EFFECTIVE INFORMATION SECURITY POLICIES FOR EFFICIENT REMOTE WORKING: SOFTWARE PROFESSIONALS' PERSPECTIVE

Amarasinghe Arachchige Dileesha Sandamali

179129N

Degree of Master of Business Administration in Information Technology

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2019

EFFECTIVE INFORMATION SECURITY POLICIES FOR EFFICIENT REMOTE WORKING: SOFTWARE PROFESSIONALS' PERSPECTIVE

Amarasinghe Arachchige Dileesha Sandamali

179129N

Thesis submitted to the Department of Computer Science and Engineering of the University of Moratuwa in partial fulfilment of the requirement for the Degree of Master of Business Administration in Information Technology.

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2019

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

………………………………. ………………….

A. A. D. Sandamali Date

(Signature of the candidate)

The above candidate has carried out research for the Masters thesis under my supervision.

……………………………….. ………………….

Dr. Shantha Fernando Date

(Signature of the Supervisor)

COPYRIGHT STATEMENT

I hereby grant the University of Moratuwa the right to archive and to make available my thesis or dissertation in whole or part in the University Libraries in all forms of media, subject to the provisions of the current copyright act of Sri Lanka. I retain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

Abstract

The increasing extensive use on mobile devices and concepts like Bring Your Own Device (BYOD) together with sophisticated technologies empower the concept of “remote working” (also called teleworking, work-from-home) as a growing trend in software practice, making the security of information more vulnerable. The necessity for security measures is significantly arising in this context. It is problematic if productivity is disturbed when it is attempted to realize the target of reducing this risk via security measures. Through this research, it was intended to find out what perception do the remote working software professionals have on the Information Security Policy (ISP) as a creator of productivity pitfalls and what considerations should there be when devising information security policies to keep remote workers in the software industry efficient. A detailed quantitative approach followed by a short qualitative analysis were engaged to learn about the perception of the remote-working software professionals based on data gathered via a survey.

Several aspects such as, "the increase of additional work and procedures due to policy", "complexities and issues in following the policy", along with "awareness of the policy and information security in general", were identified to have a significant positive impact on the remote working software professional’s productivity. Also, it shows that not only the non-managerial staff but also the managerial staff need to improve, disapproving the assumption that management is following the correct procedures. Based on these findings, recommendations were made that could be considered when setting up an ISP. However, due to limitations in accessing the data, results are mostly relevant to the private sector. It is expected that this study would be beneficial to policy-makers by getting prior knowledge of what is affecting the performance of the ISP and to the end-users by enabling them to involve in policy making to make finally their own lives easy.

Keywords: Information Security, Remote Working, Telework, Software, Productivity

ACKNOWLEDGEMENT

My research study on "Effective Information Security Policies for Efficient Remote Working: Software Professionals' Perspective" would have been impossible without the support of a number of people and I'm profoundly grateful to each and every one of them.

Thank you, Dr. Shantha Fernando, for mentoring, supervising and guiding me. Your immense knowledge, insightful comments and unswerving support were like a blessing. I am also grateful to you Dr. Dilum Bandara for always encouraging while giving the theoretical and practical knowledge of research. I sincerely appreciate the insights given by Mr. Thilan Jayathilaka, as my external resource person. Moreover, I would like to thank the lecturer panel of the Master of Business Administration in Information Technology degree program for the knowledge and wisdom they shared, which helped me throughout the project, more or less and to the staff of Department of Computer Science and Engineering at University of Moratuwa, including Mr. Dinesh Bandara, for assisting cordially.

Further, I would also like to show my gratitude to my colleagues, professional connections, fellow members in ResearchGate and all the participants in the survey. I could not have imagined getting this study completed without their help.

My family and friends, thank you for bearing with me, encouraging me by having an eye on the progress and showering me with warm wishes. I am always grateful to my mother and father, who worked by the sweat of their brow to make me who I am today.

Most importantly, I'm thankful to my loving husband Indika, who stood with me through all the ups and downs during this project as with everything else in life, creating purpose, caring and understanding the situations, being supportive all the time, bringing back my focus every time I lost it.

Finally, I would like to thank all who helped in delivering this thesis. Even if the names were not mentioned, your support is greatly valued.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation		**Description**
BYOD	-	Bring Your Own Device
GDPR	-	General Data Protection Regulation
IoT	-	Internet of Things
IS	-	Information Security
ISP	-	Information Security Policy
IT	-	Information Technology
PESTEL	-	Political, Economic, Social, Technological, Environmental, Legal factors
SOHO	-	Small Office – Home Office concept
ROI	-	Return on investment

1. INTRODUCTION

The current study links three of the important elements of software discipline; remote working, information security and productivity. This chapter focuses on what inspired to initiate the study, the details of the problem under study and the significance of the research. Also, it guides the reader on how the contents of the rest of the chapters are lined.

