats required and requirement of the security restrictions to determine the software and hardware configuration.	✓	□
16	Figure out the basic common programming flaws.	✓	□
17	Figure out the expected consequences and consequently apply suitable mechanisms within decentralized and centralized environments in the organization’s IT machines.	□	✓
19	Amend the current software to remove the errors, in order to align it with new hardware, and enhance the performance.	✓	□
20	Perform QA for security functionality and resilience to attacks.	□	✓
21	Conduct secure programming and look for flaws if any in the code to reduce security weaknesses.	✓	□
22	Perform risk analysis (e.g. vulnerability, threat and likelihood) when a system or an software app undergoes any change.	✓	□
23	Create the flow charts describing input, process, output, relevant the logical operations, then turn those into the instructions which are coded in a suitable machine language.	✓	□
25	Convert the security requirements into elements of application design that includes documentation of cyber attack vectors elements, and determination of any security criteria that may be needed.	✓	□
26	Conduct software penetration testing if needed for updated or new applications.	□	✓
27	Apply the defensive security measures (e.g., encryption, identity management an access control) to reduce chances of successful vulnerability exploitations.	✓	□
28	Propose controls and countermeasures for potential exploitations of security weaknesses of programming language in the systems or apps.	✓	□
29	Find the suitable software patches for the bugs which could render the software vulnerable.	✓	□

Table 6.3 Skill set - Software Assurance and Security Engineering

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Embedded Computers	□	□	✓
2	Object Technology	□	✓	□
3	Information Assurance	□	□	✓
4	Systems Testing and Evaluation	✓	□	□
5	Computer Languages	✓	□	□
6	Infrastructure Design	✓	□	□
7	Operating Systems	✓	□	□
8	Vulnerabilities Assessment	□	□	✓
9	Personnel Safety and Security	□	✓	□
10	Computer Languages	✓	□	□
11	Configuration Management	□	□	✓
12	Software Development	✓	□	□
13	Software Engineering	✓	□	□
14	Logical Systems Design	✓	□	□
15	Web Technology	✓	□	□
16	Modeling and Simulation	□	□	✓
17	Software Testing and Evaluation	✓	□	□
18	Identity Management	□	□	✓
19	Information Systems/Network Security	✓	□	□
20	Quality Assurance	□	□	✓
21	Incident Management	□	□	✓
22	Risk Management	□	□	✓

Table 6.4 Training modules: Software Assurance and Security Engineering

Knowledge unit	All	Manage	Design	Implement	Evaluate
Security Risk Management	N/A	N/A	SRM-7, SRM-19, SRM-22, SRM-23, SRM-29	SRM-32	N/A
Data Security	N/A	N/A	DS-2, 4, 7, 13, 18	N/A	N/A
Information Systems	N/A	N/A	IS-5, IS- 6, IS-7, IS-9, IS-10, IS-11, IS-12, IS-14, IS-17, IS-19, IS-21, IS-25,	N/A	N/A
Systems and Applications Security	N/A	SAS-1, SAS- 10, SAS-12	SAS-1, 3, 5, 10, 12 SAS- 17, SAS-22, SAS-28, SAS- 30, SAS-34	N/A	N/A
Architecture	N/A	N/A	ARC-1, ARC-4, ARC-13, ARC-9, ARC-15, ARC-18	ARC-1	N/A
Personnel Security	N/A	N/A	PS-9, PS-10	N/A	N/A
Identity Management/ Privacy	N/A	N/A	IMP-2, IMP- 3, IMP-4, IMP- 6, IMP-8, IMP- 10,	N/A	N/A
Configuration Management	N/A	N/A	CM-3,CM-5, CM-6,CM- 7, CM-9, 10, 12, CM-9-15	N/A	N/A

Modeling and Simulation	N/A	N/A	MS-1, MS-2	N/A	N/A
Web Security	N/A	N/A	WS-1, WS-2, WS-4, WS-8, WS-10	N/A	N/A
Network and Telecommunications Security	N/A	N/A	NTS-1-6	N/A	N/A

6.6.2.2 Role Area: Systems Development

Description: Working on the systems development lifecycle's development phases.

Table 6.5 Job details - Systems Development

Roles/Job titles	Minimum qualification	Years of experience
Firewall Engineer	BS	Min 1 Max 5
Systems Engineer	BS	Min 1 Max 5
Security Engineer	BS	Min 1 Max 5
Information Assurance (IA) Developer	BS	Min 1 Max 5

Table 6.6 Job Tasks - Systems Development

Sr. No.	Tasks	Status	
		Yes	No
1	Assess the system design constraints, detailed system, trade-offs, and security design	✓	□
2	Apply the IT policies to software applications which are linked with each another.	□	✓
3	Analyze the effectiveness of protection measures used by IT systems.	✓	□
4	Analyze the vulnerabilities of and threats to IT systems for creation of a reliable risk profile.	✓	□

5	Create, check, and renew the prototypes by using practical models.	✓	□
6	Perform the Privacy Impact Assessments of the applications' designing the right controls, which protect the integrity, privacy and confidentiality of data.	□	✓
7	Propose and create information assurance (IA) or IA-related products.	□	✓
8	Create the secure interface requirements/specifications between the resources that are interconnected.	✓	□
9	Design, create, develop, combine, and update the IT /system security controls (along with policies, procedures and requirements) which ensure integrity and confidentiality,	✓	□
10	Design hardware, OS, and software applications to sufficiently fulfill IA security needs.	✓	□
11	Designing the suitable data backup techniques and make sure that the suitable technical, managerial and procedural procedures are present for secure backups.	✓	□
12	Identify the security requirements to make sure that they are met for all applications.	✓	□
13	Create and orient the direct system testing procedure and processes.	✓	□
14	Design and check architecture of system components that are compatible with the technical specifications.	✓	□
15	Prepare the security documentation in detail for components and interface requirements.	✓	□
16	Develop DR (disaster recovery) and operations continuity plans, and make sure that the testing is done prior to systems entering the production environment.	□	✓
17	Develop the risk management measures to counter threats and vulnerabilities and propose suitable changes in terms of security.	✓	□
18	Develop required IA countermeasures and risk mitigation measures for applications and systems.	□	✓
19	Figure out elements/components, assign the security functions to those components, and determine the relationships among them.	✓	□
20	Find out and orient the remedies of technical problems emerged in implementation of new IT assets.	✓	□
21	Find and prioritize necessary system function, required to assist necessary enterprise functions; in case of resource failure, analyze the system requirements for availability and successful continuity.	✓	□
22	Determine, analyze, and recommend suitable IA products for the system use and make sure that the proposed products comply with organization's requirements.	□	✓

23	Implement the security designs for existing or new systems.	✓	□
24	Incorporate IA vulnerability solutions into the system designs.	□	✓
25	Conduct IS risk analysis and propose security safeguards to reduce the expected risk.	✓	□
27	Conduct the security review, determine the grey areas that need to be addressed in security architecture.	✓	□
27	Conduct risk assessment after a system or application goes through a change.	✓	□
29	Give input to the implementation plans and SOP.	✓	□
30	Provide required input to RMF procedures, processes and relevant documents.	□	✓
31	Retrieve, store and manipulate the data for analysis and needs of capabilities of system.	✓	□
32	Give necessary support to certification evaluation processes and procedures.	✓	□
33	Trace back all the security needs and specifications to design and create required components.	✓	□
35	Verify interoperability, scalability, stability and portability of system architecture	✓	□
37	Assess the user requirements and needs to plan and perform system security development.	✓	□
39	Make sure that the design and development processes are documented regularly, giving the description of the security implementation, and necessary updating.	□	✓

Table 6.7 Skill set - Systems Development

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Vulnerabilities Assessment	✓	□	□
2	Identity Management	□	□	✓
3	Mathematical Reasoning	✓	□	□
4	Cryptography	□	□	✓
5	Database Management Systems	✓	□	□
6	Information Assurance	□	✓	□
7	Systems Testing and Evaluation	✓	□	□

8	Hardware Engineering	✓	□	□
9	Embedded Computers	□	□	✓
10	Systems Integration	□	□	✓
11	Human Factors	□	✓	□
12	Information Systems/Network Security	✓	□	□
13	Infrastructure Design	✓	□	□
14	Computers and Electronics	✓	□	□
15	Operating Systems	✓	□	□
16	Information Technology Architecture	✓	□	□
17	Personnel Safety and Security	□	□	✓
18	Logical Systems Design	✓	□	□
19	Configuration Management	□	□	✓
20	Software Engineering	✓	□	□
21	Requirements Analysis	□	□	✓
22	Systems Life Cycle	✓	□	□
23	Telecommunications	□	□	✓
24	Information Systems Security Certification	□	✓	□
25	Modeling and Simulation	□	□	✓
26	Computer Languages	✓	□	□
27	Information Technology Performance Assessment	□	✓	□
28	Security	✓	□	□
29	Risk Management	✓	□	□
30	Network Management	✓	□	□

Table 6.8 Training modules - Systems Development

Knowledge unit	All	Manage	Design	Implement	Evaluate
Software	N/A	SW-15, SW-16	SW-1, SW-2, SW-3, SW-4, SW-5, SW-6, SW-8, SW-9, SW-10,	N/A	N/A

			SW-11, SW-15, SW-16, SW-24, SW-25, SW-26, SW-28, SW-30, SW-31, SW-32,		
Configuration management	N/A	CM-8, CM-13, CM-10	CM-5,CM-7, CM-9, CM-10, CM-11	N/A	N/A
Identity management/Privacy	N/A	IMP-1, IMP-11	IMP-1, IMP-2, IMP-4, IMP-6,	N/A	N/A
IT systems and operations	N/A	N/A	ITSO-7	N/A	N/A
Information Assurance	N/A	IA-1	IA-3, IA-4, IA-5, IA-7, IA-9,	N/A	N/A
Cryptography and encryption	N/A	N/A	CE-1, CE-3, CE-5, CE-7, CE-9, CE-12, CE-13	N/A	N/A
Information Systems	N/A	N/A	IS-2, IS-7, IS-9, IS-11, IS-13, IS-25,	N/A	N/A
Database	N/A	DB-9	DB-3, DB-7, DB-11	N/A	N/A
Network and Telecommunications security	N/A	NTS-7	NTS-7 -11, NTS: 13-19	N/A	N/A
Architecture	N/A	ARC-3	ARC-5, ARC-8, ARC-11, ARC-14, ARC-17, ARC-20	N/A	N/A
Systems and applications security	N/A	N/A	SAS-4, SAS-6, SAS-12, SAS-25, SAS-27,	N/A	N/A
Personnel security	N/A	PS-1, PS-7, PS-10	PS-1, PS-7, PS-10	N/A	N/A

Security risk management	N/A	SRM-12, SRM-18, SRM-24, SRM-30	SRM-7, SRM-13, SRM-16, SRM-19, SRM-22	N/A	N/A
Procurement	N/A	PRC-1,PRC-3, PRC-5, PRC-7, PRC-9	N/A	N/A	N/A
Modeling and simulation	N/A	N/A	MS-2	N/A	N/A

6.6.3 Functional Area: Operate and Maintain

This functional area includes the following role areas:

- Data administration
- Network services
- System administration

6.6.3.1 Role Area: Data administration

Description: Developing and administering data management systems and databases that allow for the query, storage and utilization of data.

Table 6.9 Job details - Data administration

Roles/Job titles	Minimum qualification	Years of experience
Database Administrator	BS	Min 1 Max 5
Data Manager	BS	Min 1 Max 5
Database Developer	BS	Min 1 Max 5
Information Dissemination Manager	BS	Min 1 Max 5

Table 6.10 Job Tasks - Data administration

Sr. No.	Tasks	Status	
		Yes	No
1	Define and analyze the data specifications and requirements.	✓	□
2	Plan and assess the incorporated amendments in the data needs.	✓	□
3	Plan and execute the database systems.	✓	□
4	Plan and execute data warehousing and the mining programs.	✓	□
5	Propose suitable standards of data, policies, processes and procedures	□	✓
6	Install and configure the software for database management systems	✓	□
7	Maintain the software for DMS.	✓	□
8	Ensure maintenance of exchange of information through alert, subscription, and the functions which enable the users exchange sensitive data as needed.	□	✓
9	Organize the caching, distribution, and the data retrieval and cataloging.	✓	□
10	Monitor the database and update it to ensure the required performance.	✓	□
11	Conduct the database backup to prevent data malfunctioning.	✓	□
12	Provision of an organized flow of relevant information aligned with the mission and vision requirements.	✓	□
13	Propose suggestions on the new architectures and technologies.	□	✓

Table 6.11 Skill set - Data administration

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Data Management	✓	□	□
2	Computer Forensics	□	✓	□
3	Database Management Systems	✓	□	□
4	Encryption	□	□	✓
5	Enterprise Architecture	□	□	✓
6	Identity Management	□	□	✓
7	Operating Systems	✓	□	□
8	Database Administration	✓	□	□

9	Modeling and Simulation	□	□	✓
10	Security	✓	□	□

Table 6.12 Training modules - Data administration

Knowledge unit	All	Manage	Design	Implement	Evaluate
Database	N/A	DB-9	DB-1, DB-3, DB-7, DB-11	DB-2, DB-4, DB-5, DB-6, DB-10	N/A
Data security	DS-5, DS-8, DS-18,	DS-9	DS-7, DS-9, DS-11, DS-12, DS-16, DS-17	DS-4, DS-6, DS-7, DS-8, DS-9, DS-11, DS-12, DS-17,	DS-1, DS-6, DS-8, DS-10, DS-15, DS-17,
Information systems	IS-1, IS-3, IS-5, IS-9, IS-24, IS-28, IS-31	IS-20	IS-7, IS-9, IS-17, IS-20, IS-25, IS-26	IS-9, IS-10, IS-13, IS-17, IS-20, IS-28, IS-30	IS-4, IS-22, IS-30
Cryptography and encryption	N/A	CE-4, CE-8	CE-1, CE-7, CE-9, CE-11,	CE-2, CE-5, CE-12, CE-13, CE-15	CE-2
Modeling and simulation	N/A	N/A	MS-1, MS-2	N/A	N/A
Architecture	N/A	ARC-3	ARC-4, ARC-12, ARC-18, ARC-19	ARC-1, ARC-5, ARC-7, ARC-10	N/A
Incident management	IM-20	IM-3, IM-5, IM-8, IM-11, IM-12, IM-16		IM-4, IM-7	IM-3,IM- 5, IM-8
Identity management/ Privacy	IMP-1,IMP- 2, IMP-6	IMP-7, IMP-11	IMP-10	IMP-3, IMP-8, IMP-11	IMP-3, IMP-8, IMP-10

6.6.3.2 Role Area: Network Services

Description: Installing, configuring, testing, operating, maintaining, and managing enterprise networks, their firewalls, including network devices (e.g., switches, bridges, hubs, IPS, IDS, proxy servers, routers) and the software that enable exchange of information in order to support privacy and integrity of information and all the IT resources.

