Assessment of cyber security awareness of ICT employees in India

Deepthy Prasad

Abstract

Due to the increase of cyber attacks around the world, ‘Cyber security is a fast-evolving topic nowadays. The research studies are more interested in discussing the impact of employees in maintaining the cyber security of an organization than the role of technological advancements. This quantitative research study aims to assess the cyber security awareness of Information and Communication Technology (ICT) employees. The scope of this research is Indian Information and Communication Technology (ICT) employees working in IT departments of large organizations. The sampling data is collected through a questionnaire using a combination of convenient and snowball non-random sampling methods. A python code is created to analyse the collected data and various correlation tests such as spearman’s correlation and crosstabulations are conducted. The data analysis was based on a conceptual model created for the study using protective motivation theory (PMT) theory. The threat appraisal and coping appraisal are measured based on various influencing factors to conclude. The findings shave shown good security awareness among Indian Information and Communication Technology (ICT) employees of Information Technology (IT) departments of large organizations. The study has also shown a strong impact of the organization’s Information Security Policies (ISP) and awareness program on the cyber security awareness of their employees.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ICT	:	Information and Communication Technology
IT	:	Information Technology
PMT	:	Protective Motivation Theory
ISP	:	Information Security Policy
AI	:	Artificial Intelligence
CSV	:	Comma Separated Values

1 Introduction

1.1 Background

'Cyber Security' is one of the most discussed research topics of the modern digital world. The introduction of the Internet made drastic changes in human life and soon it became an indispensable part of our day-to-day life. A large amount of data becomes accessible through the internet from anywhere anytime. But the security of sensitive data over the internet has become a major problem. 'Cyber security' refers to 'the practise of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security' (kaspersky, n.d.). As per a recent study (Cyber Crime 2020, n.d.) '*Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025*.' The main area of this research study is cybersecurity.

Nowadays most organizations are aware of the importance of cyber security, as a security breach can lead to the destruction of the organization's reputation, business performance issues, and intellectual property loss (Torten, Reaiche, & Boyle, 2018). The cyber security of an organization is maintained through both technical and human support. The research studies always describe the human factor as the weakest link in information security and also states that the attackers are more interested to exploit human vulnerabilities ((Boss, Kirsch, Angermeier, Shingler, & Boss, 2017), (Nifakos, et al., 2021), (Joinson & van Steen, 2018), (Torten, Reaiche, & Boyle, 2018), (Ergen, Ünal, & Saygili, 2021)). Most of the employees working in ICT (ICTemployment) might have access to the organization's internal network. The hackers are more interested in hacking the employees' credentials to get access to authorized data. The research (Torten, Reaiche, & Boyle, 2018) discusses the impact of security awareness in IT professionals' behavior. These study results show us the importance of security awareness in employees. The present research study is an investigation to assess the cyber security awareness of Indian ICT employees working in different organizations.

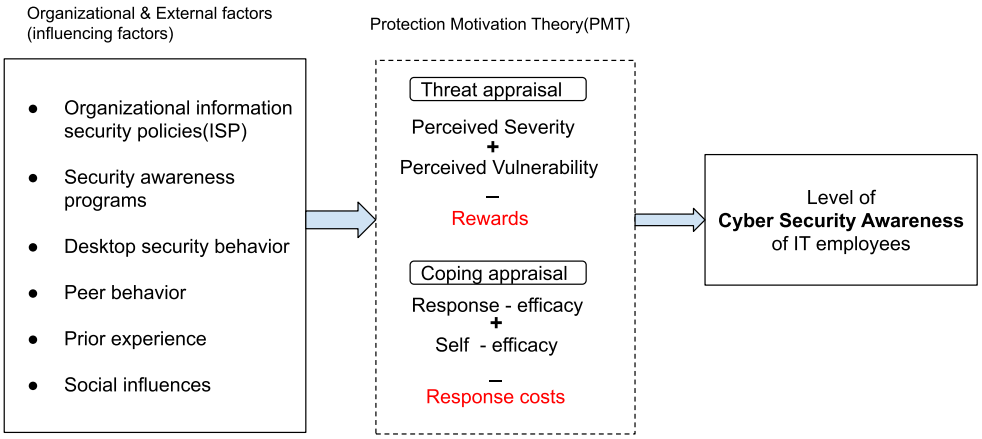


Fig. 1 Conceptual model

This research study is based on the Protection Motivation Theory (PMT) applied to information security. The PMT was first developed by R.W. Rogers in 1975 and then later in 1983, he expanded the theory to a more general theory of persuasive communication. According to Ruth Shillair (Shillair, 2020) the PMT is '*a widely-used framework to understand responses to triggers that appraise individuals of a potential threat*'. Here, the potential threat is cyber-attacks, and the triggers are the countermeasure to prevent it. This study explores the way employees respond to these cyber-attacks and find out a quantitative measure of their cyber security awareness. A conceptual model (Fig. 1) is created for our research study based on some qualitative research literature results ((Li & He, 2019), (Torten, Reaiche, & Boyle, 2018), (kadir, İbrahim, & Göksel, 2017)) and the PMT theory.

The conceptual model Fig. 1 shows how the level of cyber security awareness can be measured from the various influencing factors based on Protection Motivation Theory. The model has 2 major parts 'Organizational & External factors (influencing factors)' and 'Protection Motivation Theory (PMT)'. Part-1 includes the factors influencing the cyber security behaviour of an employee and part-2 includes the employee's perceived security threats and their efficacy in dealing with them.

Part-2 is constructed from PMT theory concepts 'threat appraisal' and the 'coping appraisal' based on which people protect themselves from a cyber attack. The threat appraisal is the combination of severity and vulnerability of information security threats subtracted by the rewards which refer to the positive aspects of continuing in the information security threats (Fig. 1). The coping appraisal defines the coping ability of a person; hence it is the sum of both response efficacy and self-efficacy subtracted by the response cost which is any type of cost required to achieve the recommended preventive responses Fig. 1.

Part-1 is constructed based on the main organizational(internal) and external factors affecting a user's intentions to comply with the cyber security policies which are identified from some previously published literature. The various identified information security compliance behaviour factors were Peer behaviour, Prior experience, Social influences (Li & He, 2019), Cyber security awareness programs, Organizational security policies (kadir, İbrahim, & Göksel, 2017), and Desktop security behaviour (Torten, Reaiche, & Boyle, 2018). The study of influencing factors helps in measuring the threat appraisal and coping appraisal and this paves the path to determine the level of cyber security awareness of employees.

1.2 Research problem

The technology advancements like cloud computing, artificial intelligence (AI), etc. brought major developments in all organizations and it enhanced an organization's productivity and reputation. At the same time, cybersecurity has become a challenging task for them as the hackers also started to make use of advanced techniques for cyber attacks. According to a 2020 Data Breach Investigations Report (Verizon.com, n.d.), the most common cause of data breach globally is social phishing which is evidence for the statement 'threat actors shift their focus towards exploiting human vulnerabilities' (Joinson & van Steen, 2018).

One of the major targeted groups for a cyber attack in an organization might be the employees with rights and privileges to access secure and sensitive data regarding the organizations and their customers. Therefore, the security behavior of such employees should be given more importance while

investigating the cyber security awareness of employees. Hence the present research study is to measure the cyber security awareness of the employees working in software development and maintenance for an organization. This study might help the organizations to understand the efficacy of their current security measures. This study may also provide a way to measure employees' self-efficacy in the cyber security area. This study can indirectly provide cyber security awareness to the small population of the employees among whom the research will be carried out.

The research paper by (Li & He, 2019) discusses the impact of cyber security policy awareness on employees' cyber security behavior. The research study (Torten, Reaiche, & Boyle, 2018) provides the quantitative study results of the relationship between cyber security awareness and desktop security behaviour of IT professionals in the US. However, this study focuses only on one factor discussed in our conceptual model which is security awareness programs. So the current study is an expanded version of this. Another research paper by (Ergen, Ünal, & Saygili, 2021) in which the qualitative study of cyber security in all types of organizations is discussed and which also describes the barriers and promoters in changing the behaviour of employees to ensure cyber security of the organization. This paper also suggests a future quantitative study of the cyber security awareness among employees because it includes a statement in future studies as follows: "*Future studies could explore how employees feel and think about cyber security risks and precautions. There is still a need for quantitative studies to support the findings of this study. This study used qualitative method, so the findings may have omitted factors that a quantitative method would have uncovered*.". So, our research study is a continuation of this research paper. Our research is to do a quantitative study to assess the cyber security awareness among ICT employees by considering this population's importance in maintaining cyber security.

1.3 Aim and research question

Most of the organizations regardless of the area of business (health, finance, education, transport, entertainment, etc) have started to make use of the technical advancements to improve cybersecurity and also provide training to employees to improve their cyber security awareness. This research aims to assess the level of cyber security awareness of Indian ICT employees in various organizations. This study can help find the role of each external and the internal influencing factor mentioned in the conceptual model Fig. 1 in assuring the cyber security of an organization.

The research question investigated in this study is:

- What is the level of cyber security awareness among Indian ICT employees in various organizations?

This question is investigated by measuring the below factors:
The level of self-efficacy in responding to cyber attacks, the previous experience in cyberattacks, and the level of peer behaviour, organization's impact, and social influences in cyber security awareness.

1.4 Delimitations of the study

The theoretical population of this research study is ICT employees. They are software developers/engineers, user support specialists and systems analysts, etc employees who are more likely to use an organizations' intranet and sensitive information compared to other employees. As per the statistics from Statista (Sava, n.d.), '*The worldwide full-time employment in the ICT sector is projected to reach 55.3 million in 2020 (pre-corona estimation)*'. Considering this statistic, the study population of the research is delimited to a small group of people who are working in the IT department of organizations. The scope is again delimited demographically to India as it is convenient for the researcher to reach this population and complete the study in a short period.

There are many influencing factors in Cyber Security to be measured to assess the awareness. The scope of the study is also delimited to only a few external and internal influencing factors such as Peer behaviour, Prior experience, Social influences, Cyber security awareness programs, Organizational security policies, Desktop security behaviour. The conceptual model Fig. 1 created reflects this delimitation in the scope of the study. The main two parts of the PMT theory threat appraisal and a coping appraisal are measured only depending on these factors.