1.1. Background and Motivation

“Information is at fingertips” is a term that is used frequently nowadays. It implies that the information is easily accessible to anyone. The usage of mobile devices for day-to-day work is increasing. This trend and the sophisticated technologies enabled the concept of “remote working” a reality, which can be used as an umbrella term for remote working, teleworking, work-from-home and the likes. Seem to have developed from the SOHO (Small Office-Home Office) concept which was there even before 19th century (“Small office/home office”, n.d.), remote working can be referred to as “work from anywhere” (Adams, 2016) even though there are recognizable differences among remote work, telework, work-from-home, etc.. Jack Nilles, a former US Air Force officer/ rocket scientist/ researcher, who is now considered as “the father of telecommuting/ teleworking” coined the terms “telecommuting” and “teleworking” in 1973 (“JALA International: Jack Nilles biography”, 2011). Despite the fact that the managers lacking the confidence of the concept due to numerous reasons such as not being able to see whether the telecommuting-employees are really working, it does show a slow but steady increase. Figure 1.1 (Jones, 2015) is a graph taken from a survey done by Gallup, an analytics company, which shows the growth of telecommuting of US workers over the years.

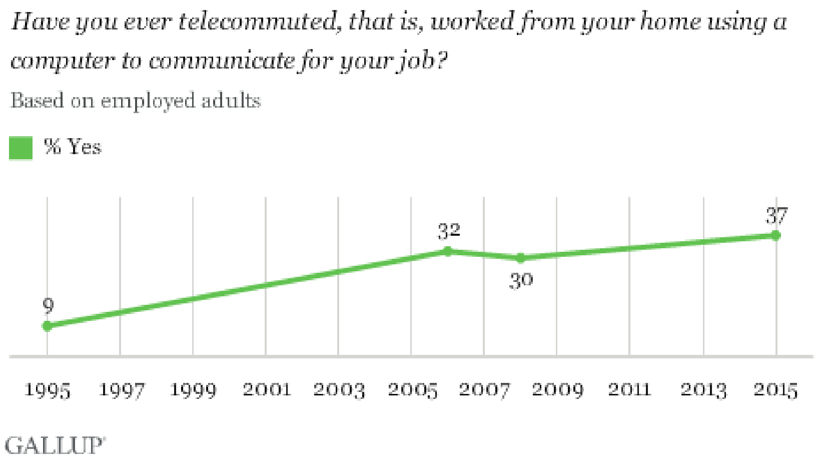


Figure 1. 1: Results from Gallup's Annual Work and Education Poll in 2015 [Source: Jones (2015)]

In addition, United States Census Bureau Report (Census Bureau Report Shows Steady Increase in Home-Based Workers Since 1999 - Employment & Occupations - Newsroom - U.S. Census Bureau, 2012) assures the steady increase even though the numbers may be different from the above due to the different sample sizes. An important fact that was highlighted in the findings was that the percentage of Home-based workers or teleworkers in computer, engineering and science occupations had been increased by 69% over the decade between 2000 and 2010.

Another trend that can be observed is “Workcation”; Wikitionary defines this as a vacation which one spends while working (“workcation”, n.d.). The employees take a vacation, most often at a faraway place from the office, sometimes even in another country; but working and being available on all work-related communication channels. Some do this for the change of the scenery and some do this to avoid certain seasons like winter (Greenawald, n.d.; Business Insider Netherlands, 2019). This trend has gone viral to an extent to which there are dedicated retreats to these so-called “digital nomads” (Springer, 2017). Springer (2017) mentions extracting from a report by the networking site AfterCollege that approximately 68% of the millennials who are in search of jobs, find it attractive if remote working is included in the job offer.

Another result of the uprising of “remote working” is the growing usage of mobile devices and concepts like BYOD. With this trend, security and privacy of information are becoming more and more vulnerable as the organization loses control over the devices that are being connected to the network.

Consequently, the need for security measures is significantly rising. This fact alone makes the Information Security Officers restless. What happens next is the addition of more and more security measures as precautions to decrease risk. As the popular saying declares, too much of something is good for nothing.

Is there anything traded off to achieve this? Some say that it is productivity which is the compromised factor to accomplish the target of reducing the risk of information security. A global Fortune 100 bank took a step to ensure information security by blocking all the uncategorized URLs from their Secure Web Gateway; this action crushed down malware infection rates remarkably, but consequently, resulted in an overwhelming number of end-user complaints on certain websites not being accessible and not being able to do their job properly because of that (Guruswamy, 2016).