Table 6.13 Job details - Network Services

Roles/Job titles	**Qualification**	**Years of experience**
Network Administrator	BS	Min 1 Max 5
Network Designer	BS	Min 1 Max 5
Network Engineer/analyst	BS	Min 1 Max 5
Systems Engineer	BS	Min 1 Max 5
Telecommunications Engineer/Personnel/ Specialist	BS	Min 1 Max 5

Table 6.14 Job Tasks - Network Services

Sr. No.	**Tasks**	**Status**	
		Yes	**No**
1	Configure the network and security devices switches (e.g., tunneling, NATing, IP whitelisting etc.)	✓	□
2	Plan, develop and execute the enterprise network and system backup policies and mechanisms.	□	✓
3	Troubleshoot and fix the connectivity related problems	✓	□
4	Modify the overall network architecture to meet new aims or enhance the network process flow	✓	□
5	Execute new test actions, system design methods and QA mechanisms.	✓	□
6	Installation and maintenance of the network architecture device Operating system software.	✓	□
7	Install or restore network devices.	✓	□
8	Integrate or merge the new systems into the current functional infrastructure.	✓	□
9	Monitor systems and network efficiency.	✓	□
10	Fix identified bugs to ensure information is protected from all illegitimate entities	✓	□
11	Provide the required feedback/input on IT network needs, including infrastructure/architecture.	✓	□

12	Fix the network connectivity problems	✓	□
13	Maintain and test the network infrastructure including hardware and software devices.	✓	□

Table 6.15 Skill set - Network Services

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Infrastructure Design	✓	□	□
2	Hardware	✓	□	□
3	Information Assurance	□	✓	□
4	Information Systems/Network Security	✓	□	□
5	Information Technology Performance Assessment	□	✓	□
6	Information Technology Architecture	□	□	✓
7	Systems Life Cycle	□	□	✓
8	Telecommunications	✓	□	□
9	Encryption	✓	□	□
10	Capacity Management	□	✓	□
11	Network Management	✓	□	□
12	Operating Systems	✓	□	□
13	Configuration Management	□	□	✓
14	Computer Network Defense	□	□	✓
15	Web Technology	✓	□	□
16	Security	✓	□	□

Table 6.16 Training modules - Network Services

Knowledge unit	All	Manage	Design	Implement	Evaluate
Information systems	IS-2, IS-3, IS-5, IS-6, IS-9, IS-11	IS-12, IS-13, IS-22, IS-24, IS-28	IS-2, IS-4, IS-6, IS-7, IS-8, IS-11, IS-12, IS-17, IS-28	IS-3, IS- 4, IS-5, IS-6, IS-7 S-8,IS-9,IS-11,IS-21,IS-16, IS-18, IS-29,IS-30	IS-3, IS-5, IS-6, IS-9, IS-12, IS-22, IS-27, IS-29, IS-31

Architecture	ARC-3, ARC-8, ARC-12, ARC-14, ARC-15	ARC-2, ARC-13	ARC-1, ARC-5, ARC-7, ARC-13, ARC-17, ARC-18, ARC-20	ARC-1, ARC-5, ARC-6, ARC-9, ARC-17, ARC-18, ARC-21	ARC-1, ARC-2, ARC-5, ARC-7, ARC-9, ARC-18, ARC-20, ARC-21
Cryptography and encryption	CE-1, CE-4, CE-5	CE-5, CE-8, CE-12	CE-3, CE-7, CE-8, CE-9	CE-4, CE-6, CE-7, CE-8, CE-11	N/A
IT systems and operations	ITSO-4, ITSO-7, ITSO-13, ITSO-18, ITSO-19, ITSO-22	ITSO-12, ITSO-14, ITSO-26	ITSO-1, ITSO-2, ITSO-3, ITSO-8, ITSO-10, ITSO-19	ITSO-1, ITSO-5, ITSO-6, ITSO-9, ITSO-11, ITSO-16, ITSO-21, ITSO-27	ITSO-2, ITSO-5, ITSO-10, ITSO-11, ITSO-12, ITSO-15
Network and Telecommunications Security	NTS-2, NTS-3, NTS-6, NTS-8, NTS-13, NTS-17, NTS-20, NTS-21, NTS-22, NTS-23	NTS-9, NTS-24, NTS-25, NTS-26, NTS-27, NTS-28, NTS-29, NTS-30	NTS-10, NTS-18, NTS-30, NTS-31, NTS-32	NTS-5, NTS-31, NTS-33, NTS-34	NTS-5, NTS-9, NTS-10, NTS-24, NTS-34, NTS-35,
Security Risk management	SRM-16	SRM-9, SRM-12, SRM-18, SRM-24, SRM-27	SRM-18, SRM-20, SRM-22	SRM-1, SRM-2, SRM-4, SRM-8, SRM-14, SRM-20, SRM-26, SRM-28, SRM-32, SRM-33, SRM-34	SRM-1, SRM-2, SRM-4, SRM-9, SRM-14, SRM-18, SRM-19, SRM-20, SRM-25, SRM-28
Configuration management	CM-1, 2, 6, 9, 11	CM-6, 8, 14	CM-10	CM-2, 3, 5, 8, 12, 15	CM-7
Web Security	WS-2	N/A	N/A	WS-7	N/A
Data security	N/A	DS-3,8	5	DS-3, 5, 10, 15	N/A
Computer network defense	CND-1, CND- 3, CND-4,	CND-2, 7, 5, 17, 21, 25, 28, 29	CND-21	CND-2, 7, 13, 25,	CND-9, CND-12, CND-17,

	CND-10, 14, 19			CND-26, CND-30	CND-23, CND-26
Incident management	IM-1, IM-5, IM-11, IM-12, IM-16, IM-20	N/A	N/A	IM-17, IM-19	IM-4, IM-6, IM-8, IM-10
Identity management/ Privacy	IMP-1, IMP-2, IMP-4, IMP-6	N/A	N/A	IMP-6, IMP-8, IMP-10	N/A

6.6.3.3 Role Area: System Administration

Description: Installing, configuring, troubleshooting and maintaining configurations of the server in order to ensure their privacy, availability and integrity. This area is also about managing the accounts, firewalls, and the patches. Moreover, includes responsibility for passwords, access control, account creation and administration.

Table 6.17 Job details - System Administration

Roles/Job titles	Minimum qualification	Years of experience
Local Area Network (LAN) Administrator	BS	Min 1 Max 5
Security Administrator	BS	Min 1 Max 5
Server Administrator	BS	Min 1 Max 5
Systems Administrator	BS	Min 1 Max 5
Website Administrator	BS	Min 1 Max 5

Table 6.18 Job Tasks - System Administration

Sr. No.	Tasks	Status	
		Yes	No
1	Check the server availability, integrity, functionality and efficiency	✓	□
2	Perform the connectivity and functional testing to make sure that operability is continuing.	✓	□

3	Perform periodic maintenance of the server including cleaning (both electronically and physically), routine reboots, disk checks, testing and data dumps.	✓	□
4	Develop access control lists (ACLs) and group policies to ensure compatibility with needs, standards and business rules of the organization.	✓	□
5	Develop and document the system administration SOPs.	✓	□
6	Develop and implement procedures and policies for usage of local network.	✓	□
7	Install server updates, enhancements and fixes.	✓	□
8	Maintain and update the baseline system security in accordance with the company policies	✓	□
9	Manage the user accounts and access or privileges to equipment or IT assets.	✓	□
10	Manage the server resources including availability, performance, recoverability capacity and serviceability.	✓	□
11	Monitor, update and maintain the configuration (of server)	✓	□
12	Oversee configuration, installation and implementation of the network devices	✓	□
13	Conduct repairs of faulty resources	✓	□
14	Coordinate and plan the installation of the modified or new OS, hardware.	✓	□
15	Plan and implement the system recovery, data redundancy mechanisms and required actions.	✓	□
16	Provision of support for problem-solving plus optimization.	✓	□
17	Address software/hardware interface and interoperability issues.	✓	□

Table 6.19 Skill set - System Administration

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Information Systems/Network Security	✓	□	□
2	Infrastructure Design	□	□	✓
3	Information Technology Performance Assessment	□	✓	□
4	Technology Awareness	□	□	✓
5	Systems Integration	✓	□	□
6	Systems Life Cycle	□	□	✓
7	Operating Systems	✓	□	□
8	Computer Forensics	□	✓	□
9	Information Technology Architecture	✓	□	□

10	Encryption	□	□	✓
11	Network Management	□	□	✓
12	Software Engineering	✓	□	□
13	Identity Management	□	□	✓
14	Computer Languages	✓	□	□
15	Configuration Management	□	□	✓
16	Security	✓	□	□
17	Telecommunications	✓	□	□

Table 6.20 Training modules - System Administration

Knowledge unit	All	Manage	Design	Implement	Evaluate
Architecture	ARC-7, ARC-10, ARC-12	ARC-2, 3, 5, 17	ARC-1, 10, 13, 16, 18	ARC-1, 4, 10, 16	ARC-18
Information Systems	IS-5, IS- 9, IS-11, IS-15, IS-19, IS-22, IS-26, IS-31	IS-10, IS-19, IS-20	IS-1, IS-2, IS-3, IS-6, IS- 7, IS-17, IS-19	IS-1, IS-2, IS-5, IS-6, IS-7, IS-9, IS-13, IS-27, IS-31	IS-1, IS-21, IS-23, IS-19, IS-25
Systems and Application security	SAS-1, 3, 4, SAS- 22-30	SAS -16, SAS -25	SAS -6, 10, 12	SAS -13, 14, 15, 20, 25, 28	SAS -14, 15, 17, 26, 29, 33
Network Telecommunication Security	NTS-2, 9, 11, 31, 36	NTS-8, NTS-28	N/A	NTS-1, 28, 29, 37, 38, 39	NTS-1, 33, 38
Cryptography and encryption	CE-1, CE-4, CE-8, CE-9	N/A	CE-3	CE-6, CE-10	N/A
Security Risk management	SRM-7, SRM-13, SRM-23, SRM-24, SRM-29	SRM-4, SRM-9, SRM-18, SRM-27	SRM-22, SRM-28	SRM-1, SRM-3, SRM-6, SRM-20, SRM-22, SRM-26	SRM-1, SRM-3, SRM-19, SRM-32,
Software	SW-2, SW-17, SW-26, SW-27, SW-20,	SW-18	SW-10, SW-13, SW-15, SW-22, SW-25, SW-30,	SW-8, SW-10, SW-18, SW-20, SW-25, SW-32	SW-8, SW-13, SW-18, SW-24
Emerging Technologies	ET-1, ET-3, ET-4	ET-2	N/A	ET-5	N/A

Configuration management	CM-1, CM-3, CM-9, CM-11	CM-2, CM-3, CM-4, CM-8, CM-12, CM-14	N/A	CM-2, CM-5, CM-8, CM-15	CM-2
Identity management/ Privacy	IMP-1, IMP-2, IMP-6, IMP-11	N/A	IMP-10	IMP-3, IMP-8	IMP-5, IMP-7
Incident management	IM-1, IM-2, IM-5, IM-11	N/A	N/A	IM-2, IM-7, IM-9, IM-17	IM-13, IM-17

6.6.4 Functional area: Protect and defend

This functional area includes following areas:

- CND Analysis
- Incident Handling
- Vulnerability assessment/management

6.6.4.1 Role Area: CND Analysis (Computer Network defense)

Description: By using the defensive security countermeasures and the information collected from a wide range of sources for identifying, assessing and reporting the events that occur or have probability to occur to prevent the privacy compromise of the information or systems.

Table 6.21 Job details - Computer Network defense (CND) Analysis

Roles/Job titles	Minimum qualification	Years of experience
CND Analyst	BS	Min 1 Max 5
Cybersecurity Intelligence Analyst	BS	Min 1 Max 5
Network Defense Technician	BS	Min 1 Max 5
Network Security Engineer	BS	Min 1 Max 5

Security Operator	BS	Min 1 Max 5

Table 6.22 Tasks - Computer Network defense (CND) Analysis

Sr. No.	Tasks	Status	
		Yes	No
1	Create the required content for CND analysis techniques and tools.	✓	□
2	Analyze and characterize the network traffic to detect malicious and abnormal activity and the threats to IT systems and services.	✓	□
3	Monitor the external data sources to maintain CND threat state currency and find out the security issues that are impactful for the organization.	✓	□
4	Escalate and document the incidents (including alerts' history and status and their severity) that can disrupt normal network processes and operations.	✓	□
5	Conduct CND analysis and documentation	✓	□
6	Conduct events' correlation using correlation rules and data from various sources in the organization to get environmental awareness and find the criticality of the detected threat.	✓	□
7	Provide periodic reports of network activity and the relevant events.	✓	□
8	Analyze and collect network based alerts from different sources in the organization and final possible attack vector and implications of these alarms/alerts.	✓	□
9	Provide timely detection of alerts and possible attacks/intrusions, misuse of the activities, suspicious activities, and segregate these events from the normal activities.	✓	□
10	Use these tools for continuous monitoring and system activity analysis to clearly categorize them into normal, suspicious and malicious activities.	✓	□
11	Assess the suspicious/malicious activity to find the exploited vulnerabilities, the attack vectors used, and impact on systems and sensitive data.	✓	□
12	Use the defense-in-depth practices and principles (e.g., layered defense and security resilience).	□	✓
13	Plan the response action for detected abnormal or malicious activities.	✓	□

14	Conduct information assurance controls' tests aligned with pre-defined test procedures and plans.	□	✓
15	Determine TTPs (tactics, techniques and procedures for given set of intrusions.	□	✓
16	Assess the network topologies to analyze data flows across the network	✓	□
18	Analyze and identify network anomalies in traffic by using metadata	✓	□
19	Perform analysis, research and correlation for diverse variety of the data sources (warnings and indications)	✓	□
20	Validate IDS engine alerts against the network based traffic using relevant network analysis tools.	✓	□
21	Identify operating systems and applications of a network system or device on the basis of network traffic.	✓	□
22	Triage malware	□	✓
23	Replay malicious network activity or an attack.	✓	□
24	Identify OS, conduct network mapping using network scanners.	✓	□

Table 6.23 Skill set - Computer Network defense (CND) Analysis

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Vulnerabilities Assessment	✓	□	□
2	Computer Network Defense	✓	□	□
3	Cryptography	□	□	✓
4	Computer Forensics	□	□	✓
5	Information Systems/Network Security	✓	□	□
6	Incident Management	□	□	✓
7	Information Assurance	□	✓	□
8	Infrastructure Design	□	□	✓
9	Technology Awareness	□	□	✓
10	Computer Languages	✓	□	□
11	Encryption	✓	□	□
12	Knowledge Management	□	✓	□
13	Telecommunications	□	□	✓
14	Operating Systems	✓	□	□

15	Configuration Management	□	□	✓
16	Data Management	✓	□	□
17	Criminal Law	□	✓	□

Table 6.24 Training modules - Computer Network defense (CND) Analysis

Knowledge unit	All	Manage	Design	Implement	Evaluate
Data Security	N/A	N/A	N/A	DS-1, DS-4	N/A
Architecture	N/A	ARC-3, ARC-6	N/A	ARC-3, ARC-5, ARC-6, ARC-19	N/A
Software	N/A		N/A	SW-7, SW-17, SW-20, SW-22	N/A
Security Risk Management	N/A	SRM-12, SRM-15, SRM-18, SRM-33	N/A	SRM-2, SRM-4, SRM-6, SRM-7, SRM-25, SRM-32	N/A
Network and Telecommunications Security	N/A	NTS-8, NTS-30	N/A	NTS-4,5, 7, 10, 11, 12, 13, 23, 24, 31, 33	N/A
Incident Management	N/A	IM-12, 14, 18, 20	N/A	IM-8, 11, 1, 14, 18, 20	N/A
Incident Management/Privacy	N/A	IMP-2, 4, 6	N/A	IMP-2-6, 8, 10	N/A
Cryptography and Encryption	N/A		N/A	CE-8	N/A
Computer Network Defense	N/A	CND-2,-6, 8-12, 14, 15,, 21, 22, 24, 27, 29, 30	N/A	CND-1 to CND-30	N/A
Configuration Management	N/A	N/A	N/A	CM-1, 3, 5, 7, 9, 11, 14	N/A
Information Systems	N/A	N/A	N/A	IS-22, IS-26, IS-29, IS-30	N/A

6.6.4.2 Role Area: Incident Response

Description: It refers to responding to the crisis or emergency situations in the particular domain for catering the potential threats and containing the damage. It also includes using the remediation, preparedness, just as per the need, plus investigating and analyzing all the related events and alarms.