2 Research Method

2.1 Research strategy

The current research study aims to assess the level of cyber security awareness of Indian IT employees. A research strategy should be selected to assess the level of cyber security awareness among employees by the conceptual model. There are several research strategies available for a quantitative study. The most suitable 3 strategies identified are Experiment, Case study and Survey. A comparison study of these strategies is carried out and the results are discussed in the next paragraphs.

An experimental research strategy is one where different hypotheses can be created based on the PMT variables and then these hypotheses are tested to determine the level of cyber security awareness. This strategy can provide a cause-effect relationship of the threat perception and response perception with the information security protection behaviour. Time is a critical factor for this strategy because it needs plenty of time to define hypotheses and test each one of them on a group of people. The selection of hypotheses is crucial as the results of this strategy depend on the variable control and sometimes it can lead to some ethical and practical problems like privacy and confidentiality issues, conflicts of interests etc. As this strategy is a time-consuming method, it may not be suitable for short-term research.

A case study is another research strategy used that investigates a phenomenon within a real-life context. Charles Schell says that 'despite the popular misconception that case studies are limited to the qualitative analysis they can use both qualitative and/or quantitative information.' (Shell, 1992). The case study can produce accurate measures of both coping appraisal and threat appraisal. But to use this strategy either a sample cyber-attack phenomenon needs to be created to assess the responses of the selected population or a population who experienced a cyber attack before needs to be selected for investigation. But the selection of a proper population and the implementation of multiple data collection methods are time-consuming tasks. This research strategy cannot be chosen as the research period is very short and the selection of population is a critical element.

The research strategy 'Survey' where the research question is solved from the information collected from a sample of individuals through the responses to several questions. The main advantage of the survey method is that it allows us to collect a large amount of data within a short period. The main challenge here is to create valid survey questions which help to assess the threat and coping appraisal of IT employees on cyber security. The results from this strategy depend on the quality of survey questions and the population on which the survey is executed. Remote collection of data is another advantage of this research method.

The case study can produce in-depth data on the research problem whereas the survey can produce a very large sample of numerical data which is very useful in the case of a quantitative survey. Both Case study and survey methods are suitable to avoid the ethical issues encountered in experimental strategy because the questions to respondents can be framed in such a way that their confidentiality and anonymity can be protected and only voluntary participation also can be ensured. Among all of these 3 methods discussed, the 'Survey' research strategy is considered to be perfect for our study because it supports quantitative research in a short period.

2.2 Data Collection Method

As per the conceptual model Fig. 1, the best way to measure the cyber security level of the employees will be to determine the quantitative measure of factors in threat appraisal and coping appraisal of PMT. Interview, Observation, and Questionnaires are widely used data collection methods for a research study.

The interview can be used to collect data from employees where we should use structured or semi-structured ways to get answers to specific questions based on PMT. One-to-one interviews are customizable and can assure the response to all questions, but it is one of the expensive and time-consuming data collection methods.

Observation is another data collection method where no questions are asked to the respondents instead the data is collected by observing the study population. But only coping appraisal of PMT can be measured through this method. To measure the perceived severity and vulnerability of each IT employee, some questions need to be asked and individual responses are essential. Hence the observation might not be a good way for data collection for this current research even though it supports the quantitative study data collection.

The questionnaire is like a structured interview. The questionnaire with closed-end questions is suitable to collect ordinal data for a quantitative study which can be used for further mathematical and statistical analysis. Hence the illustration of study results in the form of graphs and charts is easier. The closed-end questions can maintain uniformity in answers and ensure minimum bias from the researcher during the data collection process. The online questionnaire is more effective for a short-term quantitative study compared to others such as face-to-face, via post, phone calls, etc. Sometimes online questionnaires can provide more genuine answers because the respondents can have enough time to think compared to interviews. A large population including respondents from distant areas can be covered using this data collection method in a shorter period. Also, the questionnaire method is cheaper and less time-consuming compared to interviews. These advantages of the questionnaire make it a suitable option for our present study.

Abdulaziz Alzubaidi (Alzubaidi, 2021) conducted a similar quantitative study to measure the level of cyber security awareness for cybercrime in Saudi Arabia and the main data collection method used was a questionnaire. He was able to prove that cyber security awareness plays a major role in controlling cyber crimes and he illustrated the result in the form of charts and graphs. So this is an inspirational research result using a questionnaire data collection method which I prefer to use in my current study.

2.3 Data Collection Strategy

The present research study is to assess the cyber security awareness only in ICT employees. The delimited population for this study is Indian ICT employees working in the IT department of organizations. The probability sampling methods are always better for a quantitative study. But there are many limitations in accessing the population via a probability sampling method as it is more time consuming, complex and usually more costly. So that a combination of a few nonprobability sampling methods needs to be used to reach the study population.

A combination of Convenience sampling, Voluntary response sampling, and Snowball sampling methods are used for the survey as they are an easy way to reach the intended population. The

combination of 3 sampling methods is chosen to reach the maximum study population. The researcher knows some people from different parts of the world working in the IT industry and the data can be collected from them. Also, snowball sampling methods can be achieved through the help of known people where the known participants of the survey help the researcher to reach some unknown participants. Then voluntary response sampling is an easy method to collect data in the modern world as there are many social networks available now like LinkedIn, Twitter, Instagram, etc. The link to the questionnaire can be posted on these networks and collect data.

The chances of bias are more in non-probability sampling methods compared to probability sampling methods. Because the non-probability sampling does not ensure minimum accuracy and an equal chance of selection of members in the sampling population. Two ways of reducing this effect are to choose the population wisely and include some preliminary questions in the questionnaire to check the background of the person to be examined. But the chance of fault data Snowball method is a challenge. This can be avoided to an extent if the questionnaire link is posted only on IT professionals' private groups on social media so that none of the general people can access them.

2.4 Data Analysis Method

This is a quantitative study through which the cyber security awareness of IT employees is assessed according to the two main aspects (threat appraisal and coping appraisal) of PMT. The questionnaire is created with only closed-end questions with single-select and multi-select categorical options so that ordinal data can be collected from the study population according to the various influencing factors explained in the conceptual model Fig. 1. The categorical values will help in the fast analysis of data.

The data is collected from Indian ICT employees working in different organizations in the world. Both inferential and predictive data analysis is rejected as our sample is collected using non-random procedures and are not large enough to draw generalized and predicted results. Descriptive and exploratory data analysis are the best suitable way to answer our research question to assess cyber security awareness. Both descriptive and exploratory data analysis can provide an insight of the collected data numerically and visually which are suitable to draw some conclusions on the cyber security awareness of the sample population. 4 major steps are included in data analysis: Visualization of demographic data, Descriptive summary tables, Exploratory analysis based on the conceptual model, Correlation test using Cross tabulation and Spearman's correlation.

Python is the chosen data analysis tool as it is a popular analysis tool among data scientists (Stančin & Jović, 2019). There are many free Python libraries available now for data analysis and visualization such as pandas, matplotlib, altir, sklearn. As a data scientist, the pre-processing of collected data and analysis of the same can be implemented using various machine learning techniques in python. Visual Studio IDE is a widely used software platform to execute python code and it is used in our current study to do the statistical analysis and visualization of the collected data. Various pie charts, bar charts, heatmaps, and scatter plots can be used to visualize the survey results as part of exploratory analysis. Then some summary tables with mean, standard deviation, minimum, maximum, etc. can be created as part of descriptive analysis. Crosstab() and spearmanr() are python libraries used for cross-tabulation and spearman's correlation tests respectively. These can be used to determine the study population's coping and threat appraisal according to PMT theory. Abdulaziz (Alzubaidi, 2021) has used a code in R language (which is very similar to Python language) to complete a similar quantitative study and that is the basic reference for our data analysis.

2.5 Research Ethics

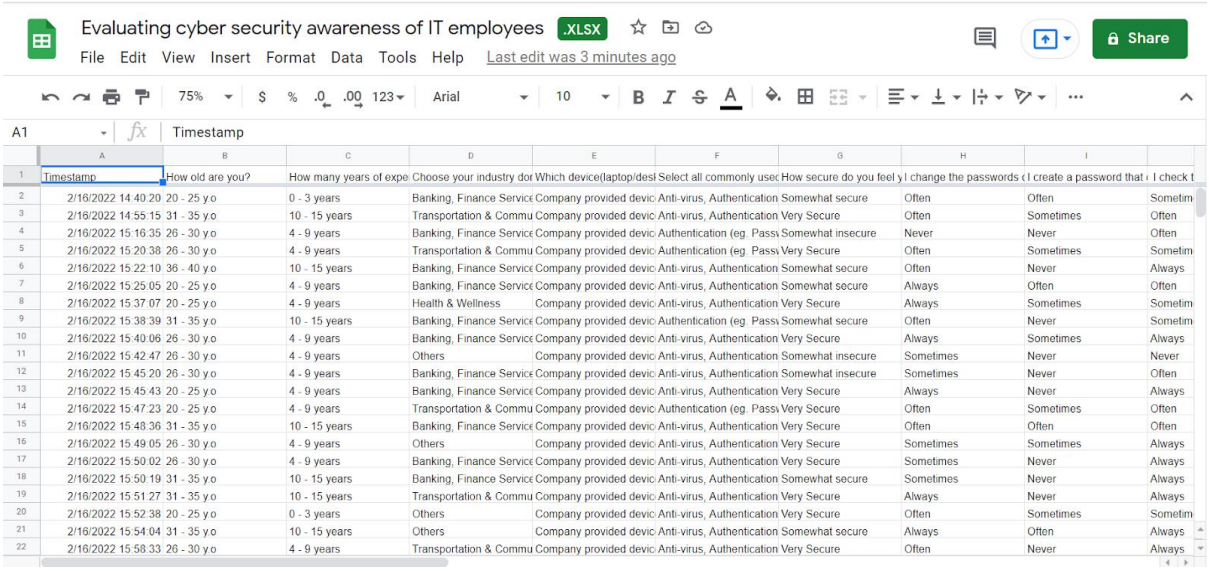
To protect the confidentiality of the person participating in the survey of the research study, no personal information and contact details (including name, telephone number, e-mail, postal addresses, credentials of any kind, and IP address) are asked in the questionnaire or disclosed to the researcher. The anonymity of the responders to this survey is protected by its design. The participants are allowed to submit the answers only one time. The questionnaire is created using Google forms and the link to the questionnaire is sent to all known participants via social media such as Instagram, LinkedIn, WhatsApp etc. In no way can the data provided be linked with any of the participant's personal data. Hence no way to distinguish the answers according to the respondents. The voluntary participation by the responder is ensured by providing a consent form to each respondent regarding the policy of the survey. The research ethics followed in this questionnaire are in adhering to the principles outlined in (Denscombe, 2010).