Would too many security measures affect productivity? Obviously, security and productivity are two different things but they are closely inter-related and each one of them is of great importance in an enterprise’s perspective. On the other hand, most of the organizations embrace remote working to gain more productivity through granting flexibility of allowing to work at a convenient place for the employees. To force maintaining a proper balance between security and productivity of remote workers, it is very important to dig into more detail on how the security measures affect their productivity so that the necessary actions could be taken to create a proper Information Security Policy (ISP). The lack of formal research done in this area is also a motivating factor to initiate this research project.

The efficiency of a security initiative is associated with the processes of the whole organization, not with a part of it or an individual; it is a collective result. The best industry practices cannot be used as they are; they need to be adapted to match the particular organization according to their culture, financial status, etc. for them to add value. Having good security practices in place and making them tolerable to the employees would bring out success in balancing security and productivity. A good security policy would be the baseline that would determine the success of the rest of the initiatives.

1.2. Problem Statement and Research Question

With the rapid advancement of technology, the security of information is becoming more and more vulnerable. The more sophisticated it gets the more threats it attracts. Proper security measures should be in place to secure information, which is the most important asset a business has. However, the security measures taken should not be causing a business disruption by prompting productivity hits. Even though people have an understanding of the fact that security and productivity have to be balanced, most of the organizations do not seem to follow. Some businesses focus only on security ending up in productivity drops and employee frustration. Some ignore security and focus only on productivity, ultimately facing losses caused by security breaches. After making all the mistakes, the world seems to be coming into an agreement on the fact that the right balance between security and productivity is a necessity. When considering the level of security needed, enterprises should consider when, where and how much security is needed to keep in line with good productivity levels. Reasons including poor communication and lack of awareness may cause the employees to take short cuts and violate the security policies.

Remote working is a current trend which most of the organizations are adopting all over the world. With the many advantages it brings in, it also opens the outer world an easy entry to an organization’s information. Therefore, the security reinforcements should be well-thought-out and implemented in that context. On the other hand, they should help balance security and productivity. It is important to understand this matter to come up with the necessary amount of information security standards needed in order to provide balanced solutions with regard to remote working.

The problem is that it is not known exactly what perception that the remote working software professionals have towards the security policies as a factor affecting the productivity in performing their day-to-day work as well as the related factors that may cause productivity drops, although the companies motivate the software developers to work more and more remotely. Therefore, we attempt to find what information security related factors have impacted the productivity of the remote workers which leads to specifically addressing the following research question:

> *"What considerations can be regarded as essential when devising information security policies to maximize the efficiency of remote workers in the software industry?"*

1.2.1. Research Objectives

By finding the answer to the research question, the following objectives are expected to be served:

- *To identify and assess the factors affecting the perception of the remote workers in the software industry on how the security policies implemented by their organizations are affecting productivity.*

- *To provide recommendations for devising effective information security policies to maintain a better balance between information security and remote worker productivity.*

- *To contribute to the research knowledge areas of information security and remote working.*

In order to meet the above objectives, a literature survey was used to identify the factors that can affect the balance between information security and productivity of remote workers. Through the findings, it lead to providing recommendations for security personnel that would be helpful in setting up effective security policies.

1.2.2. Research Significance

The findings of this research will contribute to the software field to a great extent in view of the growing tendency for remote working. Information security policy is the tool that is used as “the controlling authority”. It should be practical and match the context in order to secure the productivity of an employee. Productivity is always a concern that comes with remote working and so as the security of information as this practice exposes an organization’s data to the outer world. These aspects need to be balanced as both are very important to sustain a company’s growth. The findings of this study guide the software organizations that are into telework to understand what aspects of information security policy are contributing as factors that lead to inefficiencies of the remote workers. It also recommends certain points to consider when devising the ISP to ensure and maximize the productivity of those workers. In addition, the study helps the teleworkers (including the researcher) understand the fact that neither productivity nor security should be compromised and that they should be balanced. Also, as the end users, they get insights so they can make suggestions to make their organizational ISPs better and applicable to their context. On top of that, this study contributes to filling a knowledge gap in the research area of remote working in consideration of information security and productivity.

1.2.3. Outline

The remainder of the thesis is structured as follows: Chapter 2 provides a review of the existing related literature associated with information security, productivity and remote working which serve as secondary data. Chapter 3 describes the methodology adopted in this research detailing the research variables, their relationships, development of hypotheses, survey approach, etc.. Analysis of the collected data comprises Chapter 4 while conclusions, recommendations, limitations of the study and openings for future work are presented in Chapter 5.