Table 6.25 Job details - Incident Response

Roles/Job titles	Minimum qualification	Years of experience
Computer Crime Investigator	BS	Min 1 Max 5
Incident Handler and responder	BS	Min 1 Max 5
Incident Response Analyst and Coordinator	BS	Min 1 Max 5

Table 6.26 Job Tasks - Incident Response

Sr. No.	Tasks	Status	
		Yes	No
1	Coordinate and provide technical required support to the CND technicians in the organization to resolve CND related incidents.	✓	□
2	Correlate the gathered data for identifying vulnerabilities and propose the recommendations accordingly.	✓	□
3	Monitor the data sources (CERTs, Security Focus, SANS) to maintain the threat state currency and determine the security issues that may be impactful for the organization.	□	✓
4	Perform log file analysis from various sources for identification of possible threats to the security of network.	✓	□
5	Conduct C2 (command and control) procedures in order to respond to security incidents.	✓	□
6	Perform CND incident triage, for inclusion of determination of urgency, scope, and impact; identification of the weakness, security loopholes; proposing recommendations which can provide quick remediation.	✓	□

7	Conduct forensically sound image acquisition and propose suitable remediation for IT assets.	✓	□
8	Perform real-time CND incident handling (e.g., threat analysis, forensic examination, direct system remediation and intrusion correlation/tracking).	✓	□
9	Analyze and receive network based alerts from different sources in the organization, find the attack-vector for these alerts.	✓	□
10	Document and track the CND incidents starting from initial detection of alerts to final resolution of them.	✓	□
11	Write network defense guidance, documents and reporting on the threat findings for concerned personnel.	✓	□
12	Collect artifacts related to the caused intrusion (e.g., malware, signature, and Trojans) and use this data to provide remediation of the incidents in the organization.	✓	□

Table 6.27 Skill set - Incident Response

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Computer Forensics	□	✓	□
2	Infrastructure Design	□	□	✓
3	Incident Management	✓	□	□
4	Computer Network Defense	✓	□	□
5	Information Systems/Network Security	✓	□	□
6	Vulnerabilities Assessment	✓	□	□
7	Information Assurance	□	✓	□

Table 6.28 Training modules - Incident Response

Knowledge unit	All	Manage	Design	Implement	Evaluate
Computer Network Defense	CND-6, CND-10, CND-11, CND-19, CND-21	CND-15, CND-27, CND-28, CND-29	CND-3, CND-4,	CND-2, CND-3, CND-4, CND-7, CND-9,	CND-2, CND-3, CND-5, CND-8, CND-9,

				CND-13, CND-14, CND-23, CND-25, CND-26	CND-21, CND-25
Architecture	ARC-12	N/A	ARC-9, ARC-13	ARC-7, ARC-9, ARC-17, ARC-19	ARC-2, ARC-4, ARC-5, ARC-9, ARC-17
Security Risk management	SRM-13, SRM-16	SRM-9, SRM-12, SRM-24, SRM-27	SRM-22	SRM-4, SRM-8, SRM-10, SRM-14, SRM-19, SRM-28	SRM-2, SRM-3, SRM-5, SRM-6, SRM-8, SRM-11, SRM-14, SRM-16, SRM-18, SRM-21, SRM-32, SRM-33, SRM-34
Information Assurance	IA-3	IA-1, IA-2, IA-3	IA-3, IA-7, IA-9	IA-6, IA-8, IA-9	IA-1, IA-8
Information Systems	IS-9, IS-13	IS-14, IS-22, IS-31	IS-2, IS-6, IS-7,	IS-7, IS-18, IS-21, IS-22, IS-23,	IS-8, IS-16, IS-22, IS-23, IS-25, IS-29,
Network and Telecommunications Security	NTS-1, NTS-2, NTS-3, NTS-6, NTS-8, NTS-9, NTS-12, NTS-15, NTS-16, NTS-19, NTS-21, NTS-25, NTS-28, NTS-39	NTS-4, NTS-5, NTS-7, NTS-9, NTS-11, NTS-14, NTS-17, NTS-19, NTS-31, NTS-32, NTS-36, NTS-37	NTS-1, NTS- 4, NTS-5, NTS-7, NTS-8, NTS-9, NTS-10, NTS-11, NTS-12, NTS-15, NTS-17, NTS-18, NTS-19, NTS-21, NTS-22, NTS-24, NTS-25, NTS-27, NTS-28, NTS-29, NTS-31,	NTS-5, NTS-6, NTS-7, NTS-8, NTS-9, NTS-10, NTS-11, NTS-13, NTS-15, NTS-17, NTS-18, NTS-19, NTS-21, NTS-27, NTS-28, NTS-29, NTS-31, NTS-32, NTS-33, NTS-34, NTS-36,	NTS-2, NTS-6, NTS-9, NTS-38

			NTS-32, NTS-33, NTS-34, NTS-35, NTS-37, NTS-38, NTS-39	NTS-37, NTS-38	
Incident Management	IM-1, IM-3, IM-20	IM-2, IM-5, IM-10, IM-11, IM-16, IM-18	N/A	IM-4, IM-5, IM-7, IM-9, IM-13, IM-18	IM-5, IM-6, IM-9, IM-10

6.6.4.3 Role Area: Vulnerability Assessment and Management

Description: Conducting the assessments of vulnerabilities and threats, determining the acceptable deviations from the configurations organizations own policies and conducting risk assessment, followed by the development of suitable mitigation safeguards for all kinds of situations.

Table 6.29 Job details - Vulnerability Assessment and Management

Roles/Job titles	**Minimum qualification**	**Years of experience**
Blue Team Technician	BS	Min 1 Max 5
Ethical Hacker	BS	Min 1 Max 5
Penetration Tester	BS	Min 1 Max 5
Red Team Technician	BS	Min 1 Max 5
Reverse Engineer	BS	Min 1 Max 5
Risk/Vulnerability Analyst	BS	Min 1 Max 5
Vulnerability Manager	BS	Min 1 Max 5

Table 6.30 Job Tasks - Vulnerability Assessment and Management

Sr. No.	Tasks	Status	
		Yes	No
1	Assess organization's CND policies and procedures and verify whether they comply with organizational directives and regulation.	✓	□
2	Perform authorized penetration testing on organization’s critical IT assets.	✓	□
3	Prepare a deployable CND audit to provide support for auditing purposes.	✓	□
4	Maintain updated CND knowledge and related policies, procedures, regulations, that are applicable and that are specifically related to CND auditing.	✓	□
5	Prepare the audit reports identifying procedural and technical findings, and give recommended solutions or mitigation strategies.	□	✓
6	Conduct non-technical (operations and people) and technical (technology) evaluation of vulnerability and risk assessments of related IT focus areas	✓	□
7	Provide assistance with the selection of economic security safeguards to cater for risk (e.g., protection of processes, information and systems)	✓	□

Table 6.31 Skill set - Vulnerability Assessment and Management

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Vulnerabilities Assessment	✓	□	□
2	Computer Forensics	□	□	✓
3	Information Assurance	□	✓	□
4	Identity Management	□	□	✓
5	Infrastructure Design	□	□	✓
6	Computer Languages	✓	□	□
7	Computer Network Defense	□	□	✓
8	Systems Testing and Evaluation	✓	□	□
9	Information Systems/Network Security	✓	□	□
10	Human Factors	□	✓	□
11	Information Assurance	□	✓	□

12	Computer Languages	✓	□	□
13	Contracting/Procurement	□	✓	□
14	Criminal Law	□	✓	□

Table 6.32 Training modules - Vulnerability Assessment and Management

Knowledge unit	All	Manage	Design	Implement	Evaluate
Software	N/A	SW-12, SW-13, SW-15, SW-27	N/A	SW-19, SW-29, SW-25, SW-32	N/A
Personnel Security	N/A	PS-1, PS-4, PS-7, PS-9, PS-10	N/A	PS-12	N/A
Computer Network Defense	N/A	CND-2, CND-4, CND-10, CND-26, CND-28	N/A	CND-2, CND-3, CND-4, CND-7, CND-9, CND-10, CND-11, CND-13, CND-23, CND-25, CND-26, CND-28, CND-30	N/A
Identity Management/Privacy	N/A	IMP-2, IMP-4, IMP-6	N/A	IMP-1, IMP-2, IMP-3, IMP-4, IMP-6, IMP-8, IMP-10	N/A
Procurement	N/A	PRC-4, PRC-5	N/A		N/A
Architecture	N/A		N/A	ARC-2, ARC-5, ARC-8, ARC-9, ARC-11, ARC-12	N/A
Information Systems	N/A		N/A	IS-6, IS-22, IS-24, IS-26, IS-30, IS-31	N/A

Network and Telecommunications Security	N/A	NTS-28	N/A	NTS-2, NTS-3, NTS-5, NTS-6, NTS-18, NTS-19, NTS-22, NTS-26, NTS-28, NTS-29, NTS-31, NTS-33, NTS-39, NTS-40	N/A
Information Assurance	N/A	IA-1, IA-2, IA-3, IA-5, IA-7	N/A	IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-9	N/A
Security Risk Management	N/A	SRM-1 to SRM-34	N/A	SRM-1 to SRM-34	N/A
Systems and Applications Security	N/A	SAS-2, SAS-4, SAS-8, SAS-14, SAS-17, SAS-22, SAS-26, SAS- 28	N/A	SAS-2, SAS-4, SAS-8, SAS-14, SAS-17, SAS-22, SAS-26, SAS-28	N/A

6.6.5 Functional Area: Oversight and Development

Only one role area ‘Education and Training’ maps this functional area according to the needs of academia sector.

6.6.5.1 Role Area: Education and Training

Description: Conducting the training of personnel within the pertinent subject domain. Also includes developing, planning, coordinating, delivering, and/or evaluating the training methods, courses, and techniques as needed.

The survey for this particular role area has been left undone since no such roles were identified in the current academic community. However, this section has been included as a proposal to be incorporated in the training program since there is a need to introduce such roles for a better and more effective security learning process. The job tasks for these roles have been listed along with the training modules that map to these tasks.

Table 6.33 Job Tasks - Education and Training

Sr. No.	Tasks	Status	
		Yes	No
1	Conduct the interactive and healthy training drills for creation of an efficient and effective learning environment.	□	□
2	Correlate the vision and mission requirements with training	□	□
3	Deliver the training modules that match the need of the target audience and that are aligned with the physical environment	□	□
4	Demonstrate relevant techniques or concepts to the subordinates or colleagues or team members.	□	□
5	Design the required course content and training syllabi.	□	□
6	Determine the requirements of training.	□	□
7	Develop new training modules that address the need of the intended audience.	□	□
8	Develop goals and objectives for cyber security awareness, education and training.	□	□
9	Evaluate the comprehensiveness and effectiveness of existing training programs	□	□
10	Develop classroom formats and techniques plan (e.g., demonstrations, lectures, multimedia presentations).	□	□
11	Plan on some non-classroom training formats and techniques (e.g., web-based training, video courses)	□	□
12	Review and update the documented training modules (e.g., lesson plans, student texts, examinations and descriptions of the course).	□	□
13	Revise the course material on the basis of the feedback obtained from the preceding training sessions.	□	□
14	Serve as an advisor and internal consultant in one's own area of forte.	□	□
15	Support the design, development and execution of the relevant case studies.	□	□
16	Write relevant instructional material (e.g., Standard operating procedures) for guidance purposes.	□	□

Table 6.34 Skill set - Education and Training

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Computer Network Defense	□	□	□
2	Technology Awareness	□	□	□
3	Infrastructure Design	□	□	□
4	Operating Systems	□	□	□
5	Multimedia Technologies	□	□	□
6	Computers and Electronics	□	□	□
8	Technology Awareness	□	□	□
9	Teaching Others	□	□	□
10	Oral Communication	□	□	□
11	Organizational Awareness	□	□	□
12	Information Systems/Network Security	□	□	□

Table 6.35 Training modules - Education and Training

Knowledge unit	All	Manage	Design	Implement	Evaluate
Personnel	N/A	1, 2, 4, 9, 11, 12	N/A	N/A	N/A
IT Security Awareness and Training	1 to 12	N/A	N/A	N/A	N/A
Management	N/A	5, 6, 10	N/A	N/A	N/A

6.7 Conclusion

The concept of a Role-based training program originates from the fact that there is a diverse and vast variety of roles and responsibilities in the world of Information technology and the topic-based training i.e. the same training program or material for all these roles is pretty inefficient. The topic based training will cause over consumption of some individuals with the training material that is not required by their job and under consumption of other individuals depriving them of the material that is required to be learnt by them owing to their relevant job role. This chapter has presented security training program for all the IT roles currently functional in the academic community. The training modules have been customized for each role area based on the survey conducted. Most of the roles have been identified to be having minimum 1 and maximum 5 years of experience in the relevant domain. The training modules highlight the knowledge units for four functional perspectives namely; '*manage'*, '*design'*, '*implement'* and '*evaluate'* for the role areas. The complexity and depth of the training material provided can vary according to the competency and experience of the particular role and depends on the training material developers and instructors.

IT is a continuous process and so is security awareness and training. This training program is mature enough to be used by the academic community with the current state of maturity. However, with more changing IT trends, more evolving IT roles and new threats with changing technology, the training process will have to be reshaped and resized accordingly.

Chapter 7

CONCLUSION

7.1 Research Summary

The research aims on the development of a Role-based cyber security program for the academic community of Pakistan. Academic community has been chosen mainly due to two reasons; firstly, it is feasible to conduct surveys in the academic organizations due to less strict privacy concerns and secondly it is the youth that has to be trained for a prosperous and well-aware nation and safer future.

The surveys have been conducted for three categories; *senior management'*, '*general users' and* '*IT staff'*. The survey for senior management was basically conducted to highlight all the efforts done and measures taken by the organizations to ensure better security posture. Unfortunately, the overall security posture of the academic community has been found to be critically concerning.

The general users include mostly students and teachers from different educational backgrounds. The survey for general users has revealed the awareness level regarding cyber security to be very low. The users do not qualify to be called a cyber-safe nation. The training program for the users has been designed on the basis of the survey results and is based on SANS standard (*Securing the human*). The training program is flexible and comprehensive enough to cover the basic awareness needs of the users.

The survey for IT staff was conducted with the purpose of identifying their roles and responsibilities in their specific job and to measure their current level of competency. The training program for IT staff has been designed according to NIST standard (SP 800-16). The role-based training program is an effective and efficient approach for the training the cyber work to ensure that every individual having an IT related responsibility gets training and education concerned with his domain.

7.2 Outcome of the research

Currently no such awareness programs have been implemented in the academia sector of Pakistan. There has never been any awareness campaign. Hence, it will not be wrong to say that this research is the very first step into the beginning of the cyber security awareness efforts in Pakistan. As mentioned by the stats in Chapter 3 and 4, there is still a huge gap between the current security awareness level of the individuals and the minimum required awareness level to be called cyber safe or cyber aware. Identification of the problem is however the very first step. At the very least, this research has highlighted all the threats of unawareness that the individuals are faced with. The general or non-technical users are especially terribly lagging behind in the phase of getting cyber aware. There is only a small fraction of users that interact with technology with security conscious attitude. On a scale of 1 to 10, only 1/10 individuals are security conscious and are aware of the general threats that the technology brings to them. Highlighting these threats because of negligence and non-awareness indicates a dire need of awareness and training programs for these individuals for a better cyber aware and ready to respond nation.