3 Results

3.1 Data Collection and Analysis

A questionnaire based on Google forms is used for the data collection. The form has been sent to 80 people (Indian ICT employees) known to the researcher via e-mail, WhatsApp messenger and LinkedIn and mentioned in the message to share the form with their known people (snowball sampling) to ensure adequate participation. Avoided posting the form on social media platforms to ensure the validity of the participants. The data is collected through 7 days. There were 24 multiple choice questions in the questionnaire. A total of 117 responses are received and all are valid as per the data analysis report.

The responses of the questionnaire are automatically stored to a google form as shown below:



Timestamp	How old are you?	How many years of expe	Choose your industry dor	Which device(laptop/desl	Select all commonly usec	How secure do you feel y	I change the passwords (	I create a password that (	I check t
2/16/2022 14:40:20	20 - 25 y.o	0 - 3 years	Banking, Finance Service	Company provided devic	Anti-virus, Authentication	Somewhat secure	Often	Often	Sometim
2/16/2022 14:55:15	31 - 35 y.o	10 - 15 years	Transportation & Commu	Company provided devic	Anti-virus, Authentication	Very Secure	Often	Sometimes	Often
2/16/2022 15:16:35	26 - 30 y.o	4 - 9 years	Banking, Finance Service	Company provided devic	Authentication (eg. Passv	Somewhat insecure	Never	Never	Often
2/16/2022 15:20:38	26 - 30 y.o	4 - 9 years	Transportation & Commu	Company provided devic	Authentication (eg. Passv	Very Secure	Often	Sometimes	Sometim
2/16/2022 15:22:10	36 - 40 y.o	10 - 15 years	Banking, Finance Service	Company provided devic	Anti-virus, Authentication	Somewhat secure	Often	Never	Always
2/16/2022 15:25:05	20 - 25 y.o	4 - 9 years	Banking, Finance Service	Company provided devic	Anti-virus, Authentication	Somewhat secure	Always	Often	Often
2/16/2022 15:37:07	20 - 25 y.o	4 - 9 years	Health & Wellness	Company provided devic	Anti-virus, Authentication	Very Secure	Always	Sometimes	Sometim
2/16/2022 15:38:39	31 - 35 y.o	10 - 15 years	Banking, Finance Service	Company provided devic	Authentication (eg. Passv	Somewhat secure	Often	Never	Sometim
2/16/2022 15:40:06	26 - 30 y.o	4 - 9 years	Banking, Finance Service	Company provided devic	Anti-virus, Authentication	Very Secure	Always	Sometimes	Always
2/16/2022 15:42:47	26 - 30 y.o	4 - 9 years	Others	Company provided devic	Anti-virus, Authentication	Somewhat insecure	Sometimes	Never	Never
2/16/2022 15:45:20	26 - 30 y.o	4 - 9 years	Banking, Finance Service	Company provided devic	Anti-virus, Authentication	Somewhat insecure	Sometimes	Never	Often
2/16/2022 15:45:43	20 - 25 y.o	4 - 9 years	Banking, Finance Service	Company provided devic	Anti-virus, Authentication	Very Secure	Always	Never	Always
2/16/2022 15:47:23	20 - 25 y.o	4 - 9 years	Transportation & Commu	Company provided devic	Authentication (eg. Passv	Very Secure	Often	Sometimes	Often
2/16/2022 15:48:36	31 - 35 y.o	10 - 15 years	Banking, Finance Service	Company provided devic	Anti-virus, Authentication	Very Secure	Often	Often	Often
2/16/2022 15:49:05	26 - 30 y.o	4 - 9 years	Others	Company provided devic	Anti-virus, Authentication	Very Secure	Sometimes	Sometimes	Always
2/16/2022 15:50:02	26 - 30 y.o	4 - 9 years	Banking, Finance Service	Company provided devic	Anti-virus, Authentication	Very Secure	Sometimes	Never	Always
2/16/2022 15:50:19	31 - 35 y.o	10 - 15 years	Banking, Finance Service	Company provided devic	Anti-virus, Authentication	Somewhat secure	Sometimes	Never	Always
2/16/2022 15:51:27	31 - 35 y.o	10 - 15 years	Transportation & Commu	Company provided devic	Anti-virus, Authentication	Very Secure	Always	Never	Always
2/16/2022 15:52:38	20 - 25 y.o	0 - 3 years	Others	Company provided devic	Anti-virus, Authentication	Very Secure	Often	Sometimes	Sometim
2/16/2022 15:54:04	31 - 35 y.o	10 - 15 years	Others	Company provided devic	Anti-virus, Authentication	Somewhat secure	Always	Often	Always
2/16/2022 15:58:33	26 - 30 y.o	4 - 9 years	Transportation & Commu	Company provided devic	Anti-virus, Authentication	Very Secure	Often	Never	Always

Fig. 2 Data collected via Questionnaire

This google form is downloaded to a local CSV file for further analysis of data using Python programming language.

The main software used for the analysis is Visual Studio Code which is a source-code editor created by Microsoft for Windows, macOS, and Linux (VisualStudio, n.d.). A Jupyter notebook with python code for data analysis is created and run on this Visual studio platform to capture the results. The below image shows the Visual Studio Code platform and the jupyter notebook with data analysis python code.

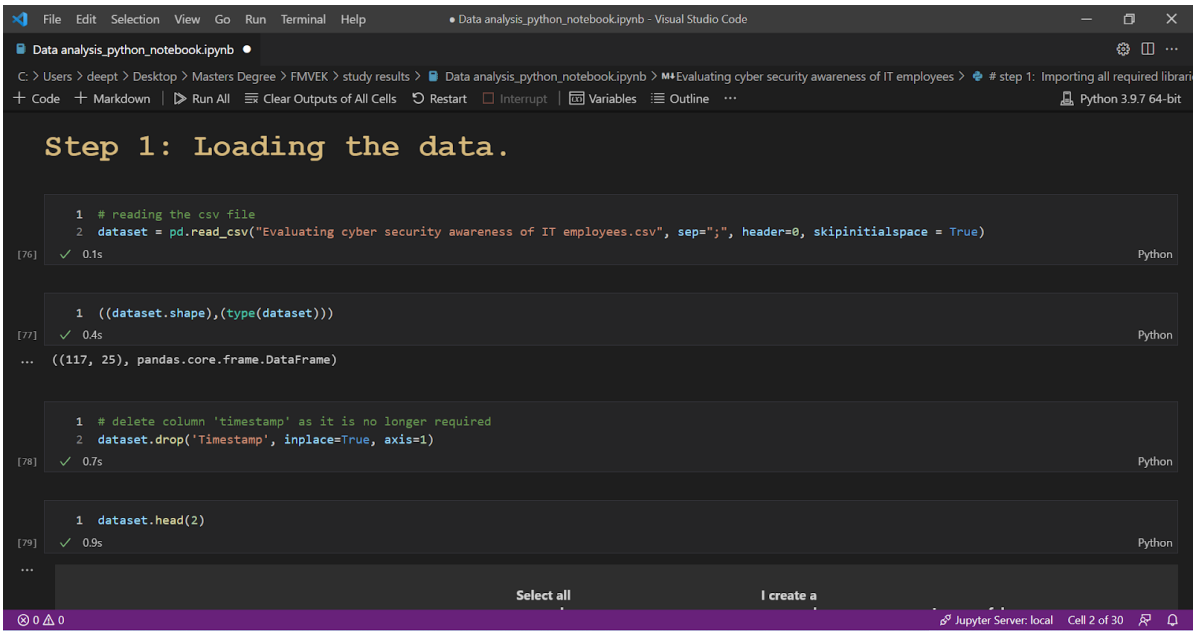


Fig. 3 Jupyter Notebook with Python code

The data analysis is done in 4 different steps and is described below:

1. Loading the data:
   The CSV file downloaded from google forms is uploaded to a Jupyter Notebook using the 'read_csv' function from the 'pandas' library (Pandas library, n.d.).

2. Data Preprocessing:
   The data is modified in this step for further analysis. The modifications were to define the column names suitable to the questions in the survey and update the data type of columns to support mathematical analysis.

3. Data Imputation:
   The validity of the data is checked and only a few 'nan' (missing values) are found in the 24th column which is the answer to a follow-up question. These values are imputed with 'NA' to indicate that is 'Not Applicable' to the specific row.

4. Quantitative Analysis:
   Various pie charts, bar charts, heatmaps, and scatter plots are created in this step using matplotlib, seaborn, altair, etc to visualize the survey results as part of exploratory analysis. Then some summary tables with mean, standard deviation, minimum, maximum, etc are also created for the descriptive analysis. To determine the Threat appraisal and Coping appraisal as per PMT theory the Cross Tabulation and Spearman's correlation methods are used as most of our data is ordinal type. The crosstab() from pandas library (Pandas library, n.d.) and spearmanr() from SciPy (Scipy, n.d.) modules are used for these tests.

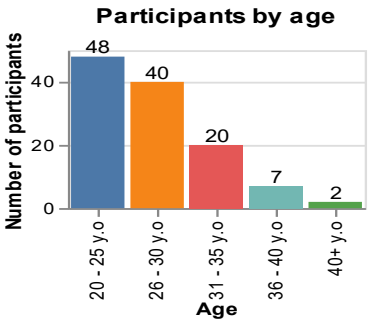
   This step is further divided into 4 sub-steps where the data analysis is completed by the conceptual model Fig. 1.
   a. Visualization of demographic data.
   b. Descriptive summary table.
   c. Exploratory analysis based on the conceptual model.
   d. Correlation test using Cross tabulation and Spearman's correlation.

3.2 Findings

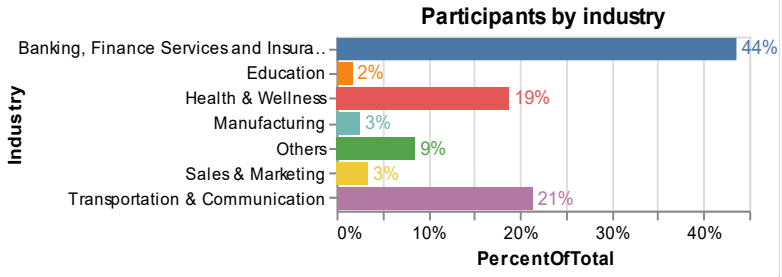
The questionnaire had 4 different sections to measure the influencing factors which are further used to find the threat appraisal and coping appraisal of the employee as mentioned in the conceptual model. The sections were Basic information, Cyber Security Activities, Cyberattack consciousness, and Security Breach Experiences. The findings from the 4 sub-steps in the quantitative analysis are described further.