2. LITERATURE REVIEW

There can be so many factors that can be categorized as the well-known PESTEL factors driving the IT team of an organization to put security policies in place or tighten the existing policies. Sometimes these requirements can be unavoidable; for example, every company that does business in/ with people in EU countries should align their policies, procedures, systems and services to be compliant with General Data Protection Regulation (GDPR), some companies need to adhere to ISO:27000 standards and other regulations such as banking and telecommunication standards. These do not essentially ensure that productivity is not disturbed. No matter if it is introducing new security policies or tightening the existing policies, it brings out a change. And it is a universal truth that change is something that is always resisted. The resistance to change itself or the difficulties associated with practicing/ adhering to the security policies eventually pose a hit on productivity. This becomes worse when the management of the organization does not really see how the individuals work and that is why there can be more pressure put on remote-workers. And of course, there can also be threats to security that can do severe damages in terms of financial as well as reputation when the employees connect to the network from outside. The next sections will review the existing literature in diverse areas that are related to information security policies and productivity and how they are linked with remote working. Section 2.2 looks at the general perception towards information security vs productivity in sub-sections focusing the need for balance between the two (section 2.2.1) and concerns on policies and related factors affecting productivity (section 2.2.2) as a support in identifying potential factors that can be related to this study. Section 2.3 goes through the concerns with regards to information security affecting remote workers drawing attention to sources related to information security challenges in remote working (section 2.3.1) and the increasing need of information security in remote working and the trends in remote working landscape (section 2.3.2). Section 2.4 attempts to evaluate existing work on remote worker productivity and information security policies to find the fit-in of this study into the research area.

2.1 Information Security vs. Productivity – The General Perception

This section reviews the literature that examines the relationship between information security and productivity and the factors that can affect the urge of the users to adhere to the security policies.

2.1.1. The Need for Balance

Davis (2011) highlighted the importance of having the right amount of information security to not to lose employee productivity and some key points to consider in achieving that.

How too-much security would badly affect the productivity and its negative consequences were well-explained by Davis. He advised determining "when", "where" and "how much" protection is needed to keep the organization safe plus to keep all happy. Davis described the elements of tools that would provide good visibility on potential security threats. They "must provide panoramic, 360-degree visibility into your complete risk posture that presents correlated data in such a way that users can quickly pinpoint where to focus their security efforts.". Picking a tool which has a good threat research capability and can provide vulnerable areas and countermeasures is crucial. Figure 1 depicts the features that a good security tool should have according to him. He emphasized that when it comes to having various security measures, what's important is "a combination that delivers balance—one that provides protection and peace of mind." (Davis, 2011).

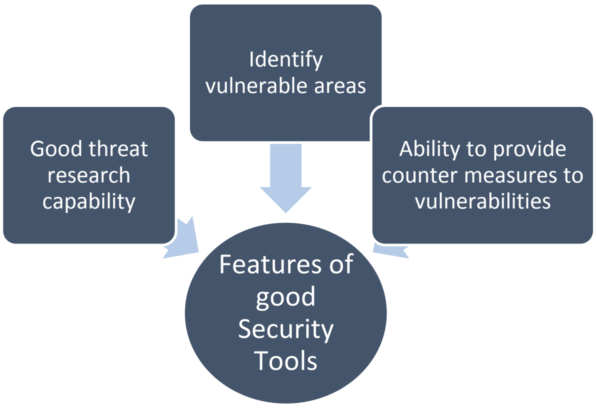

Identify vulnerable areas
Good threat research capability
Ability to provide counter measures to vulnerabilities
Features of good Security Tools

Figure 2. 1: Features to be considered when picking a security tool

Author further explains the consequences like frustration because of losing the balance between security and productivity and compared them to Yin and Yang in Chinese philosophy (according to Wikipedia, “polar or seemingly contrary forces are interconnected and interdependent in the natural world, and give rise to each other in turn.” (“Yin and yang”, n.d.)), so the reader could clearly understand what he tried to share. Further, he suggested actions such as having a proper risk management policy that provides visibility, which the organizations could take to strike that balance in a confident, short and a simple way. He strongly states about the inability to have perfect and one-fits-for-all solutions, and that the solution needs to be customized to serve the requirement.

Today, according to one of Barkly’s new survey reports, the most difficult thing that the organizations have to deal with when it comes to cybersecurity is the security solutions slowing down the system as well as the rest of the processes by slowing down the data transfers because they have to go through firewalls and routers (Gilchrist, 2016). Inadvertently, this results in decreasing productivity which then results in a chain of activities such as taking insecure/ unauthorized shortcuts in order to improve efficiency and productivity.

It looks like system slowness is not the only one alone in the corner of dissatisfaction. According to the report, while 41% of the respondents claimed that the reason for their frustration about the system was slowness, 36%, 33% and 33% accounted respectively for too many updates, high cost and not providing necessary protection against zero-day attacks, respectively. Figure 2.2 depicts the most prominent results of the survey.