7.3 Contribution

The research has designed training programs on the basis of the surveys conducted. The survey for senior management has presented overall security posture of the academia sector. The survey for general users has been conducted for the purpose of risk assessment due to non-awareness in various security domains taking into account the KAB theory (Knowledge, Attitude and Behavior). The final training program has been devised on the basis of survey results. The survey for IT staff has been conducted to identify the tasks associated with each role reflecting the awareness needs of that role. The final training program for the IT Staff is based on these survey results.

7.4 Limitations of the research

Surveys via questionnaires help a lot in doing the analysis in a particular area and in this case, assessing the need of the awareness and training programs in IT security domain. However, questionnaires are never cent percent reliable. There can never be a guarantee of a true and careful response from the individuals filling out the questionnaires. The assessments done in this research are based on the assumption that all the responses from the individuals who participated in the surveys are genuine and true to their maximum capacity. However, one cannot completely rely on the results that this survey has come up with. But still in most of the domains discussed, one can always see the consistency in the responses which shows an acceptable level of reliability to build a program based on these responses. The purpose of the research is basically to highlight the dire need to starting efforts in cyber security awareness across the country, however is still served.

7.5 Future Work

Security awareness is a continuous ongoing process. The proposed training program has been designed on the basis of the current awareness needs of the academic community. The training program if properly executed will ensure a far better awareness level of the individuals, both general users and IT individuals. This research has covered the awareness needs for the academic community. It is highly recommended to extend this effort to the corporate and government sector as well. A well-aware academic community will lead to a more cyber safe nation but it is the corporate and government sectors that are under more threat and risk when it comes to cyber warfare. Pakistan is a developing country and is growing in terms of Internet technology and solutions. Hence, it is necessary to protect the critical IT assets of the country that are possessed by the government and industry. The similar surveys can be conducted in both corporate and government sectors with some amendments according to the maturity of the IT infrastructure of the company under survey. A detailed role-based training program can be developed for each sector which should be flexible enough to be customized for any organization with any level of maturity.

7.6 Concluding remarks

As mentioned earlier, the foundation of information security is based on three major pillars; people, process and technology. When it comes to technology and processes and their vulnerabilities, there are fixes and patches but there is no patch to human stupidity or misjudgment. Organizations develop security policies and procedures to ensure a better security posture but these security policies and procedures alone are not enough. Failure to pay enough attention to IT security training poses huge risk to organizations because the security of IT resources is not merely a technology issue but also a human issue. A nation's future relies largely on its youth and so does the future of its cyberspace. The country youth with good IT knowledge and skills help in creating a healthy cyberspace and ultimately a powerful country. Lack of awareness and training is a vacuum in IT security world and this research aims to fill this vacuum. Since, this research is based on the survey conducted in a very limited domain hence the results cannot be relied upon in the long run but it is a good kick-start for an organized process of security awareness. The need to take an initiative in security awareness domain in the country is justified by this research. Security is a continuous process, so is the security awareness. The threats and attacks keep evading and changing with the technology advancements. Hence, the security awareness efforts also need to keep pace with the ever growing technology trends. But first step to accomplish is to begin and for that purpose, this research is the first step. As long as a proper, polished, organized and mature effort process in security domain is concerned, there is no limit. Precisely, the country needs to have a comprehensive, flexible and scalable awareness and training programs for the individuals who have interaction with technology on daily basis, to educate, recruit and train them to make proactive, defensive and data-driven decisions about their work.

Appendix A: Questionnaire for Management

Survey for Cybersecurity Training

Risk Analysis Questionnaire

Sector: Academia
Category: IT
Institute: ____________________

Every year, nearly 430 million adults worldwide fall victims to cyber-crime, at a price of approximately $400 billion on basis of time as well as monetary loss, costing the world more than even drugs and smuggling related crimes combined. Cyber-security involves protection of sensitive information by detecting, preventing, and responding to attacks. Our lives largely rely on information technology, which makes cyber security one of the country’s top national security preferences. While the Pakistan government is taking steps to ensure the safety of cyber community, the government cannot solve the issue alone. In fact it is a shared responsibility. You are encouraged to step ahead and make your contribution to this survey which will help enhance the security posture of the academic community of the country.
(Note: You can rest assured that the information you provide shall be kept confidential and will only be reported as aggregate)

Security Positions:

Mark the following security roles currently present in your institute and ones that are required. Leave the ones unfilled that are neither present nor required.

Position	Status		Position	Status	
	Present	Required		Present	Required
Database Administrator	□	□	Security Training Coordinator	□	□
Data Manager	□	□	IS Policy Analyst	□	□
Database Developer	□	□	Policy Strategist	□	□
Information Dissemination Manager	□	□	IS Project Manager	□	□
Network Administrator	□	□	CND Analyst	□	□
Network Engineer	□	□	Cybersecurity Intelligence Analyst	□	□
Network analyst	□	□	Network Defense Technician	□	□
Computer Engineer	□	□	Network Security Engineer	□	□

Telecommunications Engineer/Personnel/ Specialist	□	□	Security Operator	□	□
Local Area Network (LAN) Administrator	□	□	Crime Investigator	□	□
Security Administrator	□	□	Incident responder	□	□
Server Administrator	□	□	Incident Response Analyst	□	□
Systems Administrator	□	□	Blue Team Technician	□	□
Website Administrator	□	□	Ethical Hacker	□	□
Computer Programmer	□	□	Penetration Tester	□	□
Research & Development Engineer	□	□	Red Team Technician	□	□
Software Developer	□	□	Reverse Engineer	□	□
Web Application Developer	□	□	Risk/Vulnerability Analyst	□	□
Firewall Engineer	□	□	Vulnerability Manager	□	□
Systems Engineer	□	□	Computer Forensic Analyst	□	□
Security Engineer	□	□	Digital Forensic Examiner	□	□
Information Assurance (IA) Developer	□	□	Digital Media Collector	□	□
Cyber Trainer	□	□	Forensic Analyst	□	□
Information Security Trainer	□	□	Crime Investigator	□	□

- How many employees in your institute have IT related responsibilities? ________________
- What is their minimum qualification? ___________________
- Do you provide them any training? Yes/No
- If all of the personnel have not received the required training, what has been the reason?
  □ Insufficient funding
  □ Insufficient time
  □ Other (specify)_________________
- Are training records maintained? Yes/No
- How many of the employees having IT related responsibilities have received the required training? ___________
- Does the institute have clearly defined policy of what constitutes the inappropriate activity within system audit logs? Yes/No
- Does the institute provide any security certifications? If yes, please specify. Yes/No
- Do you have the policy of 'separation of duties'? Yes /No
- Have you conducted risk assessment of the critical assets of the organization? Yes/No
  If yes,
  □ Annually □ Every 6 months □ Quarterly
- Have you conducted vulnerability assessment of your assets? Yes/No
  □ Annually □ Every 6 months □ Quarterly

Hacks, Attacks and Flaws:

Which of the following threat factors exploited your institute in 2014 and 2015?

☐ Cyber criminals
☐ Nation/State
☐ Hacktivists
☐ None
☐ Hackers
☐ Malicious insiders
☐ Non-malicious insiders
☐ Other (specify)

Which of the following attack types have exploited your institute in 2014 and 2015?

☐ Hacking attempts
☐ Malware
☐ Social engineering
☐ Insider Theft
☐ None
☐ Man-in-the-middle Attacks
☐ Phishing
☐ SQL injections
☐ Loss of mobile devices
☐ Other (specify)

Security Threats:

Has your institute experienced increase or decrease in security attacks as compared to 2014?

☐ More attacks ☐ Fewer attacks

How likely do you think it is that your organization will experience a cyber attack in 2016?

☐ Very likely ☐ Likely ☐ Not very likely ☐ Not at all likely

What do you think the incident motivation is?

☐ Financial gain
☐ Intellectual property gain
☐ Theft of classified data
☐ Theft of personally identifiable data
☐ Disruption of service
☐ Other (specify)

Has your institute experienced physical loss of assets? What type of assets?

☐ Workstations
☐ Servers
☐ Network devices
☐ Mobile devices
☐ None

Organizational Security:

On average, how long does it take you to fill a security position?

☐ <2 weeks
☐ 1 month
☐ 2 months
☐ 3 months
☐ 6 months
☐ Cannot fill

What is the biggest skill gap you see in today’s security professionals?

☐ Technical skills
☐ Ability to understand the business
☐ Communication

How much did your institute spend on continuing education opportunities for security professionals (e.g., training, conferences, etc.)?

□ Rs.______________ □ Nothing

Are you comfortable with your security team's ability to detect and respond to incidents?

□ Yes
□ Yes, but only for simple issues
□ No

Where does the security report go to in your organization? ______________________

Do you test security controls?

□ No
□ No, but we are planning to do so
□ No, but we are developing tests
□ Periodically (at least annually)
□ Routinely (at least quarterly)

Do you have a security awareness program in place?

□ Yes □ No

Is there any computer crime investigation cell in the institute?

□ Yes □ No

Does your institute have CSIRT (Computer security Incident response team) set up?

□ Yes □ No

Is your senior management concerned with security?

□ Yes □ No

Do you restrict access to social media in your organization?

□ Yes □ No

Are records kept of which employees have significant security responsibilities?

□ Yes □ No

Physical security:	**Status**	
	Yes	**No**
Are doors to the server rooms and computer spaces locked and guarded?	□	□
Do only authorized people have access to the server rooms?	□	□
How have you secured sensitive physical documents?	□	□
Have you provided the employees with separate badges to ensure authorization?	□	□
How have you maintained physical password files?	□	□
What is the policy of shredding physical media? ____		
Digital security:		
Are anti-viruses installed on all systems?	□	□
Are they updated regularly?	□	□
Are anti-spyware installed on all systems?	□	□

Is logging activated on the systems?	□	□
How is user-authentication ensured on systems? ____		

Assets and Threats:

Rank the following **assets** out of scale of **10** based on their criticality:

Assets	**Rating**
Information systems	
Institute’s official website	
Institute’s learning management system	
Physical documents	
Employee records	
Students’ records	
Server Rooms	
Labs	
Staff rooms/offices	
IT Department	
IT staff	
Faculty	
Students	
Other (specify)	

Rank the following **threats** out of scale of **10** according to your institute:

Threats	**Rating**	**Threats**	**Rating**
Denial-of-service attack		Mobile devices	
Insider threat		Malware	
Virus		Internal employee	
Phishing		Employee negligence	

Spyware		Cloud-based services	
Key loggers		Contractors	
Security unawareness		Hacktivists	
Irresponsible behavior		Trusted third parties	
Hacker		Cyber terrorism	
Application vulnerabilities		Organized crime	

Institute’s top security priorities:

Rank the following according to your institute’s top priorities out of scale of **10**:

Priorities	**Rating**
Governance, risk management, and compliance (GRC)	
Security management	
Security leadership	
Security Operations	
Provide advice on security	
Researching new technologies	
Incident Response	
Software Development	

Kindly enlighten in two lines what improvement do you want to see in your institute from cyber security perspective?

____

____

Representative name (IT Dept.): ____________________

Signature:

Thank you for sparing your valuable time to fill out this questionnaire.
Best Regards!

Appendix B: Questionnaire for general users

Survey for Cybersecurity Training

Risk Analysis Questionnaire

Sector: Academia
Category: General Users

Every year, nearly 430 million adults worldwide fall victims to cyber-crime, at a price of approximately $400 billion on basis of time as well as monetary loss, costing the world more than even drugs and smuggling related crimes combined. Cyber-security involves protection of sensitive information by detecting, preventing, and responding to attacks. Our lives largely rely on information technology, which makes cyber security one of the country's top national security preferences. While the Pakistan government is taking steps to ensure the safety of cyber community, the government cannot solve the issue alone. In fact it is a shared responsibility. You are encouraged to step ahead and make your contribution to this survey which will help enhance the security posture of the academic community of the country.
(Note: You can rest assured that the information you provide shall be kept confidential and will only be reported as aggregate)

Designation: ___________________________________
Discipline/Department: _________________________
Institute: ___________________________________
Email ID: _________________________________ *(Optional)*

General awareness	**Status**		
	Low	**Medium**	**High**
How much do you know about Cyber-security?	□	□	□
How often have you been a victim of a cyber-attack? (Specify the attack)	□	□	□
How much security conscious are you?	□	□	□
How interested are you to know about/get trained on cyber security?	□	□	□
Attacks and threats	**Status**		
	Low	**Medium**	**High**
How often do you use licensed software?	□	□	□
How often do you keep your software patched and updated?	□	□	□

How often do you visit the vendor sites directly to purchase or renew software subscription?	□	□	□
How often do you make use of the security settings on your PC?	□	□	□
How much cautious are you of downloading files from the websites?	□	□	□
How much aware are you of threats of USB drives?	□	□	□
How often do you disable auto-run (in USB drives)?	□	□	□
How much do you know about spyware?	□	□	□
How much do you know about recognizing spyware on your computer?	□	□	□
How much do you know what a Denial-of-service attack?	□	□	□
How much do you know about online frauds?	□	□	□
How much cautious are you of providing personal information on telephone?	□	□	□
How often do you share personal information or finance related data in email?	□	□	□
How often do you check the website’s security before sharing your personal information?	□	□	□
Email and Communication	**Status**		
	Low	**Medium**	**High**
How much aware are you of the dangers of instant messaging and chat rooms?	□	□	□
How often do you reveal the personal information (email ID, phone number etc.) in chat rooms?	□	□	□
How often do you verify the identity of the person you are talking to?	□	□	□
How often do you open unsolicited attachments directly, even from people you know?	□	□	□
How often do you scan the attachments before downloading?	□	□	□
How often do you turn off the option to automatically download attachments?	□	□	□
General Security	**Status**		
	Low	**Medium**	**High**
How much do you know about firewall configuration settings?	□	□	□
How often do you lock your computer when you’re away?	□	□	□
How often do you disconnect your computer from the internet when you’re away?	□	□	□
How often do you back up your data?	□	□	□
What is the level of strength of password you use?	□	□	□
How often do you encrypt personal files?	□	□	□
Mobile Devices	**Status**		
	Low	**Medium**	**High**

How often do you password protect your device?	□	□	□
How often do you use public Wi-Fi networks?	□	□	□
How often do you turn off blue-tooth when not in use?	□	□	□
Privacy	**Status**		
	Low	**Medium**	**High**
How much do you know about how to securely erase the data?	□	□	□
How much do you know about the security implications of the use of cookies?	□	□	□
What is your level of understanding about encryption?	□	□	□
Safe Browsing	**Status**		
	Low	**Medium**	**High**
How much are you aware of security concerns associated with Bluetooth?	□	□	□
How often do you use proxy unblockers?	□	□	□
How much do you know about the difference between http and https?	□	□	□
Software and Applications	**Status**		
	Low	**Medium**	**High**
What is your level of awareness about the security implications of VoIP (Skype, Viber, Whatsapp etc.)?	□	□	□
How much aware are you of the risks of File sharing technology?	□	□	□
How often do you go through the privacy policies of the apps (Angry bird, Flappy bird etc.) before downloading?	□	□	□
Social Networking	**Status**		
	Low	**Medium**	**High**
How much do you know about social networking sites?	□	□	□
How much do you know about the security implications they have?	□	□	□
How often do you check their privacy policies?	□	□	□
How many friends do you share your personal information with online?	□	□	□
How often has your account been hacked?	□	□	□
Internet Usage			

How often do you use internet? (Tick mark)

□ 2-4 hours □ 4-5 hours □ More than 5 hours □ Other (specify)________

Which device do you mostly use for internet access?