1. Visualization of demographic data

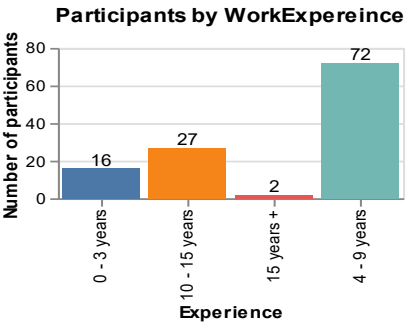
The visualization of data collected in the section 'Basic information' is used to show the demographic characteristics of the study group.



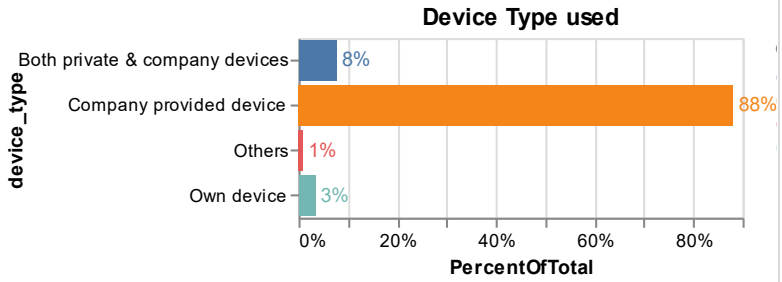
4. 1 No of Participants by Age



4. 2 Percentage of participants by industry



4. 3 No of Participants by Work experience



4. 4 Percentage of Device type used

Fig. 4 Demographic data visualization

92.3% of the study population is in the age group 20-35 and 61.5% of the population have 4 to 9 years of experience working in the IT industry for different organization domains. The 'participants by industry' chart show that 44% of the people in the study population are working in finance industries like Bank, Insurance, etc. The research was able to reach people working in 6 different industry

domains. 88% of the survey participants use the company-provided devices to work which is a key finding that there can be some inbuilt security tools because the company is concerned about its cyber security awareness (Fig.4).

2. Descriptive summary table

Fig. 5 shows the mean, standard deviation and variance of 13 questions with categorical outputs. The standard deviation shows 'the spread of each value from the mean and variance shows 'the average degree to which each point differs from the mean' (std-var, n.d.). In our sample data, the standard deviation is less than '1' for all questions except the 3rd question in the table and variance is also follow a similar fashion to standard deviation as it is the square of the standard deviation.

No	Questions	Mean	std	var
1	How secure do you feel your working devices are?	3.42735	0.746443	0.557177
2	I change the passwords of important accounts frequently.	2.12821	0.97855	0.95756
3	I create a password that contains my personal information (e.g. name, date of birth, nickname)	3.05128	1.04919	1.1008
4	I check the legitimacy of a website before accessing it	1.97436	0.969016	0.938992
5	I am careful about clicking on links in an email, pop-up screens, advertisements, or socialmedia posts.	1.53846	0.914806	0.83687
6	I manually lock my computer screen when I step away from it.	1.60684	0.918744	0.844091
7	I attend security awareness programs conducted by my organization	1.60684	0.918744	0.844091
8	I always follow the information security policies (ISP) of my organization.	1.60684	0.918744	0.844091
9	The IT employees have a major impact on an organization's cyber security.	3.73504	0.443209	0.196434
10	I believe the cyber security awareness of my colleagues/friends affects my cyber security awareness too.	3.4188	0.619222	0.383436
11	I am concerned that my working environment is not secure enough against cyber attacks.	1.94872	0.797044	0.635279
12	I feel my organization is good at providing cyber security awareness to employees.	3.75214	0.489651	0.239758
13	I am willing to accept increased Internet surveillance from my organization if it can enhance Internet security	3.52991	0.689486	0.475391

Fig. 5 Descriptive summary table

The mean value shows the average answer value observed for each question and the below table (Fig. 6) gives the categorical value corresponding to the numerical value of the 'Mean' column in Fig. 5.

No	Questions	Mean value
1	How secure do you feel your working devices are?	Somewhat secure
2	I change the passwords of important accounts frequently.	Often
3	I create a password that contains my personal information (e.g. name, date of birth, nickname)	Sometimes
4	I check the legitimacy of a website before accessing it	Often
5	I am careful about clicking on links in an email, pop-up screens, advertisements, or socialmedia posts.	Always
6	I manually lock my computer screen when I step away from it.	Often
7	I attend security awareness programs conducted by my organization	Often
8	I always follow the information security policies (ISP) of my organization.	Often
9	The IT employees have a major impact on an organization's cyber security.	Strongly Agree
10	I believe the cyber security awareness of my colleagues/friends affects my cyber security awareness too.	Agree Partially
11	I am concerned that my working environment is not secure enough against cyber attacks.	Disagree
12	I feel my organization is good at providing cyber security awareness to employees.	Agree Partially
13	I am willing to accept increased Internet surveillance from my organization if it can enhance Internet security	Agree Partially

Fig. 6 Mean values of the answers

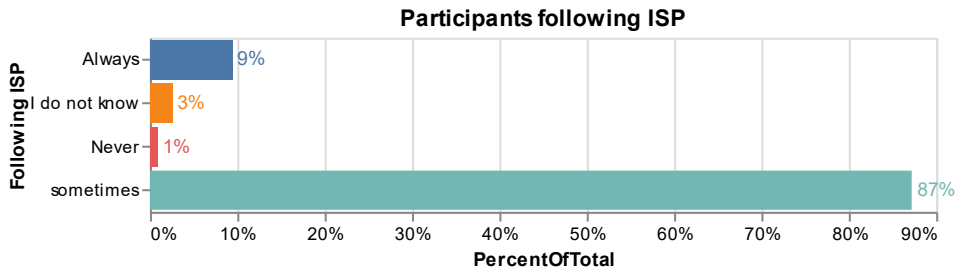
The answers to questions 2 to 8 reveal the security practices that are followed by the participants, and they are measured on a scale of 4 levels with options ('Always', 'Often', 'Sometimes', 'Never'). The coping appraisal of each participant towards cyber security can be assessed from these answers. The answers to questions 1 and questions 9 to 13 support the assessment of threat appraisal of each participant because those questions check whether they are concerned about cyber security. This is achieved by asking the participants how much they agree to certain statements regarding security concerns.

3. Exploratory analysis based on a conceptual model

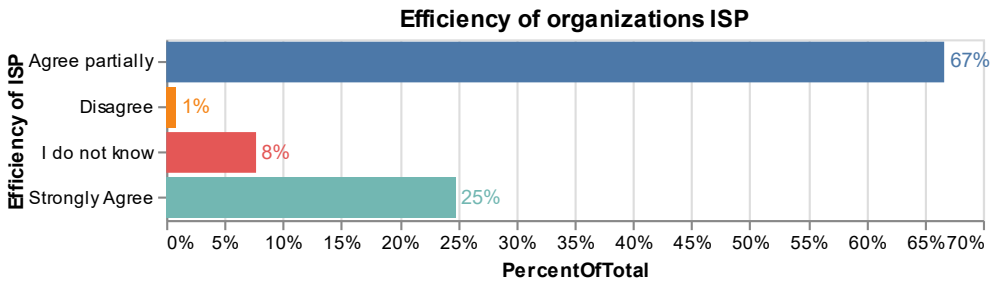
This section includes the exploratory analysis results of 7 influencing factors that are mentioned in the conceptual model (Fig. 1). The results of the influencing factors can support the assessment of cyber security awareness based on PMT theory. The analysis results are summarized into a table to assess the threat appraisal and coping appraisal of the sample population.

3a. Information Security Policy (ISP) of the organization.

Fig. 7 shows that 96% of participants are aware of their organization's ISP and follow them. Only 4% of participants are either not aware of it or not following them. Also, 91% of participants agree that the ISPs of the organization are effective against cyber attacks. Only 1% of the sample population shows disagreement with the statement 'the ISPs of the organization are effective in managing cybersecurity. But, 8% of the sample population is not aware of the effectiveness of an organization's ISP.



7. 1 Percentage of participants follows ISP



7. 2 Percentage of participants agrees current organization ISP's are effective

Fig. 7 Visualization of ISP of the organization

3b. Security awareness programs by the organization.

As per the diagram Fig. 8 Only 61% of the participants are always attending the security awareness programs conducted by their organization and the rest 29% includes the participants who are less likely or not attending them.

Only 20% strongly agrees that the awareness programs by the organization are effective and 78% agrees to the statement partially. Only 3 % says the awarness programs by the organization are not effective.

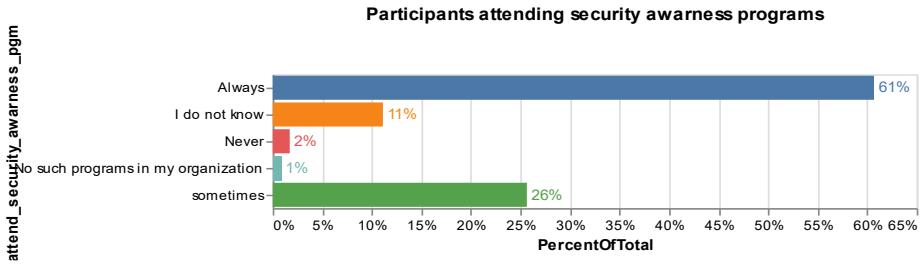


Fig. 8 Percentage of participants attending security awarness programs

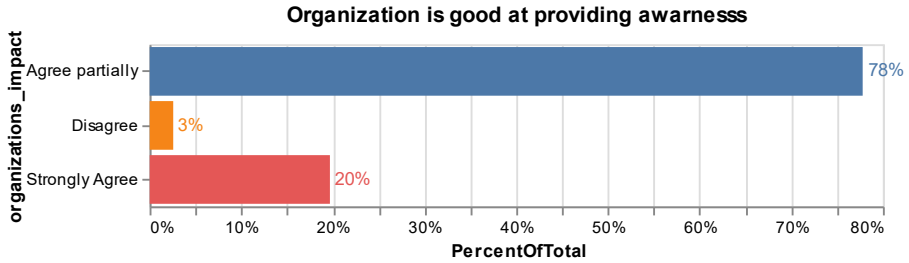


Fig. 9 Effectiveness of organization's awarness programs

3c. Desktop Security behaviour of the participant.