Gilchrist (2016) also noted that the top management’s concerns are more on insider threats by quoting Jack Danahy, co-founder and CTO of Barkly. According to Danahy, “This report proves that from the CISO to the entry-level IT pro, organisations must be better aligned when it comes to security. When there's a disconnect in priorities, level of understanding and measurement, even a seemingly strong security initiative is destined to fail,” and further “Once teams understand each other's priorities and concerns around security, they can implement the tools they really need, that will best protect their endpoints from ever-increasing, complex threats." (Gilchrist, 2016).

Gilchrist clearly expresses the discontent that the end-users could go through with so many security measures in their systems. The productivity of the workforce of an organization can go down due to various reasons but most accounting for the security initiatives.

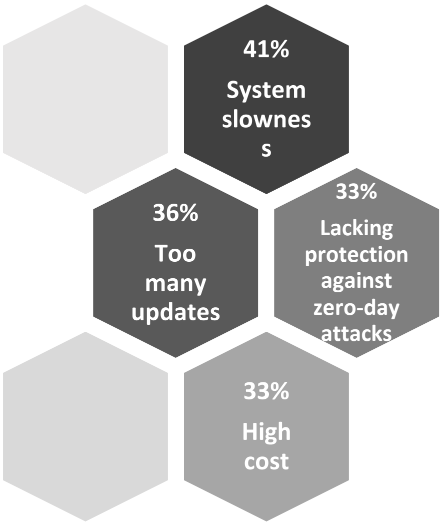


Figure 2. 2: Major reasons for dissatisfaction of end-users due to security measures - according to 2016 Cybersecurity Confidence Report by Barkly

White (2016), who is an author and a CIO, wrote about a contradictory argument to the above in a feature article, that the IT leaders give preference and priority to productivity over security. She pointed out that organizations can be forced to neglect some of the security practices because some implementations of the same can make the systems slow and affect productivity. She has based her statements on two recent studies done on cybersecurity practices (one of them being the same report which Gilchrist (2016) referred above – 2016 Cybersecurity Confidence Report by Barkly, done using 350 IT Pros).

Furthermore, White listed the root causes for most of the problems as:

- poor communication,
- lack of employee awareness,
- slowed productivity and
- lack of budget

Those studies have revealed major drawbacks in the security-approach, how the lack of awareness and communication is connected with those and the way security measures badly affect productivity which leads to general frustration. This indicates that most of the organizations need to revisit their security policies and refine them. As quoted in the article, according to Jack Danahy, CTO and co-founder of Barkly, a good security-approach wouldn't affect productivity in a bad way. Also, the efficiency of a particular approach is associated with the whole organization, not with a part of it or an individual.

The confidence level in information security should not be something that determines whether or not to deploy security measures. In the same studies mentioned above, when asked from IT leaders of organizations, it has not revealed that a good level of confidence on security is there. There are some notable figures on IT leaders' views such as 50% reporting about lack of confidence in the current security measures, 20% not believing that effective security is possible and ¾ assuming that the employees' cybersecurity-awareness is moderate. On the contrary, security initiatives are only some obstacles to the way the employees see it. But they should know that a slight delay in completing the security requirements would not cause a downfall in the productivity in the whole organization; as mentioned above this trade-off should be measured against the total process not according to a part of it. This is becoming tougher since the IT Pros fail in defining the ROI of security in an accurate way.

White (2016) further said "IT leaders are being forced to choose between strong security and productivity, and most companies are sticking to the latter" and, "Ultimately, these solutions aren't stopping breaches, as the study points out, and the effects are simply slowing down day-to-day business".

White attempts to emphasize that productivity is given priority over security and how that puts cybersecurity at threat by using the same data set which Gilchrist (2016) has used above as one of the bases for her statements. She brings up an unseen side with facts to prove her assumptions. Even though there are many good points in this article, a problem with White's statements is that they are supporting the side of security the most and not productivity even if she has approved that some security approaches affect efficiency badly. The other study she had chosen is from the ISACA/RSA, which discusses more cybersecurity than productivity, therefore, it's not relevant to this research.

Bacik (2011) seems to support the idea of balancing security and productivity while sharing a similar opinion with White (2016). She clarified about the "security paradox", in which the businesses tend to prioritize productivity over defence (Bacik, 2011). She described how the increasing mobility of data, which supports intensifying productivity, in turn, contributes to bringing in threats to information security. A key area highlighted by Bacik is the need of identifying an accepted risk level to maintain security without affecting productivity. According to her, "To ensure there is a balance of productivity and security, the enterprise needs to baseline the network activities" (Bacik, 2011). She also mentioned that the security practices can be done centrally at the IT administrator's level, as well as the enterprise users' level in a tolerable extent, balancing productivity and security using careful planning and review. Moreover, she suggested some actions that could be taken at various levels without disturbing productivity such as implementing "single sign-on" feature and whitelisting. All of such activities are revolving around the single fact "baselining the environment".