□ Mobile □ Laptop □ Desktop computer

What purpose do you mostly use internet for?

□ Entertainment □ Study □ Social networking □ Research

Which operating system do you prefer the most for mobile device considering the security?

□ iOS □Android □Windows

Rate the following social media networks in accordance with your usage.	Status		
	Low	Medium	High
Facebook	□	□	□
Twitter	□	□	□
Snapchat	□	□	□
Whatsapp	□	□	□
Other (specify)	□	□	□
Rate the following in accordance with their vulnerability to threats and attacks.	Status		
	Low	Medium	High
Facebook	□	□	□
Twitter	□	□	□
Snapchat	□	□	□
Line	□	□	□
Other (specify)	□	□	□

Debunking Common Myths	**Status**	
	True	**False**
If you format a hard drive or erase the files on it all the information on it is permanently lost.	□	□
Your computer has no value to hackers, they do not target you.	□	□
If you delete a file from your computer or USB stick, that information can no longer be recovered.	□	□

Please indicate to which age group you belong:

□ Under 20

□ 20-29

□ 30-39

□ 60-69

□ 50-59

□ 40-49

□ 70 or above

Thank you for sparing your valuable time to fill out this questionnaire.
Best Regards!

Appendix C: Questionnaire for IT Staff

Survey for Cybersecurity Training

Sector: Academia
Category: IT
Institute: ___________________

Every year, nearly 430 million adults worldwide fall victims to cyber-crime, at a price of approximately $400 billion on basis of time as well as monetary loss, costing the world more than even drugs and smuggling related crimes combined. Cyber-security involves protection of sensitive information by detecting, preventing, and responding to attacks. Our lives largely rely on information technology, which makes cyber security one of the country's top national security preferences. While the Pakistan government is taking steps to ensure the safety of cyber community, the government cannot solve the issue alone. In fact it is a shared responsibility. You are encouraged to step ahead and make your contribution to this survey which will help enhance the security posture of the academic community of the country.
(Note: You can rest assured that the information you provide shall be kept confidential and will only be reported as aggregate)

(Note: Every role area is to be filled by the staff performing the concerned job tasks)

Role Area: Software Assurance and Security Engineering

Description: Developing plus writing/coding new (or modifying current) computer software, applications, or programs by following the best practices of software assurance..

Roles/Job titles	Yes	No	Qualification	Years of experience
Computer Programmer	□	□		
Research & Development Engineer	□	□		
Software Developer	□	□		

Web Application Developer	□	□		

JOB TASKS

Mark the tasks that are part of your job responsibility:

Sr. No.	Tasks	Status	
		Yes	No
1	Analyze the related information to find, provide recommendation and modify an existing application or plan development of a new application.	□	□
2	Assess the needs of the user and the software requirements to identify if the design is suitable for the cost and time constraints.	□	□
3	Apply the testing and coding policies and standards, apply the security testing techniques and tools.	□	□
4	Application of the ‘secure code documentation’.	□	□
5	List the controls that were used in requirements gathering phase to combine security with the processes, figure out the main objectives, and above all to enhance software/app security while reducing hindrance in schedules and plans.	□	□
6	Finalize the program development documentation and the following revised versions.	□	□
7	Perform the trial runs of applications and programs to ensure they return the required information and ensure the correct instructions given.	□	□
8	Coordinate with relevant individuals i.e. programmer, engineers etc. for the applications development and to get the required information on project capabilities and limitations, interfaces and performance measurements.	□	□
9	Make the security threat model aligned with users’ input by conducting the interviews.	□	□
10	Confer the engineering and IT personnel to assess interfacing between software and hardware.	□	□
11	Error correction by incorporating the required changes and then re-evaluating the program to get the desired results.	□	□
12	Design, create and amend the software systems, by using mathematical models for the measurement of the design outcome.	□	□
13	Create the system testing and the validation procedures, coding and documentation and direct them.	□	□
14	Development of the secure code and address the related (error) messages.	□	□

15	Assess the concerned factors like cost, load and time constraints, reporting formats required and requirement of the security restrictions to determine the software and hardware configuration.	□	□
16	Figure out the basic common programming flaws.	□	□
17	Figure out the expected consequences and consequently apply suitable mechanisms within decentralized and centralized environments in the organization’s IT machines.	□	□
19	Amend the current software to remove the errors, in order to align it with new hardware, and enhance the performance.	□	□
20	Perform QA for security functionality and resilience to attacks.	□	□
21	Conduct secure programming and look for flaws if any in the code to reduce security weaknesses.	□	□
22	Perform risk analysis (e.g. vulnerability, threat and likelihood) when a system or an software app undergoes any change.	□	□
23	Create the flow charts describing input, process, output, relevant the logical operations, then turn those into the instructions that are coded in a suitable machine language.	□	□
25	Convert the security requirements into elements of application design that includes documentation of cyber attack vectors elements, and determination of any security criteria that may be needed.	□	□
26	Conduct software penetration testing if needed for updated or new applications.	□	□
27	Apply the defensive security measures (e.g., encryption, identity management an access control) to reduce chances of successful vulnerability exploitations.	□	□
28	Propose controls and countermeasures for potential exploitations of security weaknesses of programming language in the systems or apps.	□	□
29	Find the suitable software patches for the bugs which could render the software vulnerable.	□	□

COMPETENCIES

Mark the competencies/ Knowledge areas that you possess.

Sr. No.	**Competencies**	**Status**		
		Yes	**No**	**Partially**
1	Embedded Computers	□	□	□
2	Object Technology	□	□	□
3	Information Assurance	□	□	□
4	Systems Testing and Evaluation	□	□	□

5	Computer Languages	□	□	□
6	Infrastructure Design	□	□	□
7	Operating Systems	□	□	□
8	Vulnerabilities Assessment	□	□	□
9	Personnel Safety and Security	□	□	□
10	Computer Languages	□	□	□
11	Configuration Management	□	□	□
12	Software Development	□	□	□
13	Software Engineering	□	□	□
14	Logical Systems Design	□	□	□
15	Web Technology	□	□	□
16	Modeling and Simulation	□	□	□
17	Software Testing and Evaluation	□	□	□
18	Identity Management	□	□	□
19	Information Systems/Network Security	□	□	□
20	Quality Assurance	□	□	□
21	Incident Management	□	□	□
22	Risk Management	□	□	□

Mark the functional perspective of your role:

- □ Manage
- □ Design
- □ Implement
- □ Evaluate

Role Area: Systems Development

Description: Working on the systems development lifecycle’s development phases

Roles/Job titles	Yes	No	Qualification	Years of experience
Firewall Engineer	□	□		

Systems Engineer	□	□		
Security Engineer	□	□		
Information Assurance (IA) Developer				

JOB TASKS

Mark the tasks that are part of your job responsibility:

Sr. No.	Tasks	Status	
		Yes	No
1	Assess the system design constraints, detailed system, trade-offs, and security design	□	□
2	Apply the IT policies to software applications which are linked with each another.	□	□
3	Analyze the effectiveness of protection measures used by IT systems.	□	□
4	Analyze the vulnerabilities of and threats to IT systems for creation of a reliable risk profile.	□	□
5	Create, check, and renew the prototypes by using practical models.	□	□
6	Perform the Privacy Impact Assessments of the applications' designing the right controls, which protect the integrity, privacy and confidentiality of data.	□	□
7	Propose and create information assurance (IA) or IA-related products.	□	□
8	Create the secure interface requirements/specifications between the resources that are interconnected.	□	□
9	Design, create, develop, combine, and update the IT /system security controls (along with policies, procedures and requirements) which ensure integrity and confidentiality,	□	□
10	Design hardware, OS, and software apps to sufficiently fulfill IA security needs	□	□
11	Designing the suitable data backup techniques, and make sure that the suitable technical, managerial and procedural procedures are present for secure backups.	□	□
12	Identify the security requirements to make sure that they are met for all applications.	□	□

13	Create and orient the direct system testing procedure and processes.	□	□
14	Design and check architecture of system components that are compatible with the technical specifications.	□	□
15	Prepare the security documentation in detail for components and interface requirements.	□	□
16	Develop DR (disaster recovery) and operations continuity plans, and make sure that the testing is done prior to systems entering the production environment.	□	□
17	Develop the risk management measures to counter threats and vulnerabilities and propose suitable changes in terms of security.	□	□
18	Develop required IA countermeasures and risk mitigation measures for applications and systems.	□	□
19	Figure out elements/components, assign the security functions to those components, and determine the relationships among them.	□	□
20	Find out and orient the remedies of technical problems emerged in implementation of new IT assets.	□	□
21	Find and prioritize necessary system function, required to assist necessary enterprise functions; in case of resource failure, analyze the system requirements for availability and successful continuity.	□	□
22	Determine, analyze, and recommend suitable IA products for the system use and make sure that the proposed products comply with organization's requirements.	□	□
23	Implement the security designs for existing or new systems.	□	□
24	Incorporate IA vulnerability solutions into the system designs.	□	□
25	Conduct IS risk analysis and propose security safeguards to reduce the expected risk.	□	□
27	Conduct the security review, determine the grey areas that need to be addressed in security architecture.	□	□
27	Conduct risk assessment after a system or application goes through a change.	□	□
29	Give input to the implementation plans and SOP.	□	□
30	Provide required input to RMF procedures, processes and relevant documents.	□	□
31	Retrieve, store and manipulate the data for analysis and needs of capabilities of system.	□	□

32	Give necessary support to certification evaluation processes and procedures.	□	□
33	Trace back all the security needs and specifications to design and create required components.	□	□
35	Verify interoperability, scalability, stability and portability of system architecture	□	□
37	Assess the user requirements and needs to plan and perform system security development.	□	□
39	Make sure that the design and development processes are documented regularly, giving the description of the security implementation, and necessary updating.	□	□

COMPETENCIES

Mark the competencies/ Knowledge areas that you possess.

Sr. No.	**Competencies**	**Status**		
		Yes	**No**	**Partially**
1	Vulnerabilities Assessment	□	□	□
2	Identity Management	□	□	□
3	Mathematical Reasoning	□	□	□
4	Cryptography	□	□	□
5	Database Management Systems	□	□	□
6	Information Assurance	□	□	□
7	Systems Testing and Evaluation	□	□	□
8	Hardware Engineering	□	□	□
9	Embedded Computers	□	□	□
10	Systems Integration	□	□	□
11	Human Factors	□	□	□
12	Information Systems/Network Security	□	□	□
13	Infrastructure Design	□	□	□
14	Computers and Electronics	□	□	□
15	Operating Systems	□	□	□
16	Information Technology Architecture	□	□	□
17	Personnel Safety and Security	□	□	□
18	Logical Systems Design	□	□	□

19	Configuration Management	□	□	□
20	Software Engineering	□	□	□
21	Requirements Analysis	□	□	□
22	Systems Life Cycle	□	□	□
23	Telecommunications	□	□	□
24	Information Systems Security Certification	□	□	□
25	Modeling and Simulation	□	□	□
26	Computer Languages	□	□	□
27	Information Technology Performance Assessment	□	□	□
28	Security	□	□	□
29	Risk Management	□	□	□
30	Network Management	□	□	□

Mark the functional perspective of your role:

□ Manage
□ Design
□ Implement
□ Evaluate

Role Area: Data administration

Developing and administering data management systems and databases that allow for the query, storage and utilization of data.

Roles/Job titles	Yes	No	Qualification	Years of experience
Database Administrator	□	□		
Data Manager	□	□		
Database Developer	□	□		
Information Dissemination Manager	□	□		

JOB TASKS

Mark the tasks that are part of your job responsibility:

Sr. No.	Tasks	Status	
		Yes	No
1	Define and analyze the data specifications and requirements.	□	□
2	Plan and assess the incorporated amendments in the data needs.	□	□
3	Plan and execute the database systems.	□	□
4	Plan and execute data warehousing and the mining programs.	□	□
5	Propose suitable standards of data, policies, processes and procedures	□	□
6	Install and configure the software for database management systems	□	□
7	Maintain the software for DMS.	□	□
8	Ensure maintenance of exchange of information through alert, subscription, and the functions which enable the users exchange sensitive data as needed.	□	□
9	Organize the caching, distribution, and the data retrieval and cataloging.	□	□
10	Monitor the database and update it to ensure the required performance.	□	□
11	Conduct the database backup to prevent data malfunctioning.	□	□
12	Provision of an organized flow of relevant information aligned with the mission and vision requirements.	□	□
13	Propose suggestions on the new architectures and technologies.	□	□

COMPETENCIES

Mark the competencies/ Knowledge areas that you possess.

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Data Management	□	□	□
2	Computer Forensics	□	□	□
3	Database Management Systems	□	□	□
4	Encryption	□	□	□
5	Enterprise Architecture	□	□	□

6	Identity Management	□	□	□
7	Operating Systems	□	□	□
8	Database Administration	□	□	□
9	Modeling and Simulation	□	□	□
10	Security	□	□	□

Mark the functional perspective of your role:

- □ Manage
- □ Design
- □ Implement
- □ Evaluate

Role Area: Network Services

Description: Installing, configuring, testing, operating, maintaining, and managing enterprise networks, their firewalls, including network devices (e.g., switches, bridges, hubs, IPS, IDS, proxy servers, routers) and the software that enable exchange of information in order to support privacy and integrity of information and all the IT resources.

Roles/Job titles	Yes	No	Qualification	Years of experience
Network Administrator	□	□		
Network Designer	□	□		
Network Engineer/analyst	□	□		
Systems Engineer	□	□		
Telecommunications Engineer/Personnel/ Specialist	□	□		

JOB TASKS

Mark the tasks that are part of your job responsibility:

Sr. No.	Tasks	Status	
		Yes	No
1	Configure the network and security devices switches (e.g., tunneling, NATing, IP whitelisting etc.)	□	□
2	Plan, develop and execute the enterprise network and system backup policies and mechanisms.	□	□
3	Troubleshoot and fix the connectivity related problems	□	□
4	Modify the overall network architecture to meet new aims or enhance the network process flow	□	□
5	Execute new test actions, system design methods and QA mechanisms.	□	□
6	Installation and maintenance of the network architecture device Operating system software.	□	□
7	Install or restore network devices.	□	□
8	Integrate or merge the new systems into the current functional infrastructure.	□	□
9	Monitor systems and network efficiency.	□	□
10	Fix identified bugs to ensure information is protected from all illegitimate entities	□	□
11	Provide the required feedback/input on IT network needs, including infrastructure/architecture.	□	□
12	Fix the network connectivity problems	□	□
13	Maintain and test the network infrastructure including hardware and software devices.	□	□

COMPETENCIES

Mark the competencies/ Knowledge areas that you possess.

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Infrastructure Design	□	□	□
2	Hardware	□	□	□
3	Information Assurance	□	□	□
4	Information Systems/Network Security	□	□	□

5	Information Technology Performance Assessment	□	□	□
6	Information Technology Architecture	□	□	□
7	Systems Life Cycle	□	□	□
8	Telecommunications	□	□	□
9	Encryption	□	□	□
10	Capacity Management	□	□	□
11	Network Management	□	□	□
12	Operating Systems	□	□	□
13	Configuration Management	□	□	□
14	Computer Network Defense	□	□	□
15	Web Technology	□	□	□
16	Security	□	□	□

Mark the functional perspective of your role:

□ Manage
□ Design
□ Implement
□ Evaluate

Role Area: System Administration

Description: Installing, configuring, troubleshooting and maintaining configurations of the server in order to ensure their privacy, availability and integrity. This area is also about managing the accounts, firewalls, and the patches. Moreover, includes responsibility for passwords, access control, account creation and administration.