Fig. 10 shows the popular desktop security tools and the percentage of their use among the sample population. Authentication, Firewall, Anti-virus, Software updates and Encryption are the most popular desktop security behaviour in the study population.

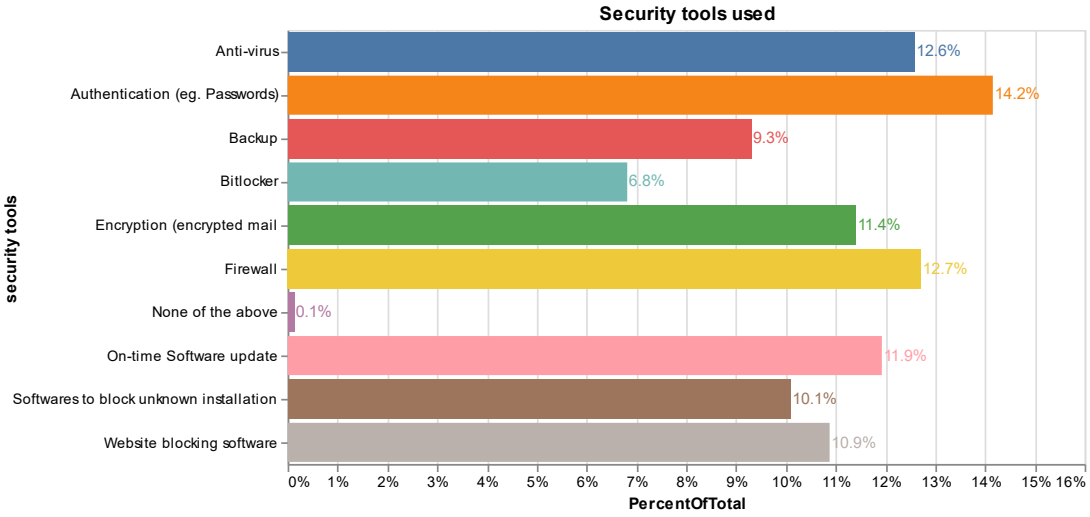
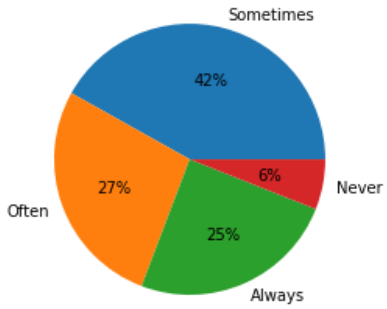
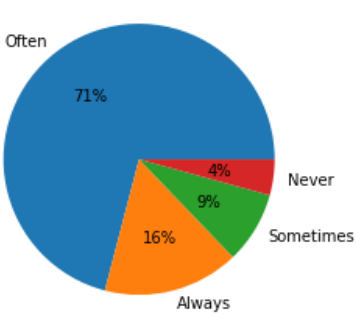


Fig. 10 Security tools used by participants

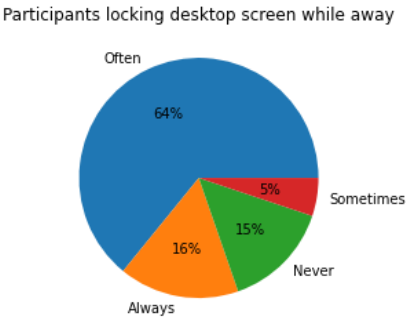
3 common desktop security practices are checked on the study population and the result in Fig. 11 shows that 52% (always or often) of the participants check the legitimacy of websites before accessing them and 6 % never checks it. 87%(always or often) of the participants are careful about clicking on links in an email, pop-up screens, advertisements on web pages, or social media posts whereas 4% never checks it. The third basic security practice checked is whether the participants are careful in locking the desktop screen while they are away and it shows that 80%(always or often) are following this practice and 15 % of participants never follows it.



11. 1 Participant checking the legitimacy of websites



11. 2 Participants click website links after checking the security



11. 3 Participants locks the working device's screen while away

Fig. 11 Visualization of few Desktop Security behaviors of the participants

3d. Influence of Peer behaviour

As per the visualization in Fig. 12, 95% (strongly agree or agree) of the study population believe that the cyber security awareness of colleagues or friends affects their cyber security awareness too. Only 5% (strongly disagree or disagree) of the study population disagree with this statement.

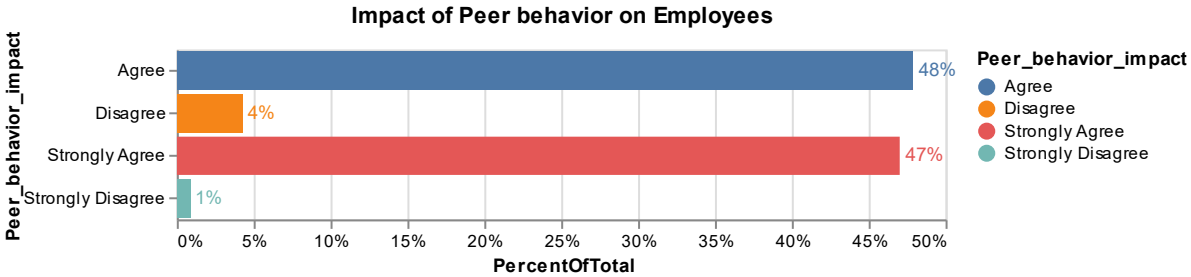


Fig. 12 Impact of peer behavior on Employees' cybersecurity awarness

3e. Prior experience in facing cyber-attacks

The visualizations (Fig. 13) on prior cyberattack experiences of participants shows that 59% of the study population is already faced some kind of cyber attack before whereas 37% never experienced a cyber attack before. A follow-up question regarding the action taken at the time of the cyberattack

shows that 51% of the participants who faced a cyberattack has reported it to an authorized authority. Only 5% has fixed the problem by themself. But 18% of these participants have either ignored it or not taken any actions as they are not aware of what to do in that situation.

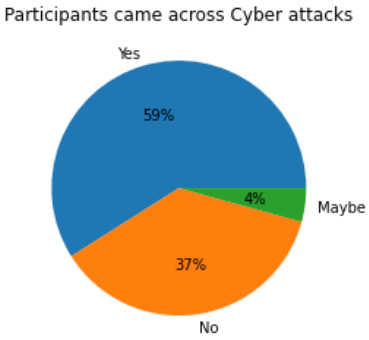


Fig. 13 Percentage of Participants who are victim of cyberattacks

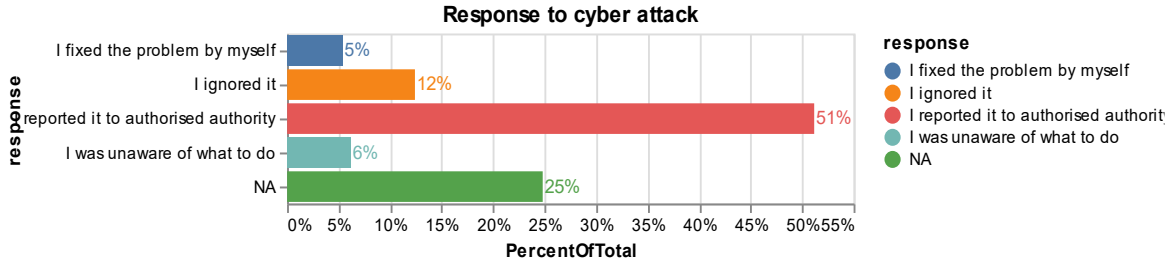


Fig. 14 Participant's response to a cyberattack

3f. Social Influences

Fig. 15 is the visualization of various resources used to enhance the cyber-security self-awareness by the sample population. Social media, e-mail and websites is the most commonly used resource and resources like news, posters and magazines are the least used ones. But 2.4% of the study population does not keep updated regarding cyber security.

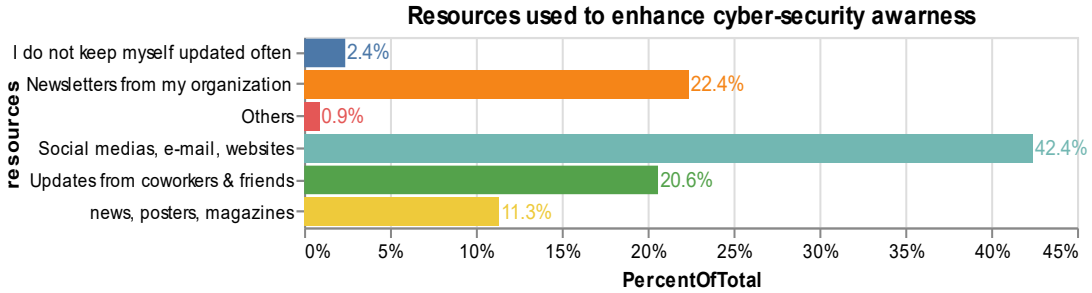


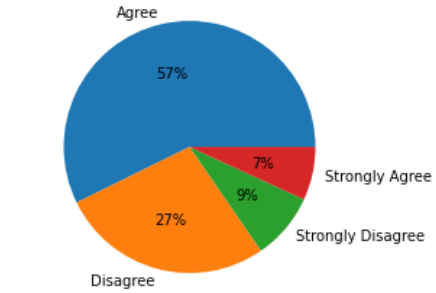
Fig. 15 Resources used by the participants to enhance cyber-security awareness

3g. Others

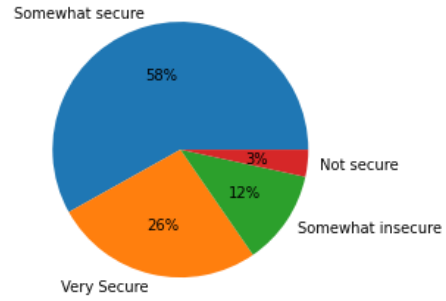
Findings from some general questions to check basic threat appraisal and coping appraisal of the participants.