Balancing security and productivity should be an ongoing act between the security needs and the organizational culture. Some organizations provide a lot of freedom to employees where they can download anything from the internet, use any tool, etc.. These should be moderated with caution. She took the Instant Messaging (IM) applications as an example; these are supposed to increase productivity but can actually have a negative influence on security; in order to overcome these threats, the enterprises can use the purchasable, proper application of the same kind without stopping the use of instant messaging.

For an enterprise to be productive and maintain proper defence level at minimum cost and risk, the following elements are to be considered by organizations:

- Integrated and layered defence across systems and networks,
- Real-time threat intelligence and reputational analysis,
- Centralized security management platform that provides a singular management console,
- Real-time network monitoring to ensure response times and employee productivity and
- All network monitoring and administration backed by a dedicated team of security research experts and competent administrators.

She also mentioned some aspects that the organizations should consider as best security practices like being proactive on identifying risks and the importance of integrated security offerings, but these are not much relevant to the research that is being carried out.

“Looking at productivity from an enterprise user's point of view also requires some consideration. How much security will the enterprise user tolerate? Many times, what users do not know will not hurt them. Well, yes and no.” (Bacik, 2011). How the end-users look at the extra steps they have to go through when adhering to security measures and resisting on security audits, etc. thinking of themselves as trusted employees are things that should be challenged, according to Bacik.

This article emphasizes the importance of striking a proper balance between productivity and security. Furthermore, it gives away some important factors and aspects to look into, in the same area. On the other hand, it contains a lot of considerations on security which is out of scope but can be used indirectly when forming the survey questionnaire of this research.

2.1.2. Concerns on Policies and Related Factors Affecting Productivity

Even though there is a need for balance between productivity and security, it should not be the case that if the security policy is made too flexible in an attempt to maintain the balance. If the policy compromises security, the question is whether it is the right policy for the organization. By keeping the policy up-to-date with approaches to deal with the most current threats rather than adding restrictions on top of what is already there in ISP and by treating ISP as an integrated strategy, it would support to maintain the balance up to some level. Non-compliance and frustration of the end-users at these changes can be avoided by continuously keeping them informed about the purpose and importance of the changes and the consequences of not making them (Stackpole, 2016). It is more advisable to identify what portion of the operations in the system needs to be controlled and how to do it (Smalley, 1999).

Farrugia (2009) explained how the convention of granting privileges only for the least an end-user can tamper with would lead to making false assumptions that they need lesser access rights than what is necessary. This is mainly because of the belief that users cannot violate security policies if they cannot meddle with them. However, Farrugia (2009) has mentioned that no matter what the target is, this results in productivity downfalls and frustration.

The author further explains this case using examples. One example was blocking access to external FTP servers; he states that a particular user who is required to access FTP servers but cannot because of the security boundaries would do more insecure things like accessing a website which allows accessing FTP servers and might go on giving his/her user credentials to the third party, primary objective being meeting deadlines without having to go through a lengthy, time-consuming process of getting access rights.

Another example he has taken is forcing users to change passwords frequently. Psychologically, this doesn’t drive a user to pick a hard-to-guess password since he/ she knows that it needs to be changed soon. Further, he said that most of the users are only concerned whether their PC works, not about security. Because of this, even if they are forced to pick a complex password, they would place it somewhere which is easily accessible to anyone causing a security policy violation in another way.

The bottom line is, even though there are industry best practices with regards to information security, we cannot adopt them in any organization as they are. “Before taking any security measure, always think about whom it will affect, what its actual effect will be, and whether it’s the right thing to do. In IT security, there’s never a one-size-fits-all solution, and the best security schemes are tailor-made for that specific scenario.” (Farrugia, 2009). These are the base stones to be laid in order to achieve efficiency while adhering to security policies. The best practices and standards should be bent and twisted until it becomes the most suitable product for the organization.

In order to do this, the organization’s risk appetite should be considered. Not only it has to be defined properly, but also it has to be reviewed every once in a while as well as when changes such as new technology adaptation, changes in organizational structure caused by mergers and acquisitions, new regulatory requirements occur (“CYBER RISK APPETITE: Defining and Understanding Risk in the Modern Enterprise”, 2016). When policy decisions are taken, it usually happens from top to bottom in the organizational hierarchy. However, it would be more successful if the top management understands the seriousness of the subject (“Information Security Top-Down”, 2004).