Roles/Job titles	**Yes**	**No**	**Qualification**	**Years of experience**
Local Area Network (LAN) Administrator	□	□		

Security Administrator	□	□		
Server Administrator	□	□		
Systems Administrator	□	□		
Website Administrator	□	□		

JOB TASKS

Mark the tasks that are part of your job responsibility:

Sr. No.	**Tasks**	**Status**	
		Yes	**No**
1	Check the server availability, integrity, functionality and efficiency	□	□
2	Perform the connectivity and functional testing to make sure that operability is continuing.	□	□
3	Perform periodic maintenance of the server including cleaning (both electronically and physically), routine reboots, disk checks, testing and data dumps.	□	□
4	Develop access control lists (ACLs) and group policies to ensure compatibility with needs, standards and business rules of the organization.	□	□
5	Develop and document the system administration SOPs.	□	□
6	Develop and implement procedures and policies for usage of local network.	□	□
7	Install server updates, enhancements and fixes.	□	□
8	Maintain and update the baseline system security in accordance with the company policies	□	□
9	Manage the user accounts and access or privileges to equipment or IT assets.	□	□
10	Manage the server resources including availability, performance, recoverability capacity and serviceability.	□	□
11	Monitor, update and maintain the configuration (of server)	□	□
12	Oversee configuration, installation and implementation of the network devices	□	□
13	Conduct repairs of faulty resources	□	□

14	Coordinate and plan the installation of the modified or new OS, hardware.	□	□
15	Plan and implement the system recovery, data redundancy mechanisms and required actions.	□	□
16	Provision of support for problem-solving plus optimization.	□	□
17	Address software/hardware interface and interoperability issues.	□	□

COMPETENCIES

Mark the competencies/ Knowledge areas that you possess.

Sr. No.	Competencies	Status		
		Yes	**No**	**Partially**
1	Information Systems/Network Security	□	□	□
2	Infrastructure Design	□	□	□
3	Information Technology Performance Assessment	□	□	□
4	Technology Awareness	□	□	□
5	Systems Integration	□	□	□
6	Systems Life Cycle	□	□	□
7	Operating Systems	□	□	□
8	Computer Forensics	□	□	□
9	Information Technology Architecture	□	□	□
10	Encryption	□	□	□
11	Network Management	□	□	□
12	Software Engineering	□	□	□
13	Identity Management	□	□	□
14	Computer Languages	□	□	□
15	Configuration Management	□	□	□
16	Security	□	□	□
17	Telecommunications	□	□	□

Mark the functional perspective of your role:

- □ Manage
- □ Design
- □ Implement

□ Evaluate

Role Area: Computer Network defense (CND) Analysis

Description: By using the defensive security countermeasures and the information collected from a wide range of sources for identifying, assessing and reporting the events that occur or have probability to occur to prevent the privacy compromise of the information or systems.

Roles/Job titles	Yes	No	Qualification	Years of experience
CND Analyst	□	□		
Cybersecurity Intelligence Analyst	□	□		
Network Defense Technician	□	□		
Network Security Engineer	□	□		
Security Operator	□	□		

JOB TASKS

Mark the tasks that are part of your job responsibility:

Sr. No.	Tasks	Status	
		Yes	No
1	Create the required content for CND analysis techniques and tools.	□	□
2	Analyze and characterize the network traffic to detect malicious and abnormal activity and the threats to IT systems and services.	□	□
3	Monitor the external data sources to maintain CND threat state currency and find out the security issues that are impactful for the organization.	□	□

4	Escalate and document the incidents (including alerts' history and status and their severity) that can disrupt normal network processes and operations.	□	□
5	Conduct CND analysis and documentation	□	□
6	Conduct events' correlation using correlation rules and data from various sources in the organization to get environmental awareness and find the criticality of the detected threat.	□	□
7	Provide periodic reports of network activity and the relevant events.	□	□
8	Analyze and collect network based alerts from different sources in the organization and final possible attack vector and implications of these alarms/alerts.	□	□
9	Provide timely detection of alerts and possible attacks/intrusions, misuse of the activities, suspicious activities, and segregate these events from the normal activities.	□	□
10	Use these tools for continuous monitoring and system activity analysis to clearly categorize them into normal, suspicious and malicious activities.	□	□
11	Assess the suspicious/malicious activity to find the exploited vulnerabilities, the attack vectors used, and impact on systems and sensitive data.	□	□
12	Use the defense-in-depth practices and principles (e.g., layered defense and security resilience).	□	□
13	Plan the response action for detected abnormal or malicious activities.	□	□
14	Conduct information assurance controls' tests aligned with pre-defined test procedures and plans.	□	□
15	Determine TTPs (tactics, techniques and procedures for given set of intrusions.	□	□
16	Assess the network topologies to analyze data flows across the network	□	□
18	Analyze and identify network anomalies in traffic by using metadata	□	□
19	Perform analysis, research and correlation for diverse variety of the data sources (warnings and indications)	□	□
20	Validate IDS engine alerts against the network based traffic using relevant network analysis tools.	□	□
21	Identify operating systems and applications of a network system or device on the basis of network traffic.	□	□
22	Triage malware	□	□
23	Replay malicious network activity or attack.	□	□
24	Find OS, conduct network mapping using network scanners.	□	□

COMPETENCIES

Mark the competencies/ Knowledge areas that you possess.

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Vulnerabilities Assessment	□	□	□
2	Computer Network Defense	□	□	□
3	Cryptography	□	□	□
4	Computer Forensics	□	□	□
5	Information Systems/Network Security	□	□	□
6	Incident Management	□	□	□
7	Information Assurance	□	□	□
8	Infrastructure Design	□	□	□
9	Technology Awareness	□	□	□
10	Computer Languages	□	□	□
11	Encryption	□	□	□
12	Knowledge Management	□	□	□
13	Telecommunications	□	□	□
14	Operating Systems	□	□	□
15	Configuration Management	□	□	□
16	Data Management	□	□	□
17	Criminal Law	□	□	□

Mark the functional perspective of your role:

□ Manage
□ Design
□ Implement
□ Evaluate

Role Area: Incident Response

It refers to responding to the crisis or emergency situations within the specific domain for catering threats and containing the damage. Also includes using the remediation, preparedness, investigation of events and high risk alarms.

Roles/Job titles	Yes	No	Qualification	Years of experience
Computer Crime Investigator	□	□		
Incident Handler and responder	□	□		
Incident Response Analyst and Coordinator	□	□		

JOB TASKS

Mark the tasks that are part of your job responsibility:

Sr. No.	Tasks	Status	
		Yes	No
1	Coordinate and provide technical required support to the CND technicians in the organization to resolve CND related incidents.	□	□
2	Correlate the gathered data for identifying vulnerabilities and propose the recommendations accordingly.	□	□
3	Monitor the data sources (CERTs, Security Focus, SANS) to maintain the threat state currency and determine the security issues that may be impactful for the organization.	□	□
4	Perform log file analysis from various sources for identification of possible threats to the security of network.	□	□
5	Conduct C2 (command and control) procedures in order to respond to security incidents.	□	□
6	Perform CND incident triage, for inclusion of determination of urgency, scope, and impact; identification of the weakness, security loopholes; proposing recommendations which can provide quick remediation.	□	□
7	Conduct forensically sound image acquisition and propose suitable remediation for IT assets.	□	□
8	Perform network incident handling (like threat analysis, forensics examination, direct system remediation and intrusion correlation/tracking).	□	□

9	Analyze and receive network based alarms from different hosts in the organization and find attack-vector for these.	□	□
10	Document and track the CND incidents starting from initial detection of alerts to final resolution of them.	□	□
11	Write the guidance, documents and reporting on the threat findings for concerned personnel.	□	□
12	Collect artifacts related to the caused intrusion (e.g., malware, signature, and Trojans) and use this data to provide remediation of the incidents in the organization.	□	□

COMPETENCIES

Mark the competencies/ Knowledge areas that you possess.

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Computer Forensics	□	□	□
2	Infrastructure Design	□	□	□
3	Incident Management	□	□	□
4	Computer Network Defense	□	□	□
5	Information Systems/Network Security	□	□	□
6	Vulnerabilities Assessment	□	□	□
7	Information Assurance	□	□	□

Mark the functional perspective of your role:

- □ Manage
- □ Design
- □ Implement
- □ Evaluate

Role Area: Vulnerability Assessment and Management

Description: Conducting the assessments of vulnerabilities and threats, determining the acceptable deviations from the configurations organizations own policies and conducting risk assessment, followed by the development of suitable mitigation safeguards for all kinds of situations.

Roles/Job titles	**Yes**	**No**	**Qualification**	**Years of experience**
Blue Team Technician	□	□		
Ethical Hacker	□	□		
Penetration Tester	□	□		
Red Team Technician	□	□		
Reverse Engineer	□	□		
Risk/Vulnerability Analyst	□	□		
Vulnerability Manager	□	□		

JOB TASKS

Mark the tasks that are part of your job responsibility:

Sr. No.	**Tasks**	**Status**	
		Yes	**No**
1	Assess organization's CND policies and procedures and verify whether they comply with organizational directives and regulation.	□	□
2	Perform authorized penetration testing on organization’s critical IT assets.	□	□
3	Prepare a deployable CND audit to provide support for audit purposes.	□	□

4	Maintain updated CND knowledge and policies, procedures and regulations, that are applicable and that are specifically related to CND auditing.	□	□
5	Prepare the audit reports identifying procedural and technical findings, and give recommended solutions or mitigation strategies.	□	□
6	Conduct non-technical (operations and people) and technical (technology) evaluation of vulnerability and risk assessments of related IT focus areas	□	□
7	Provide assistance with the selection of economic security safeguards to cater for risk (e.g., protection of processes, information and systems)	□	□

COMPETENCIES

Mark the competencies/ Knowledge areas that you possess.

Sr. No.	Competencies	Status		
		Yes	No	Partially
1	Vulnerabilities Assessment	□	□	□
2	Computer Forensics	□	□	□
3	Information Assurance	□	□	□
4	Identity Management	□	□	□
5	Infrastructure Design	□	□	□
6	Computer Languages	□	□	□
7	Computer Network Defense	□	□	□
8	Systems Testing and Evaluation	□	□	□
9	Information Systems/Network Security	□	□	□
10	Human Factors	□	□	□
11	Information Assurance	□	□	□
12	Computer Languages	□	□	□
13	Contracting/Procurement	□	□	□
14	Criminal Law	□	□	□

Mark the functional perspective of your role:

- □ Manage

- □ Design
- □ Implement
- □ Evaluate

Role Area: Education and Training

It refers to conducting the personnel training within the pertinent subject domain. Also includes developing, planning, coordinating, delivering, and/or evaluating the training methods, courses, and techniques as needed.

Roles/Job titles	Yes	No	Qualification	Years of experience
Cyber trainer	□	□		
Information Security Trainer	□	□		
Security Training Coordinator	□	□		

JOB TASKS

Mark the tasks that are part of your job responsibility:

Sr. No.	Tasks	Status	
		Yes	No
1	Conduct the interactive and healthy training drills for creation of an efficient and effective learning environment.	□	□
2	Correlate the vision and mission requirements with training	□	□
3	Deliver the training modules that match the need of the target audience and that are aligned with the physical environment	□	□
4	Demonstrate relevant techniques or concepts to the subordinates or colleagues or team members.	□	□
5	Design the required course content and training syllabi.	□	□
6	Determine the requirements of training.	□	□

7	Develop new training modules that address the need of the intended audience.	□	□
8	Develop goals and objectives for cyber security awareness, education and training.	□	□
9	Evaluate the comprehensiveness and effectiveness of existing training programs	□	□
10	Develop classroom formats and techniques plan (e.g., demonstrations, lectures, multimedia presentations).	□	□
11	Plan on some non-classroom training formats and techniques (e.g., web-based trainings, video courses etc.)	□	□
12	Review and update the documented training modules (e.g., lesson plans, student texts, examinations and descriptions of the course).	□	□
13	Revise the course material on the basis of the feedback obtained from the preceding training sessions.	□	□
14	Serve as an advisor and internal consultant in one's own area of forte.	□	□
15	Support the design, development and execution of the relevant case studies.	□	□
16	Write relevant instructional material (e.g., Standard operating procedures) for guidance purposes.	□	□

COMPETENCIES

Mark the competencies/ Knowledge areas that you possess.

Sr. No.	**Competencies**	**Status**		
		Yes	**No**	**Partially**
1	Computer Network Defense	□	□	□
2	Infrastructure Design	□	□	□
3	Technology Awareness	□	□	□
4	Operating Systems	□	□	□
5	Multimedia Technologies	□	□	□
6	Computers and Electronics	□	□	□
8	Technology Awareness	□	□	□
9	Teaching Others	□	□	□

10	Oral Communication	□	□	□
11	Organizational Awareness	□	□	□
12	Information Systems/Network Security	□	□	□

Mark the functional perspective of your role:

- □ Manage
- □ Design
- □ Implement
- □ Evaluate

Appendix D: IT Training Modules

Skill set ID	**Skill set**
	Overall
OV-1	Communication skill in writing and orally both
OV-2	Skill in reasoning techniques
OV-3	Knowledge of basic concepts of Information Awareness
OV-4	Knowledge of organizational awareness
OV-5	Knowledge of the Risk Management Framework and the corresponding guidance
OV-6	Knowledge of risks associated with social media
OV-7	Knowledge of the NIST SP 800-53, "*Guide for Assessing the Security Controls in Federal Information Systems"* security controls and the corresponding guidance
OV-8	Knowledge of the ethical standards
OV-9	Knowledge of technical reports and documents
OV-10	Skill in ethical testing and the implementation of security measures
OV-11	Skill in problem solving
OV-12	Knowledge of mathematical reasoning
OV-13	Knowledge and skill of quality assurance
	Architecture
ARC-1	Knowledge of the embedded systems
ARC-2	Knowledge of enterprise messaging systems and relevant software
ARC-3	Knowledge and skill of digital rights management
ARC-4	Knowledge of the organization's IT related objectives and goals
ARC-5	Knowledge of VPN security
ARC-6	Skill in implementing the standards, methods and approaches for analyzing, describing and documenting the organization's IT architecture
ARC-7	Skill in usage of VPN devices
ARC-8	Skill in analysis and securing the IT architecture
ARC-9	Knowledge of IT architecture frameworks and concepts

ARC-10	Knowledge of the industry-standard and the organizationally accepted security methods and principles
ARC-11	Knowledge of distributed and parallel computing concepts
ARC-12	Knowledge of the engineering concepts
ARC-13	Knowledge of concepts of remote access technology
ARC-14	Knowledge of structured analysis methods and principles
ARC-15	Knowledge of the enterprise IT architecture
ARC-16	Knowledge of system design methods, tools and techniques, including automated systems design and analysis tools
ARC-17	Knowledge of communication principles, methods, and concepts which support network infrastructure
ARC-18	Knowledge of the routing principles
ARC-19	Knowledge of computer networking concepts
ARC-20	Knowledge of local specialized system requirements for performance, safety and reliability
ARC-21	Knowledge of the common networking services and protocols and their way of interaction to provide the network communications
	Computer Network Defense
CND-1	Knowledge of Computer Network Defense and the vulnerability assessment tools, including the open source tools and techniques and their capabilities
CND-2	Knowledge of the network layer common attack vectors
CND-3	Knowledge of prevention system and intrusion detection tools, techniques and applications
CND-4	Knowledge of different attack classes
CND-5	Knowledge of the Content dev
CND-6	Knowledge of the operational threat environments
CND-7	Knowledge of the intrusion detection and prevention system software and software types
CND-8	Knowledge of malware analysis methodology and concepts
CND-9	Skill in malware handling
CND-10	Knowledge of the general attack stages