- As per 16. 1 Workplace security, 64% of the study population believes that the workplace is secure against any kind of cyber-attacks and 36% of the population are concerned about workplace security as they do not agree with this statement.

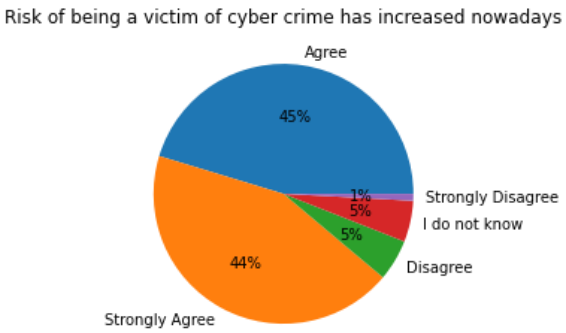
- As per 16. 2 Working device security Only 26% of participants say the working device is secure and 58% tells the device is partially secure. 15% of participants are very concerned as they tell the device is not secure against any cyber-attacks.
- As per 16. 3 Awareness of the risk of cyber security, 89% of the sample population aware that cybercrime has been increased nowadays whereas the rest 11% marked either disagreement with this statement or not aware of the current situation.



16. 1 Workplace security



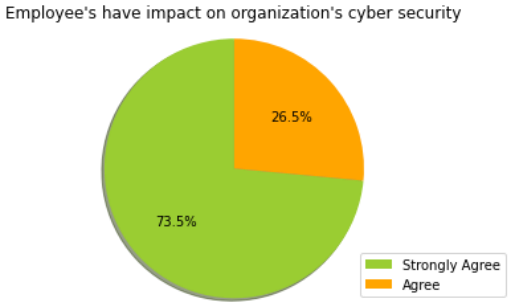
16. 2 Working device security



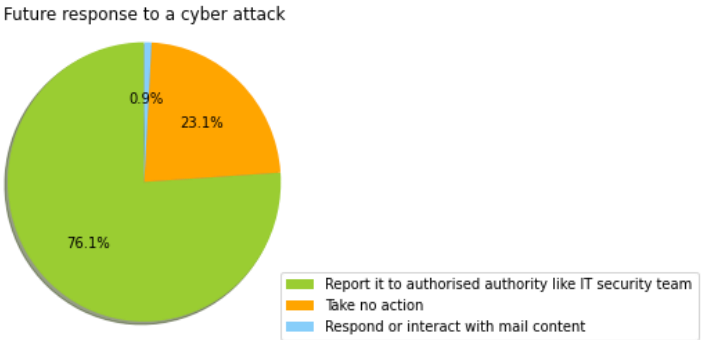
16. 3 Awareness of the risk of cyber security

Fig. 16 Perceived severity

- As per 17. 1 Employee have impact on cyber security 73.5% of participants agrees that the employees have a major impact on an organization's cyber security.
- As per 1 , 76.1% of the participants claims that if they are coming across any cyber attacks in future, they will report the same to an authorised authority. But 23.1% tell that they take no action.



17. 1 Employee have impact on cyber security



17.2 future response to a cyber attack

Fig. 17 Self efficacy

4. Correlation test using Cross tabulation and Spearman's correlation.

Most of our collection data are categorical, so spearman's correlation and cross tabulation are the most suitable correlation tests. Functions spearmanr() and crosstab() in python are used to do the tests. Another function linregress() is used to plot only perfect positive correlated columns. The code snippet of these tests is available in Fig. 188Fig. 18 python code to find spearman's correlation , Fig. 199 and Fig. 20.

```
# prepare data
data1 = dataset['follow_ISP'] * 20
data2 = dataset['attend_security_awarness'] * 20

# calculate spearman's correlation
coef, p = spearmanr(data1, data2)
print('Spearmans correlation coefficient: %.3f' % coef)
# interpret the significance
alpha = 0.05
if p > alpha:
  print('Samples are uncorrelated (fail to reject H0) p=%.3f' % p)
else:
  print('Samples are correlated (reject H0) p=%.3f' % p)
```

Fig. 18 python code to find spearman's correlation

```
pd.crosstab(dataset_bkp.risk_awarness, dataset_bkp.legitimacy_chk,
            margins=True, margins_name="Total")
```

Fig. 19 Python code for cross tabulation test

```
import scipy.stats
def regrsnline(x,y,a,b):
  slope, intercept, r, p, stderr = scipy.stats.linregress(dataset['follow_ISP'],
                                        dataset['attend_security_awarness'])
  line = f'Regression line: y={intercept:.2f}+{slope:.2f}x, r={r:.2f}'
  fig, ax = plt.subplots()
  ax.plot(x, y, linewidth=0, marker='s', label='Data points')
  ax.plot(x, intercept + slope * x, label=line)
  ax.set_xlabel(a)
  ax.set_ylabel(b)
  ax.legend(facecolor='white')
  plt.show()

y= dataset['lock_screen_while_away']
x = dataset['follow_ISP']
x_l = 'follow_ISP'
y_l = 'lock_screen_while_away'
regrsnline(x,y,x_l,y_l)
```

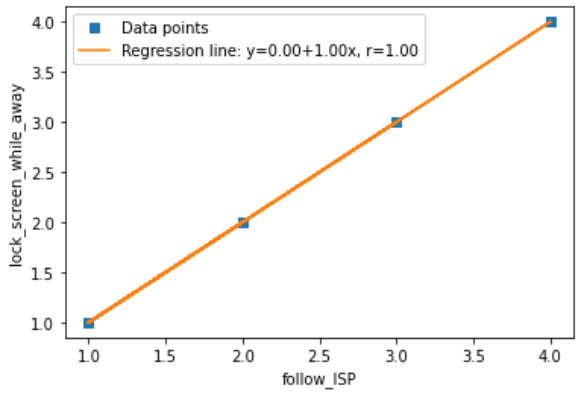
Fig. 20 Python code to plot linear regression between 2 variables

The results obtained from these tests are consolidated to a table in Table 1:

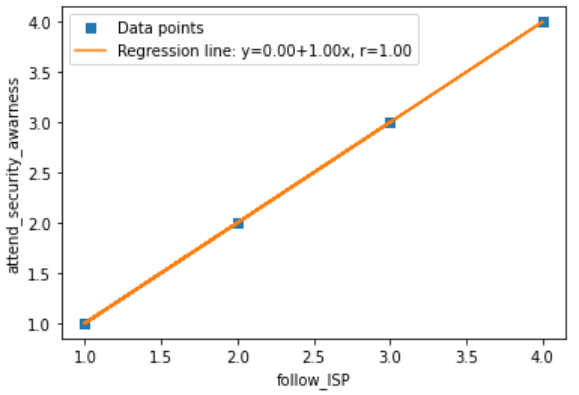
Questions	Correlation coefficient	p-value	Conclusion
1. How secure do you feel your working devices are? 2. I am careful about clicking on links in an email, pop-up screens, advertisements on web pages, or social media posts.	+ 0.286	0.002	Correlated (positive)
1. How secure do you feel your working devices are? 2. I check the legitimacy of a website before accessing it.	+ 0.242	0.009	Correlated (positive)
1. I always follow the information security policies (ISP) of my organization. 2. I attend security awareness programs conducted by my organization.	+ 1.000	0.000	Correlated (positive)
1. IT employees have a major impact on an organization's cyber security. 2. I believe the cyber security awareness of my colleagues/friends affects my cyber security awareness too.	+ 0.360	0.000	Correlated (positive)
1. I feel my organization is good at providing cyber security awareness to employees. 2. I am concerned that my working environment is not secure enough against cyber attacks.	- 0.297	0.001	Correlated (negative)
1. I feel my organization is good at providing cyber security awareness to employees. 2. I always follow the information security policies (ISP) of my organization.	- 0.295	0.001	Correlated (negative)
1. I manually lock my computer screen when I step away from it. 2. I always follow the information security policies (ISP) of my organization.	+ 1.000	0.000	Correlated (positive)

Table 1 Spearman's correlation test results

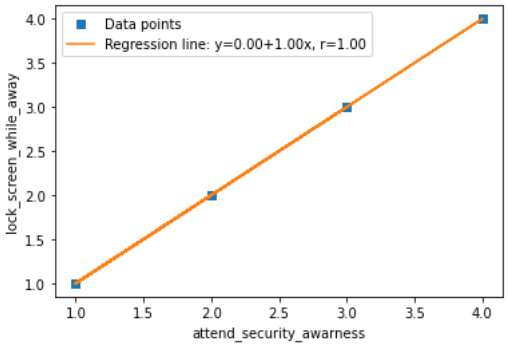
The results of linear regression Table 2:



20. 1 Somebody follows ISP, follows some desktop security practices.



20. 2 Somebody follows ISP, attend the security awareness programs too



20. 3 Somebody attends security awarness program, follows some desktop security practices

Table 2 Linear regression results

Table 3 shows the results of cross-tabulation where the correlation of risk awareness and security practices are assessed.

follow_ISP risk_awarness	Always	I do not know	Never	sometimes	Total
Agree	46	1	0	6	53
Disagree	5	0	0	1	6
I do not know	3	2	0	1	6
Strongly Agree	47	0	1	3	51
Strongly Disagree	1	0	0	0	1
Total	102	3	1	11	117

legitimacy_chk risk_awarness	Always	Never	Often	Sometimes	Total
Agree	29	0	14	10	53
Disagree	2	1	2	1	6
I do not know	2	1	1	2	6
Strongly Agree	27	2	14	8	51
Strongly Disagree	1	0	0	0	1
Total	61	4	31	21	117

lock_screen_while_away risk_awarness	Always	Never	Often	Sometimes	Total
Agree	44	0	6	3	53
Disagree	6	0	0	0	6
I do not know	3	2	1	0	6
Strongly Agree	42	0	7	2	51
Strongly Disagree	1	0	0	0	1
Total	96	2	14	5	117

Table 3 cross tabulation results

4 Discussion

4.1 Analysis of the results

A code in python programming has been used for the exploratory and descriptive analysis of the collected data. The findings from this research are suitable to answer the research question to assess the cyber security awareness of employees based on the conceptual model(Fig. 1). The observations summarized in Table 4 Findings based on PMT theory provide the answers to threat appraisal and coping appraisal of the participants according to various influencing factors.