A study done by Bulgurcu, Cavusoglu and Benbasat (2010) takes the reader to a new dimension by introducing attitude, normative beliefs and self-efficacy as factors affecting non-compliance to information security policies while most of the authors argue on reasons such as negligence and seeking shortcuts to meet deadlines. They put forward a theory which is “along with normative belief and self-efficacy, an employee's attitude toward compliance determines intention to comply with the ISP” (Bulgurcu, Cavusoglu & Benbasat, 2010, p.523). They have assumed that an employee’s attitude is based on various elements such as the benefit of compliance, cost of compliance and cost of non-compliance (See Figure 2.3).

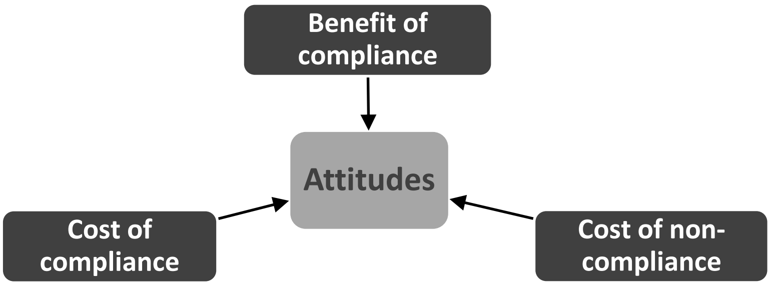


Figure 2.3: Factors affecting user attitudes towards security measures according to Farrugia (2009)

The study has provided them with results that would support their theory and showed that the above-mentioned factors have a significant impact on compliance with the security measures taken by the organization. Even though these authors did not focus on employee productivity, this is a good resource to get an idea on a new level of evaluating the end-users which would eventually guide to learn more on the end-user's perception with regard to the security policies.

Sun, Ahluwalia and Koong (2011) support the above communique with their research titled "The more secure the better? A study of information security readiness". In their study, they measured Information Security Readiness (ISR) and have found a non-linear relationship between security level and ISR (Sun, Ahluwalia & Koong, 2011). Even though they have done a thorough investigation, there's a doubt whether this relationship is a mere coincidence. And to add to that, only undergraduates of a particular university have been selected as participants of the survey, which could limit the possibilities of the results. The study has exposed important facts;

> For data of high criticality, enhancing security level had a positive impact on ISR, but only up to the point perceived as appropriate by the participants. For data of low criticality, the enhancement of security level was perceived as unnecessary. In addition, IT proficiency was found to be a significant covariate, especially when data criticality was high (Sun, Ahluwalia & Koong, 2011).

This exposes us to the fact that the end-users are not always resisting towards the security initiatives taken by their organizations as a habit; but at a certain point, they say “enough is enough”. The security officers have to find this equilibrium and refine their security policies to reach that.

This research has attempted to measure the factors and has been able to get an idea on equilibrium. In addition to examining user attitudes, they have also pointed out the importance of user training in order to achieve success in making security measures something that is pleasing to the end-user. This research can be considered as a base to any of the new research that will be taking place.

A research done by Al-Mukahal and Alshare (2015) targetting the organizations in Qatar was also reviewed while doing this literature survey. Even if it’s limited to one country, this gave some insight on what to look for when doing the research. It looks into the factors that influence the number of information security policy violations in Qatari organizations. Getting an idea on the factors that can influence one particular set of people would be helpful in steering research towards a different or a wider group and to gather more information on different aspects.

Among the findings of this research are significant factors that are contributing to information security policy violations (Al-Mukahal & Alshare, 2015) such as,

- trust
- the impact of implementing information security policy on work environment and
- the clarity of the scope of the information security policy.

Moreover, they have spotted cultural dimensions such as the likelihood of avoiding uncertainty and collectivism having influence up to a high level when it comes to the relationship between the above factors and security policy violations.

At the outset, this research seems to have nothing to do with the productivity of the end-users. Additionally, the sample set is limited to people in a particular country. But when looked at in another angle, being researched for done not long ago, this provides some fresh tips to identify why the end-user violates security policies and what perception towards the same makes him/ her do so.

Chan, Woon and Kankanhalli (2014) mentioned in their article “Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior” that according to surveys 78% of computer attacks are spread via emails and for this reason the employees who ignore the security policies and open them while infecting others in the same network. Therefore, they stressed that “more attention needs to be paid to learning why non-compliant behavior takes place so that appropriate measures for curbing the occurrence of such behavior can be found.” (Chan, Woon & Kankanhalli, 2014).

The main objective behind their research is to examine the way that certain factors are affecting the compliance of the employees to the security policies. According to them, the following aspects are positively related to an employee’s perception of the security measures of the organization:

- management and supervisory practices and
- co-worker’s socialization.