CND-11	Skill in detecting network-based and host-based intrusions via intrusion prevention and detection , and the other network monitoring tools
CND-12	Skill in deep analysis of the captured malicious code
CND-13	Skill in mimicking the threat behaviors
CND-14	Knowledge of the malware analysis and relevant tools
CND-15	Skill in tuning the security monitoring sensors
CND-16	Knowledge of the debugger aware malware, virtual machines aware malware and packing
CND-17	Knowledge of Insider Threat investigations, investigative tools, reporting, and laws or regulations
CND-18	Skill in analysis of the anomalous code as benign or malicious
CND-19	Knowledge of the computer network methodologies and operations, including exploitation and analysis.
CND-20	Skill in identifying the obfuscation techniques and malware removal
CND-21	Knowledge of the common adversary tactics, capabilities, tactics, procedures and techniques in assigned responsibility area
CND-22	Skill in conducting the investigations and developing the comprehensive reports
CND-23	Knowledge of network security architecture and Defense-In-Depth principles
CND-24	Skill in interpreting the results of debugger to ascertain techniques, tactics, and procedures
CND-25	Skill in data collection from a variety of CND resources
CND-26	Skill in the malware analysis
CND-27	Skill in network protection against malware
CND-28	Knowledge of the CND Service Provider reporting processes and structure within the organization
CND-29	Knowledge of CND procedures, policies, and regulations
CND-30	Skill in de-conflicting the cyber operations and the activities from the operational activities
	Cryptography and Encryption
CE-1	Knowledge of the encryption methodologies

CE-2	Skill in one way hash functions
CE-3	Knowledge of the encryption algorithms
CE-4	Knowledge of the computer algorithms
CE-5	Knowledge of concept of cryptography
CE-6	Skills in implementing the cryptography (standard based)
CE-7	Knowledge of cryptographic implementation
CE-8	Skill in implementation and maintenance of transmission confidentiality, availability and integrity
CE-9	Skill in the encryption methodologies
CE-10	Skill in implementing NSA approved cryptography (For mature organizations)
CE-11	Skill in cryptographic implementation
CE-12	Knowledge of FIPS validated cryptography (For mature organizations)
CE-13	Skill in decryption of the digital data
CE-14	Knowledge of NSA approved cryptography (For mature organizations)
CE-15	Knowledge of certificate management infrastructures
	Database
DB-1	Skill in allocating the storage capacity in database management systems design
DB-2	Skill in conducting queries and development of algorithms of analysis of data structures
DB-3	Skill in database designing
DB-4	Skill in generating reports and queries
DB-5	Skill in optimizing the database performance
DB-6	Skill in database maintenance
DB-7	Knowledge of database management systems, table relationships, query languages and views
DB-8	Skill in backup plans implementation
DB-9	Knowledge of the database systems
DB-10	Skill in implementing the maintenance plans
DB-11	Knowledge of the query languages.

	Emerging Technologies
ET-1	Knowledge of the new and emerging IT and IT security technologies
ET-2	Knowledge of the emerging computer-based technology which have the potential for exploitation by adversaries
ET-3	Knowledge of the technological developments in server administration
ET-4	Knowledge of industry indicators that are useful for identification of the technology trends
ET-5	Knowledge of the functionality and capabilities associated with various technologies of content creation
ET-6	Knowledge of products of major vendors and how the differences impact the exploitation or vulnerabilities
ET-7	Knowledge of the capabilities and functionality of various collaborative technologies
ET-8	Knowledge of the emerging security risks, issues and weaknesses
ET-9	Skill in application and incorporation of the IT technologies into the proposed solutions
ET-10	Knowledge of cloud computing environments and the associated risks
ET-11	Skill in the determination of validity of the technology trend data
	Identity Management/Privacy
IMP-1	Knowledge of the access authentication methods
IMP-2	Knowledge of the organizational IT user security policies
IMP-3	Knowledge of identity management and network access
IMP-4	Skill in identification of privacy issues and the associated mitigation
IMP-5	Knowledge of the risk adaptive and policy-based access controls
IMP-6	Knowledge of the use, collection and maintenance and sharing of PII
IMP-7	Skill in applying network/host access controls
IMP-8	Skill in conducting PIA (Privacy Impact Assessment)
IMP-9	Skill in developing and applying the security system access controls
IMP-10	Skill in monitoring the privacy controls and the internal privacy policies
IMP-11	Skill in maintenance of the directory services

	Web Security
WS-1	Knowledge of theweb services
WS-2	Knowledge of the common web application attack vectors
WS-3	Knowledge of session management , web collection, searching/analysis of the tools, techniques and cookies
WS-4	Knowledge of the user input validation tools/techniques for the web applications
WS-5	Knowledge of the web filtering technologies
WS-6	Skill in performing the web applications testing
WS-7	Knowledge of OWASP, ISO, and other standards relating to web based applications (For mature infrastructures)
WS-8	Knowledge of the web applications firewalls
WS-9	Skill in building, developing and testing the security of the web services and web applications
WS-10	Skill in training the authorized individuals to make sure that the publicly available information does not contain private information
	IT Systems And Operations
ITSO-1	Knowledge of the circuit analysis
ITSO-2	Skill in managing the information system accounts and their access to the information systems
ITSO-3	Knowledge of the microprocessors
ITSO-4	Skill in determination of the organizationally defined auditable events
ITSO-5	Skill in using the appropriate tools for repairing hardware, software and peripheral equipment of a system
ITSO-6	Skill in handling the audit processing failures
ITSO-7	Knowledge of basic physical computer architecture and components, including the functions of various peripherals and components (e.g., CPUs, data storage, Network Interface Cards,)
ITSO-8	Knowledge of the audit records and the protection thereof
ITSO-9	Skill in physically assembling and disassembling the PCs
ITSO-10	Skill in implementation of the protection of audit records
ITSO-11	Skill in conducting the information searches

ITSO-12	Skill in tracking use of software
ITSO-13	Skill in the basic computer operation
ITSO-14	Skill in monitoring the policy compliance for the user-installed software
ITSO-15	Skill in processing the collected data for the follow-on analysis
ITSO-16	Skill in protecting the privacy/confidentiality of transmitted information
ITSO-17	Knowledge of storage capacity
ITSO-18	Knowledge how information can be protected during the transmission
ITSO-19	Knowledge of applications and capabilities of network equipment including switches, hubs, routers, servers, bridges, transmission media, and the related hardware
ITSO-20	Skill in performing the information system backups
ITSO-21	Knowledge of network hardware functions and devices.
ITSO-22	Knowledge of processes to maintain the user and system documentation
ITSO-23	Skill in implementing the auditable events
ITSO-24	Skill in employing the audit reduction and the report generation capabilities
ITSO-25	Skill in configuring and utilizing hardware-based computer protection components
ITSO-26	Knowledge of report generation and audit reduction
ITSO-27	Knowledge of electrical engineering as applied to computer architecture, including chips, processors, circuit boards, and the associated computer hardware
	Modeling and Simulation
MS-1	Skill in developing the data models
MS-2	Skill in creating and utilizing statistical or mathematical models
MS-3	Skill in the use of design modeling
	Personnel Security
PS-1	Knowledge of the human-computer interaction principles
PS-2	Knowledge of the third party access requirements

PS-3	Knowledge of promotion of general awareness regarding use of social engineering techniques
PS-4	Knowledge of ethical testing
PS-5	Knowledge of PIA (Privacy Impact Assessments)
PS-6	Knowledge of social dynamics of computer attackers in a global context
PS-7	Knowledge of the operations security
PS-8	Knowledge of threat list countries' cyber intent, capabilities, opportunities, and presence
PS-9	Skill in assigning the position descriptions
PS-10	Knowledge of the correct behavior for use of information systems
PS-11	Knowledge of hiring, terminating and transferring actions that impact the information systems access
PS-12	Skill in writing the rules which govern the correct behavior for use of information systems.
	Software
SW-1	Knowledge of the software debugging principles
SW-2	Skill in creating the programs that process and validate multiple inputs including the command line arguments, input streams and environmental variables
SW-3	Knowledge of the software design tools, techniques and methods
SW-4	Skill in tailoring the code analysis for concerns that are application-specific
SW-5	Skill in conducting the software debugging
SW-6	Knowledge of all low-level computer languages
SW-7	Skill in developing the applications that can log errors, application faults, exceptions and logging
SW-8	Knowledge of programming language logic and structures
SW-9	Skill in using code analysis tools to remove the bugs
SW-10	Skill in writing the code in a modern programming language
SW-11	Skill in writing the kernel level applications
SW-12	Knowledge of the language command line(s)
SW-13	Knowledge of Middleware

SW-14	Knowledge of compiled and interpreted computer language
SW-15	Knowledge of the debugging tools and procedures
SW-16	Knowledge of the secure coding techniques
SW-17	Skill in developing the technical design documentation
SW-18	Skill in use of the binary analysis tools
SW-19	Skill in developing the software design documentation
SW-20	Skill in reading the Hexadecimal data
SW-21	Knowledge of the software development models
SW-22	Skill in identifying the common encoding techniques
SW-23	Knowledge of principles of software engineering
SW-24	Knowledge of the system security plans
SW-25	Skill in optimizing and configuring software
SW-26	Skill in the implementing the security plans
SW-27	Knowledge of processes of software quality assurance
SW-28	Knowledge of firmware, software and information integrity verification tools
SW-29	Knowledge of secure software deployment tools, practices and methodologies.
SW-30	Skill in employing firmware, software and tools for information integrity verification.
SW-31	Skill in configuration and utilization of the tools for software-based computer protection.
SW-32	Knowledge of software assurance
	Advanced Network Technology and Protocols
ANTP-1	Knowledge of the mobile technologies
ANTP-2	Knowledge of the security impacts of advanced network protocols and technology
ANTP-3	Skill in implementing and securing the mobile technologies
ANTP-4	Knowledge of how advanced network protocols and services interact to provide the network communications
ANTP-5	Skill in implementing the advanced protocols
	Configuration Management
CM-1	Knowledge of secure configuration management techniques

CM-2	Knowledge of information system component inventory
CM-3	Skill in developing configuration baselines per appropriate hardening guides
CM-4	Skill in developing information system component inventory
CM-5	Skill in documenting configuration settings
CM-6	Knowledge of configuration management plan and how it is used
CM-7	Skill in security impact analysis of changes to the configuration
CM-8	Skill in developing configuration management plan
CM-9	Knowledge of configuration change control
CM-10	Knowledge of configuration management requirements for developers
CM-11	Knowledge of access restrictions for change
CM-12	Skill in implementing configuration change controls
CM-13	Skill in developing configuration management policy and procedures
CM-14	Skill in implementing configuration management plan
CM-15	Skill in maintaining configuration baseline of the information system
	Data Security
DS-1	Skill in analyzing network traffic capacity and performance characteristics
DS-2	Knowledge of database theory
DS-3	Knowledge of data administration and data standardization policies and standards
DS-4	Skill in data reduction
DS-5	Knowledge of data mining and data warehousing principles
DS-6	Skill in the interpretation and incorporation of data from multiple tool sources
DS-7	Knowledge of sources, characteristics, and uses of the organization’s data assets
DS-8	Knowledge of complex data structures
DS-9	Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information
DS-10	Knowledge of computer programming principles such as object-oriented design

DS-11	Knowledge of the characteristics of physical and virtual data storage media
DS-12	Skill in Data Loss Prevention technologies (DLP)
DS-13	Skill in developing data dictionaries
DS-14	Knowledge of logical access to system functions
DS-15	Skill in developing data repositories
DS-16	Skill in enforcing logical access controls
DS-17	Skill in data mining techniques
DS-18	Skill in enforcement of information flow policies
	Emerging Technologies
ET-1	Knowledge of new and emerging IT and IT/cybersecurity technologies
ET-2	Knowledge of emerging computer-based technology that have potential for exploitation by adversaries
ET-3	Knowledge of new technological developments in server administration
ET-4	Knowledge of industry indicators useful for identifying technology trends
ET-5	Knowledge of the capabilities and functionality associated with various content creation technologies
ET-6	Knowledge of products and nomenclature of major vendors and how differences affect exploitation/vulnerabilities
ET-7	Knowledge of the capabilities and functionality of various collaborative technologies
ET-8	Knowledge of emerging security issues, risks, and vulnerabilities
ET-9	Skill in applying and incorporating IT technologies into proposed solutions
ET-10	Knowledge of cloud computing environments and the risks
ET-11	Skill in the determination of the validity of technology trend data
	Incident Management
IM-1	Knowledge of procedures used for documenting and querying reported incidents
IM-2	Knowledge of secure transfer of evidence to forensics

IM-3	Knowledge of incident categories, incident responses, and timelines for responses
IM-4	Skill in security monitoring to determine possible incidents
IM-5	Knowledge of incident response and handling methodologies
IM-6	Skill to correlate and combine data to develop information about the capabilities, intent, and operations of criminal and/or adversary organizations
IM-7	Skill in recovering failed servers
IM-8	Skill in recognizing and categorizing types of vulnerabilities and associated attacks
IM-9	Skill in using incident handling methodologies
IM-10	Skill in performing damage assessments from incidents
IM-11	Knowledge of enterprise incident response program, roles, and responsibilities
IM-12	Knowledge of processes for reporting security related incidents
IM-13	Knowledge of root cause analysis for incidents
IM-14	Skill in monitoring and evaluating security incident trends
IM-15	Skill in performing root cause analysis for incidents
IM-16	Knowledge that security incident trends exist
IM-17	Skill in isolating compromised systems
IM-18	Skill in providing incident response support
IM-19	Knowledge in performing traffic analysis
IM-20	Knowledge of security alerts, advisories, and directives
	Information Systems
IS-1	Knowledge of how system components are installed, integrated, and optimized
IS-2	Knowledge of operating system's ports and services
IS-3	Knowledge of principles and methods for integrating server components
IS-4	Skill in installing and configuring virtual machines
IS-5	Knowledge of technology integration processes
IS-6	Skill in matching the appropriate knowledge repository technology for a given application or environment

IS-7	Skill in designing the integration of hardware and software solutions
IS-8	Knowledge of “knowledge base” capabilities in identifying the solutions to less common and more complex system problems
IS-9	Knowledge of operating systems
IS-10	Skill in conducting knowledge mapping
IS-11	Knowledge of server and client operating systems
IS-12	Skill in conducting open source research for troubleshooting client-level problems
IS-13	Knowledge of systems administration concepts
IS-14	Skill in using knowledge management technologies
IS-15	Skill in system administration for operating systems
IS-16	Knowledge of Storage Area Networks
IS-17	Knowledge of file system implementations
IS-18	Knowledge of external information system impact to the security baseline
IS-19	Knowledge of virtualization technologies and virtual machine development and maintenance
IS-20	Knowledge of information backed up and schedule of information system backup
IS-21	Knowledge of command lines
IS-22	Knowledge of identification and authentication techniques
IS-23	Skill in identifying, modifying, and manipulating applicable system components
IS-24	Skills in implementing identification and authentication through various means
IS-25	Skill in reading, interpreting, writing, modifying, and executing simple scripts on systems that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data
IS-26	Knowledge of various types of Spam and other attack methodologies
IS-27	Skill in operating virtual machines
IS-28	Skill in implementing protective measures for various types of Spam and other attacks