No	Threat appraisal	Coping appraisal
1.	• 64% of the study population believes that the workplace is secure against any kind of cyberattacks. • 36% of the population tells the workplace is insecure.	• 77% of the study population who faced a cyberattack has reported it to an authorized authority. • Only 5% has fixed the problem by themself. • But 18% of these participants have either ignored it or not taken any actions as they are not aware of what to do in that situation.
2.	• 26% of the study population says the working device is secure against any cyber-attacks. • 58% says the working device is partially secure. • 15% says the working device is insecure.	• 73.5% of the study population agrees that the employees have a major impact on an organization's cyber security. • 26.5% disagree with this statement.
3.	• 89% of the study population agrees that cybercrime has been increased nowadays. • The rest 11% marked either disagreement with this statement or not aware of the current situation.	• 76.1% of the study population claims that if they are coming across any cyber attacks in future, they will report the same to an authorised authority. • 23.1% says that they take no action.
4.	• 91% of the study population agree that the ISP of the organization is effective against cyber attacks. • 9% are either not aware of ISP or tells that the organization's ISP is not effective against cyber attacks.	• 96% of the study population are aware of their organization's ISP. • Only 4% are either not aware of it or not following them.
5.	• 20% of the study population strongly agrees that the awareness programs by the organization are effective. • 78% agrees to the statement partially. • Only 3% says the awareness programs by the organization are not effective.	• 61% of the participants are always attending the security awareness programs conducted by their organization. • 29% are less likely or not to attend them.

Table 4 Findings based on PMT theory

Spearman's correlation and cross tabulation tests are used as the type of collected data were ordinal. The test results (Table 1,Table 2) helps to draw more conclusions regarding the relationship between various influencing factors of cyber security awareness in employees. The participants who follow the basic security practices such as website legitimacy check, lock desktop screen while away, etc. are more concerned about their device security which is an implication of perceived severity and

vulnerability. The participants who follow ISP and attend awarness programs by the organization claims that the organization has a major impact on the security awarness of their employees. This is can be considered as a reward to enhance the threat appraisal. The cross-tabulation results (Table 3) shows that the participants with good risk awareness are more likely to follow various security practices. The main implications of our research study are:

a. The awarness programs conducted by the organization and ISPs of the organization have a major role in improving the cyber security awarness of an employee.
b. Employees who are more concerned about the security of their working environment seems to correctly follow the desktop security behaviours.
c. 95% of the study population agrees that their peer behavior affects their cyber security behavior too.
d. Social influences build up the security awareness of employees and increases their threat appraisal in terms of perceived severity.
e. The exposure to cyber attacks improves the security behaviors like various desktop security practices of the employee. This helps the employee to achieve good response and self-efficacy which is the basis for the coping appraisal towards cyber-attacks.

The study is providing significant results on the role of organization, prior experience and desktop behaviour on security awareness as we have obtained a good correlation among them through spearman's correlation and cross-tabulation tests. These results are enough to prove the level of awareness of an IT employee in the selected sample population because the participants can check their awareness of their organization's security measures and follow them to achieve a good understanding of how to deal with or avoid a cyber attack. But there is not much evidence received to prove the impact of peer behavior and social media platforms on the security awareness of employees.

A similar survey by (Alzubaidi, 2021) found that more than 70% of the population did not report the cyber attack to the authorised authority whereas in our study we can find that 77% of the study population who has faced an attack has reported it correctly to the authorised authority. The difference is raised as the sample population chosen in both studies are different. Our research study could prove a close relationship between desktop security behaviour and the perceived severity which is an important finding in another referenced study by (Torten, Reaiche, & Boyle, 2018). The importance of cyber security training in security awareness is a major finding in the research study (Ergen, Ünal, & Saygili, 2021). Our research is providing good support to this finding.

The analysis stage also detected some limitations in the study. A non-random sampling is selected for this study due to the time constraints, so the validity of the results may not be high. Another limitation is a long questionnaire which the participants found hard to finish with maximum accuracy and this might have led to some bias in the collected data. Also, the less number of samples affected the correlation tests which could have given accurate results if there were enough samples to compare.

4.2 Future research

The current research study provides an assessment result of cyber security awareness of Indian employees working in IT departments of large organizations based on PMT theory. The future scope of the current study includes expanding the study to different regions of the world as the trend of security awareness changes across the regions. Another scope is to choose another type of ICT employees community such as employees from the financial department, health department, etc. Also, the study can be further narrowed down to assess only the social influence such as peer behaviour, working environment, social media, etc. in improving an employee's cyber security awareness.

The limitations encountered in the current study can be solved in future research by choosing a random sampling such as cluster sampling method instead of non-random sampling to obtain more accurate results from a large population. Also, choose a short questionnaire to reduce the bias in the answers from the participants. Also, various data collection methods such as sharing questionnaires through the post, e-mail, social media platforms, etc. can be implemented to collect more samples to improve the findings from the research results.

4.3 Conclusion

Our research was a quantitative analysis to assess the cyber security awareness of ICT employees in a selected sampling population. The findings in the study show that Indian employees working in IT departments of various organizations have a good awareness of the importance of cyber security. The study population was aware of most of the security threats and the countermeasures for them. But still, there was a small percentage of this sampling population that did not meet all the criteria to have a good cyber security awareness either due to lack of knowledge or limitations in the working environment. Another major finding from the study was the contribution of organizations in the security awareness of their employees. The employees who follow the organization's ISP and attend the awareness programs on cyber security are more likely to show good threat appraisal and coping appraisal towards cyber-attacks. So a strong ISP and mandatory training programs can assure an average of level security awareness among its employees. So that the organizations can give more attention to training their employees in security awareness in order to reduce the effect of cyberattacks.

References

(n.d.). Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

(n.d.). Retrieved from https://data.oecd.org/ict/ict-employment.htm

Alzubaidi, A. (2021). *Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia*. Retrieved from ScienceDirect: https://www.sciencedirect.com/science/article/pii/S2405844021001213

Borkovich, D. J., & Robert J Skovira. (2020). *Working from home: cybersecurity in the age of covid-19*. Retrieved from Iacis: https://iacis.org/iis/2020/4_iis_2020_234-246.pdf

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, W. R. (2017). *If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security*. Retrieved from Taylor & Francis Online: https://www.tandfonline.com/doi/abs/10.1057/ejis.2009.8?journalCode=tjis20

Cassetto, O. (2019). *The 8 Elements of an Information Security Policy*. Retrieved from https://www.exabeam.com/information-security/information-security-policy/

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). *Using behavioural insights to improve the public's use of cyber security best practice*. Retrieved from Researchgate: https://www.researchgate.net/publication/274192536_Using_behavioural_insights_to_improve_the_public'_s_use_of_cyber_security_best_practices

Cyber Crime 2020. (n.d.). Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Datareportal. (2022). Retrieved from https://datareportal.com/global-digital-overview

Denscombe, M. (2010). The Good Research Guide For small-scale social research projects. In M. Denscombe, *The Good Research Guide For small-scale social research projects.* Open University Press McGraw-Hill Education.

Dr., R. (1983). *Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change*. Retrieved from ScienceDirect: https://www.sciencedirect.com/science/article/pii/0022103183900239

Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). *Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters*. Retrieved from https://www.richtmann.org/journal/index.php/ajis/article/view/12588

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). *Working from home during COVID-19 crisis: a cyber security culture assessment survey*. Retrieved from springer: https://link.springer.com/article/10.1057/s41284-021-00286-2

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). *Correlating human traits and cyber security behavior intentions*. Retrieved from sciencedirect: https://www.sciencedirect.com/science/article/pii/S0167404817302523

Joinson, A., & van Steen, T. (2018). *Human aspects of cyber security: Behaviour or culture change?* Retrieved from ingentaconnect: https://www.ingentaconnect.com/content/hsp/jcs/2018/00000001/00000004/art00008

Jupyter Notebook. (n.d.). Retrieved from Jupyter: https://jupyter.org/

kadir, A., İbrahim, H., & Göksel. (2017). *Investigation of Cyber Security Behaviors of University Students*. Retrieved from Dergipark (DP): https://dergipark.org.tr/en/pub/kefdergi/issue/31577/351517

Li, L., & He, W. (2019). *Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior*. Retrieved from Sciencedirect: https://www.sciencedirect.com/science/article/pii/S0268401218302093

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). *Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review*. Retrieved from https://pubmed.ncbi.nlm.nih.gov/34372354/

Pandas library. (n.d.). Retrieved from https://pandas.pydata.org/

Protection motivation theory. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Protection_motivation_theory#Measures
Sava, J. A. (n.d.). *Number of ICT professionals worldwide 2019-2023*. Retrieved from https://www.statista.com/statistics/1126677/it-employment-worldwide/
Scipy. (n.d.). Retrieved from https://scipy.org/
Shell, C. (1992). *The Value of the Case Study as a Research Strategy*. Retrieved from Sage journals: https://journals.sagepub.com/doi/full/10.1177/1609406919862424
Shillair, R. (2020). *Protection Motivation Theory*. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119011071.iemp0188
Stančin, I., & Jović, A. (2019). *An overview and comparison of free Python libraries for data mining and big data analysis*. Retrieved from IEEE: https://ieeexplore.ieee.org/abstract/document/8757088
Statista. (n.d.). Retrieved from https://www.statista.com/statistics/1126677/it-employment-worldwide/
std-var. (n.d.). Retrieved from investopedia: https://www.investopedia.com/ask/answers/021215/what-difference-between-standard-deviation-and-variance.asp
Torten, R., Reaiche, C., & Boyle, S. (2018). *The impact of security awarness on information technology professionals' behavior*. Retrieved from ScienceDirect: https://www.sciencedirect.com/science/article/pii/S0167404818304656
Verizon.com. (n.d.). *Results and analysis 2020*. Retrieved from https://www.verizon.com/business/resources/reports/dbir/2020/results-and-analysis/
VisualStudio. (n.d.). *VisualStudioCode*. Retrieved from VisualStudio: https://code.visualstudio.com/

Appendix A Glossary of terms

Spearman's correlation:

Spearman's correlation measures the strength and direction of monotonic association between two variables. (spearmans, n.d.)

Cross tabulation:

Cross tabulation is a statistical tool that is used to analyze categorical data. Categorical data is data or variables that are separated into different categories that are mutually exclusive from one another. (cross tabulation, n.d.)

Variance:

variance is a measure of dispersion that takes into account the spread of all data points in a data set. (variance, n.d.)