IS-29	Knowledge of troubleshooting basic systems and operating system related issues
IS-30	Skill in utilizing virtual networks for testing
IS-31	Knowledge of operating system structure and internals
	IT Security Awareness And Training
ISAT-1	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain
ISAT-2	Skill in developing and executing technical training programs and curricula
ISAT-3	Skill in developing curriculum that speaks to the topic at the appropriate level for the target audience
ISAT-4	Skill in maintaining and retaining security training records
ISAT-5	Skill in identifying upcoming IA topics to ensure awareness
ISAT-6	Skill in developing and executing tests of the contingency plans
ISAT-7	Skill in preparing and delivering education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures
ISAT-8	Knowledge of requirements for developer provided IT/cybersecurity training
ISAT-9	Skill in identifying gaps in technical capabilities
ISAT-10	Skill in training individuals in contingency planning
ISAT-11	Knowledge of academic institutions dealing with cybersecurity issues
ISAT-12	Skill in training individuals in incident response procedures
	Network And Telecommunications Security
NTS-1	Skill in conducting server planning, management, and maintenance
NTS-2	Knowledge of the CND Service Provider reporting structure and processes within one’s own organization for network incidents
NTS-3	Skill in correcting physical and technical problems which impact server performance
NTS-4	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities
NTS-5	Skill in diagnosing connectivity problems

NTS-6	Skill in developing and deploying intrusion detection/protection signatures
NTS-7	Skill in diagnosing failed servers
NTS-8	Skill in discerning the protection needs (i.e., security controls) of networks
NTS-9	Skill in testing and configuring network hardware and peripherals
NTS-10	Skill in implementing, maintaining, and improving established network security practices
NTS-11	Skill in using network management tools to analyze network traffic patterns
NTS-12	Knowledge of front-end collection systems, including network traffic collection, filtering, and selection
NTS-13	Knowledge of the capabilities of different electronic communication systems and methods
NTS-14	Knowledge of security event correlation tools
NTS-15	Knowledge of the range of existing networks
NTS-16	Knowledge of current and emerging threats/threat vectors
NTS-17	Knowledge of network systems management principles, models, methods and tools
NTS-18	Knowledge of basic network administration, and network hardening techniques
NTS-19	Skill in configuring and utilizing network protection components
NTS-20	Knowledge of network security architecture concepts including topology, protocols, components, and principles
NTS-21	Knowledge of organization's LAN/WAN pathways and other telecommunication pathways
NTS-22	Skill in reading and interpreting intrusion detection/protection signatures
NTS-23	Knowledge of how network services and protocols interact to provide network communications
NTS-24	Knowledge of intrusion detection/protection signature implementation impact

NTS-25	Knowledge of local area and wide area networking principles and concepts including bandwidth management
NTS-26	Skill in enforcement of policies
NTS-27	Knowledge of network protocols
NTS-28	Knowledge of packet-level analysis
NTS-29	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs
NTS-30	Knowledge of telecommunications concepts
NTS-31	Knowledge of how traffic flows across the network
NTS-32	Knowledge of basic concepts, terminology, and operations of a wide range of communications media
NTS-33	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches
NTS-34	Knowledge of different types of network communication
NTS-35	Skill in network mapping and recreating network topologies
NTS-36	Knowledge of the nature and function of the relevant information structure
NTS-37	Skill in using sub-netting tools
NTS-38	Knowledge of Voice over IP (VoIP)
NTS-39	Knowledge of common network tools
NTS-40	Knowledge of mobile communications architecture
NTS-41	Knowledge of host/network access controls
NTS-42	Knowledge of transmission methods
NTS-43	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins
NTS-44	Skill in establishing a routing schema
NTS-45	Knowledge of IT security principles and methods
NTS-46	Skill in applying network programming towards client/server model
NTS-47	Knowledge of current industry methods for evaluating, implementing, and disseminating network security assessment, monitoring, detection and remediation tools and procedures utilizing standards-based concepts and capabilities
NTS-48	Knowledge of organization's LAN/WAN pathways

NTS-49	Knowledge of network traffic analysis methods
NTS-50	Skill in testing alternate telecommunication services
NTS-51	Knowledge of network security design tools, methods, and techniques
NTS-52	Knowledge of collaborative computing devices and their risk to the information system security baseline
	Security Risk Management
SRM-1	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
SRM-2	Knowledge of how different file types can be used for anomalous behavior
SRM-3	Skill to identify systemic security issues based on the analysis of vulnerability and configuration data
SRM-4	Knowledge of measures or indicators of system performance and availability
SRM-5	Knowledge of application vulnerabilities
SRM-6	Knowledge of performance tuning tools and techniques
SRM-7	Knowledge of penetration testing principles, tools, and techniques
SRM-8	Skill in identifying and anticipating server performance, availability, capacity, or configuration problems
SRM-9	Knowledge of system and application security threats and vulnerabilities
SRM-10	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system
SRM-11	Knowledge of network security threats and vulnerabilities
SRM-12	Skill in monitoring and optimizing server performance
SRM-13	Skill in assessing the robustness of security systems and designs
SRM-14	Skill in conducting audits or reviews of technical systems
SRM-15	Skill in designing countermeasures to identified security risks
SRM-16	Skill in risk management processes, including steps and methods for assessing risk
SRM-17	Skill in evaluating the adequacy of security designs

SRM-18	Knowledge of organization's risk tolerance and/or risk management approach
SRM-19	Skill in performing packet-level analysis
SRM-20	Knowledge of supply chain risk management processes and practices
SRM-21	Skill in the use of penetration testing tools and techniques
SRM-22	Knowledge of risk threat assessment
SRM-23	Skill in using protocol analyzers
SRM-24	Skill in implementing IT supply chain security/risk management policies, requirements, and procedures
SRM-25	Skill in applying white hat hacking/security auditing techniques, procedures, and tools
SRM-26	Knowledge of Risk Management Framework
SRM-27	Skill in using network analysis tools to identify vulnerabilities
SRM-28	Skill in creating policies that reflect system security goals
SRM-29	Skill in utilizing exploitation tools to identify system/software vulnerabilities
SRM-30	Skill in correlation of data to develop information about the capabilities, intent, and operations of criminal and/or adversary organizations
SRM-31	Skill in utilizing network analysis tools to identify software communications vulnerabilities
SRM-32	Knowledge of hacking methodologies
SRM-33	Knowledge of reverse engineering concepts and techniques
SRM-34	Skill in analyzing audit records
	Systems And Application Security
SAS-1	Knowledge of server administration and systems engineering theories, concepts, and methods
SAS-2	Skill in evaluating test plans for applicability and completeness
SAS-3	Knowledge of systems lifecycle management principles, including software security and usability
SAS-4	Skill in secure test plan design
SAS-5	Knowledge of the operations and processes for diagnosing common or recurring system problems

SAS-6	Knowledge of known system and application vulnerabilities from alerts, advisories, errata, and bulletins
SAS-7	Knowledge of the systems engineering process
SAS-8	Knowledge of IT/cybersecurity systems engineering principles
SAS-9	Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly
SAS-10	Knowledge of system and application security principles and methods
SAS-11	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation
SAS-12	Knowledge of current industry methods for evaluating, implementing, and disseminating IT security assessment, monitoring, detection and remediation tools and procedures utilizing standards-based concepts and capabilities
SAS-13	Skill in installing computer and server upgrades
SAS-14	Knowledge of security system design tools, methods, and techniques
SAS-15	Knowledge of the life cycle process
SAS-16	Knowledge of the Service Provider reporting structure and processes within one’s own organization
SAS-17	Knowledge of systems diagnostic tools and fault identification techniques
SAS-18	Skill in discerning the protection needs (i.e., security controls) of information systems
SAS-19	Knowledge of systems testing and evaluation methods
SAS-20	Knowledge of system and application security event correlation tools
SAS-21	Skill in applying organization-specific systems analysis principles and techniques
SAS-22	Knowledge of software related IT security principles and methods
SAS-23	Skill in conducting test events
SAS-24	Knowledge of basic system administration, and operating system hardening techniques
SAS-25	Skill in designing a data analysis structure

SAS-26	Skill in basic system administration, and operating system hardening techniques
SAS-27	Skill in determining an appropriate level of test rigor for a given system
SAS-28	Knowledge of signature implementation impact
SAS-29	Skill in developing operations-based testing scenarios
SAS-30	Knowledge of malicious code protection mechanisms
SAS-31	Skill in systems integration testing
SAS-32	Skill in implementing malicious code protection
SAS-33	Skill in writing test plans
SAS-34	Knowledge of current and emerging threats/threat vectors against information systems and applications

BIBLIOGRAPHY

[1] Michael Portnoy, Seymour Goodman, “Global Initiatives to Secure Cyberspace: An Emerging Landscape”, Advances in Information Security, 2008

[2] Cybercore Technologies, “The Information Assurance Process: Charting a Path Towards Compliance” [Online] Available: http://docplayer.net/6483577-The-information-assurance-process-charting-a-path-towards-compliance.html

[3] [Online] Available: https://www.sans.org/reading-room/whitepapers/basics/protection-information-assets-594

[4] Patricia Toth, Penny Klein , NIST Special Publication 800-16 Revision 1 (3rd Draft), “ A Role-Based Model for Federal Information Technology/ Cybersecurity Training”, March 2014.

[5] Global Learning Systems, “Investing in Security Awareness Training: A complete guide to Security” [Online] Available: http://www.globallearningsystems.com/security-awareness-training-guide

[6] Pierluigi Paganini, “Why humans could be the weakest link in cyber security chain?” [Online] Available: http://securityaffairs.co/wordpress/9076/social-networks/why-humans-could-be-the-weakest-link-in-cyber-security-chain.html

[7] Manny Salvacion,” CAC Promotes Cyber-Security Awareness of China's Youth” [Online] Available: http://en.yibada.com/articles/36469/20150604/cac-cyber-security-awareness-chinas-youth.html, June 2004

[8] Ludwig Slusky, Parviz Partow-Navid, “Students Information Security Practices and Awareness”, Journal of Information security and Privacy, Volume 8, 2012

[9] [Online] Available: http://tribune.com.pk/story/718865/cyber-crime-fia-arrests-alleged-facebook-blackmailer/

[10] Cisco, “Protect Against Social Engineering” [Online] Available: http://www.cisco.com/c/en/us/about/security-center/protect-against-social-engineering.html

[11] Homeland Security, “National Cyber Security Awareness Month” [Online] Available: https://www.dhs.gov/national-cyber-security-awareness-month

[12] Australian Communications and Media Authority, “An overview of international cyber-security awareness raising and educational initiatives”, Research report commissioned by the Australian Communications and Media Authority, May 2011

[13] Action Fraud, National Fraud and Cyber crime reporting centre, [Online] Available: http://www.actionfraud.police.uk/fraud_protection/identity_fraud

[14] [Online] Available: http://www.identitytheft.org.uk/

[15] Dr. Michael Busch, "EU Safer Internet programme – current developments and policy update", September 2009 [Online] Available: http://www.saferinternet.pl/images/stories/michael_busch_29-30.09.2009.pdf

[16] Centre for cyber safety and education, ISC2 [Online] Available: https://www.isc2cares.org/safe-and-secure/

[17] [Online] Available: http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf

[18] Australian Communications and Media Authority, "An overview of international cyber-security awareness raising and educational initiatives", Research report commissioned by the Australian Communications and Media Authority, May 2011

[19] [Online] Available: https://securingthehuman.sans.org/security-awareness-training/enduser/

[20] [Online] Available: https://twitter.com/watchyourweb?lang=en

[21] Patricia Toth, Penny Klein , NIST Special Publication 800-16 Revision 1 (3rd Draft), " A Role-Based Model for Federal Information Technology/ Cybersecurity Training", March 2014.

[22] Ludwig Slusky, Parviz Partow-Navid, "Students Information Security Practices and Awareness", Journal of Information security and Privacy, Volume 8, 2012

[23] Michael Portnoy, Seymour Goodman, "Global Initiatives to Secure Cyberspace: An Emerging Landscape", Advances in Information Security, 2008

[24] Patricia Toth, Penny Klein , NIST Special Publication 800-16 Revision 1 (3rd Draft), " A Role-Based Model for Federal Information Technology/ Cybersecurity Training", March 2014.

[25] Dr. Jane LeClair, Dr. Sherly Abraham, Dr. Lifang Shih, "An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce", Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference, October 2013

[26] Noluxolo Kortjan, Rossouw von Solms, "A conceptual framework for cyber-security awareness and education in SA" [Online] Available: https://pdfs.semanticscholar.org/9ea6/28ec868e9c3347b0ff93cf61e5453e74ada0.pdf

[27] Saeed S. Basamh, Hani A. Qudaih, Jamaludin Bin Ibrahim, “An Overview on Cyber Security Awareness in Muslim Countries”, International Journal of Information and Communication Technology Research, Volume 4 No. 1, January 2014

[28] John Malgeri, “Cyber Security: A National Effort to Improve”, Information Security Curriculum Development Conference, 2009

[29] Harpal Dhillon, Mariana Hentea, “Getting a Cybersecurity Program Started on Low Budget”, Proceedings of the 43rd annual Southeast regional conference - Volume 1, March 2005

[30] SANS Institute InfoSec Reading Room, “The Importance of Security Awareness Training” [Online] Available: https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

[31] B. Ngoqo, S.V. Flowerday, “Linking Student Information Security Awareness and Behavioural Intent” Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)

[32] Hamza Amor, “Training general users on the non-policy side of the IS Program”, InfoSecCD '10 2010 Information Security Curriculum Development Conference, October 2010

[33] SANS Institute
InfoSec Reading Room, “Developing an Integrated Security Training,
Awareness, and Education Program”, [Online] Available: https://www.sans.org/reading-room/whitepapers/awareness/developing-integrated-security-training-awareness-education-program-1160

[34] National Initiative for Cyber security and Education (NICE), “The National Cybee security workforce framework” [Online] Available: http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf

[35] NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”, April 2013

[36] S. L. Pfleeger, C. Irvine and M. Kwon, "Guest Editors' Introduction," in *IEEE Security & Privacy*, vol. 10, no. 2, pp. 19-23, March-April 2012.

[37] [Online] Available: http://securingthehuman.sans.org/

[38] [Online] Available: http://www.fia.gov.pk/en/NR3C.php

[39] [Online] Available: https://www.isea-pmu.in/home/About

[40] Andrea Cullen, Lorna Armitage, “The social engineering attack spiral”, 2016 Internal Conference on Cyber Security and Protection of Digital Services, June 2016

[41] Ashley A. Cain, David Schuster, “Applying measurement to complementary situation awareness”, 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), March 2016

[42] Gary M. Deckard, L. Jean Camp, “Measuring Efficacy of a classroom training week for a cybersecurity training exercise”, 2016 IEEE Symposium on Technologies for Homeland Security (HST), May 2016.

[43] Ibrahim Ghafir, Vaclav Prenosil, “Social Engineering Attack Strategies and Defense Approaches”, 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCLoud), August 2016

[44] Ileen E. Van Vuuren, Elmarie Kritzinger, “Identifying gaps in IT retail Information Secuirty policy implementation processes”, 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), Nov 2015

[45] Robert D. Campbell, Elizabeth K. Hawthorne, Karl J. Klee, “The role of two-year colleges in educating the cyber-security workforce”, ACM SIGCSE Bulletin – Proceedings of the 8th annual conference on Innovation and Technology in computer science education, Spetember 2013.

[46] Cuong Pham, Dat Tang, Razvan Beuran, “CyRIS: A cyber range instantiation system for security training”, SoICT Proceedings of the Seventh Symposium on Information and Communication Technology, December 2016

[47] Edwin D. Frauentein, Rossouw von Solms, “Combatting phishing: A holistic human approach”, 2014 Information Security for South Africa, November 2014

[48] P.G. Schrader and Kimberly A. Lawless, “The knowledge, attitudes and behaviors approach”, Performance Improvement, v43 n9 p8-15