Standard deviation:

Standard deviation is a number used to tell how measurements for a group are spread out from the average (mean or expected value). A low standard deviation means that most of the numbers are close to the average, while a high standard deviation means that the numbers are more spread out. (standard deviation, n.d.)

Appendix B Informed Consent Form

Evaluating cyber security awareness of IT employees

Informed Consent Form

Trust of the information taken via a questionnaire about cyber security awareness of IT employees.

Origin:
This internet-based survey was designed to serve the educational needs of the FMVEK course of the SCSSO Master's program, held by the University of Stockholm, Sweden.

Purpose of the research:
This questionnaire aims to provide a view of the awareness of cyber security amongst IT employees. The results of the survey will be used only to fulfill the requirements of the FMVEK course.

Structure:
The questionnaire includes only multiple-choice questions. The survey is designed to take 3-5 minutes of your time.

Confidentiality:
No personal information and contact details (including name, telephone number, e-mail, postal addresses, credentials of any kind, and IP address) are asked in this questionnaire or disclosed to the researcher. The anonymity of the responders to this survey is protected by design. In no way can the data provided be linked with any of the participants.

Voluntary Participation:
This survey is entirely voluntary. If at any time, you do not wish to continue the survey, please exit the webpage.

By filling out this questionnaire, I hereby declare that:

1. I am an IT employee and 18+ years old.
2. I completely understand the intention and purpose of the research study
3. I understand the way data I submit is going to be handled
4. I give my consent for the use of my submitted data in the way described in the questionnaire

- Thank you for your cooperation

Appendix C Questionnaire

Evaluating cyber security awareness of IT employees

Informed Consent Form

Trust of the information taken via a questionnaire about cyber security awareness of IT employees.

Origin:
This internet-based survey was designed to serve the educational needs of the FMVEK course of the SCSSO Master's program, held by the University of Stockholm, Sweden.

Purpose of the research:
This questionnaire aims to provide a view of the awareness of cyber security amongst IT employees. The results of the survey will be used only to fulfill the requirements of the FMVEK course.

Structure:
The questionnaire includes only multiple-choice questions. The survey is designed to take 3-5 minutes of your time.

Confidentiality:
No personal information and contact details (including name, telephone number, e-mail, postal addresses, credentials of any kind, and IP address) are asked in this questionnaire or disclosed to the researcher. The anonymity of the responders to this survey is protected by design. In no way can the data provided be linked with any of the participants.

Voluntary Participation:
This survey is entirely voluntary. If at any time, you do not wish to continue the survey, please exit the webpage.

By filling out this questionnaire, I hereby declare that:

1. I am an IT employee and 18+ years old.
2. I completely understand the intention and purpose of the research study
3. I understand the way data I submit is going to be handled
4. I give my consent for the use of my submitted data in the way described in the questionnaire

- Thank you for your cooperation

Basic information

How old are you? *

- 20 - 25 y.o
- 26 - 30 y.o
- 31 -35 y.o
- 36 -40 y.o
- 40+ y.o

How many years of experience do you have in the IT industry? *

- 0 - 3 years
- 4 - 9 years
- 10 - 15 years
- 15 years +

Choose your industry domain of work? *

- Banking, Finance Services and Insurance.
- Transportation & Communication
- Health & Wellness
- Education
- Sales & Marketing
- Manufacturing
- Law enforcement
- Others

Which device(laptop/desktop) are you using to work? *

- Company provided device
- Own device
- Both private & company devices
- Others

Cyber Security Activities

Select all commonly used security tools, activities, and applications that are applicable on your working device. (Tick all that apply) *

- [ ] Anti-virus
- [ ] Authentication (eg. Passwords,PIN)
- [ ] Encryption (encrypted mail, message, etc)
- [ ] On-time Software update
- [ ] Backup
- [ ] Firewall
- [ ] Bitlocker
- [ ] Updates/softwares to block certain websites
- [ ] Updates/softwares to block installation of certain softwares
- [ ] None of the above

How secure do you feel your working devices are? *

- ( ) Very Secure
- ( ) Somewhat secure
- ( ) Somewhat insecure
- ( ) Not secure
- ( ) Very insecure

Some security practices are described below. Please choose the most appropriate option for each practice.

I change the passwords of important accounts frequently. *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Never

I create a password that contains my personal information (e.g. name, date of birth, nickname) *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Never

I check the legitimacy of a website before accessing it *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Never

I am careful about clicking on links in an email, pop-up screens, advertisements on web pages, or social media posts. *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Never

I manually lock my computer screen when I step away from it. *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Never

If I discover a security problem such as phishing mail, identity theft, malware etc: *

- ◯ Report it to authorised authority like IT security team
- ◯ Respond or interact with mail content
- ◯ Take no action

I attend security awareness programs conducted by my organization *

- ◯ Always
- ◯ sometimes
- ◯ Never
- ◯ There are no such programs in my organization
- ◯ I do not know if there are any such programs in my organization

I always follow the information security policies (ISP) of my organization. (such as data disclosure, desktop security, etc) *

- ◯ Always
- ◯ sometimes
- ◯ Never
- ◯ I do not know about ISPs of my organization

Cyberattack consciousness

How do you keep yourself updated about cyberattacks/cybersecurity? (Tick all that apply) *

- ☐ TV, news, posters, magazines, radio
- ☐ Internet, website, email bulletins, blogs, etc
- ☐ Updates from my coworkers and friends
- ☐ Newsletters from my organization
- ☐ Social medias such as Twitter, Instagram, Facebook, etc
- ☐ I do not feel that I keep myself updated often
- ☐ Others

Please select your opinion about the below statements:

The IT employees have a major impact on an organization's cyber security. *

- ◯ Strongly Agree
- ◯ Agree
- ◯ Disagree
- ◯ Strongly Disagree

I believe the cyber security awareness of my colleagues/friends affects my cyber security awareness too. *

- ◯ Strongly Agree
- ◯ Agree
- ◯ Disagree
- ◯ Strongly Disagree

I am concerned that my working environment is not secure enough against cyber attacks. *

- ◯ Strongly Agree
- ◯ Agree
- ◯ Disagree
- ◯ Strongly Disagree

I feel that the risk of becoming a victim of cybercrime has increased in the past years. *

- ◯ Strongly Agree
- ◯ Agree
- ◯ Disagree
- ◯ Strongly Disagree
- ◯ I do not know

I believe that the ISPs (Information Security Policies) of my organization are effective in managing cybersecurity. *

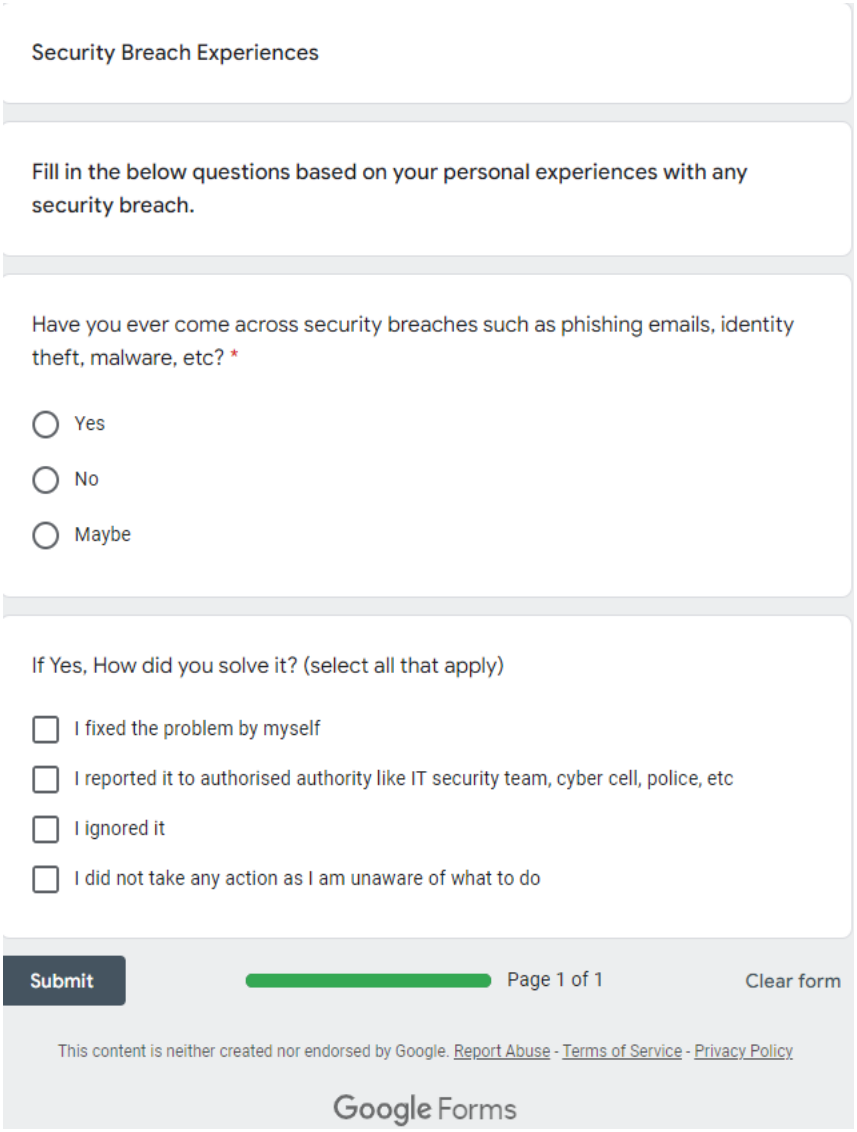
- ◯ Strongly Agree
- ◯ Agree partially
- ◯ Disagree
- ◯ I do not know

I feel my organization is good at providing cyber security awareness to employees. *

- ◯ Strongly Agree
- ◯ Agree partially
- ◯ Disagree
- ◯ Strongly Disagree

I am willing to accept increased Internet surveillance from my organization if it can enhance Internet security *

- ◯ Strongly Agree
- ◯ Agree partially
- ◯ Disagree
- ◯ Strongly Disagree


Security Breach Experiences
Fill in the below questions based on your personal experiences with any security breach.
Have you ever come across security breaches such as phishing emails, identity theft, malware, etc? *
Yes
No
Maybe
If Yes, How did you solve it? (select all that apply)
I fixed the problem by myself
I reported it to authorised authority like IT security team, cyber cell, police, etc
I ignored it
I did not take any action as I am unaware of what to do
Submit
Page 1 of 1
Clear form
This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy
Google Forms