Furthermore, the perception delivered through these, along with self-efficacy has had a positive impact on the end-users being compliant.

The findings of this research pointed out some major aspects which are mentioned above to look through to find possible scenarios to gain knowledge on end-user’s perception.

Figure 2.3 illustrates how the factors that affect the end-users’ to perceive information security policies as having a negative impact on productivity. The inward arrows represent a causality while the outward arrows represent consequences. Factors that are root causes for the causes are linked with lines.

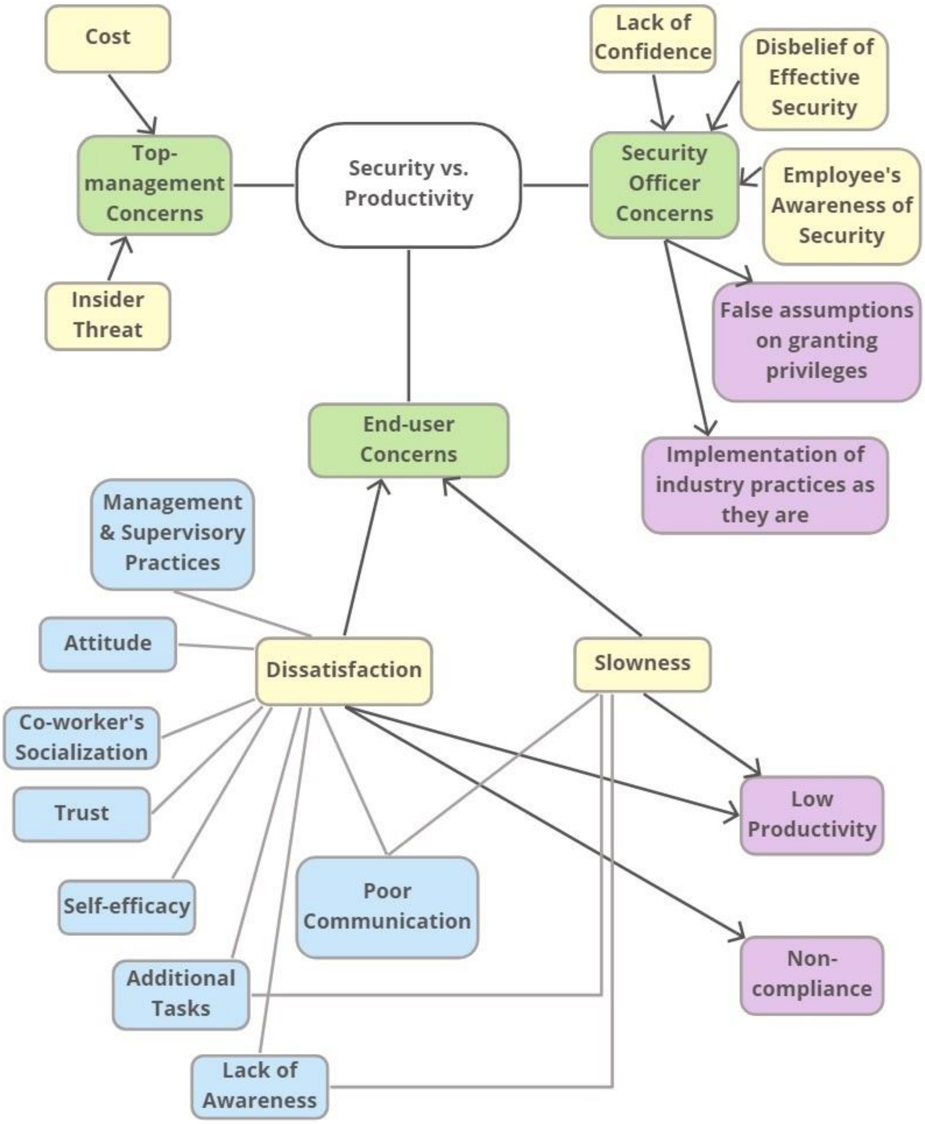

Cost
Lack of Confidence
Disbelief of Effective Security
Top-management Concerns
Security vs. Productivity
Security Officer Concerns
Employee's Awareness of Security
Insider Threat
False assumptions on granting privileges
End-user Concerns
Implementation of industry practices as they are
Management & Supervisory Practices
Attitude
Dissatisfaction
Slowness
Co-worker's Socialization
Trust
Low Productivity
Self-efficacy
Poor Communication
Non-compliance
Additional Tasks
Lack of Awareness

Figure 2. 3: Concerns on IS and Productivity as derived from Literature Review

2.2. Concerns with Regards to the Information Security Affecting Remote Workers

This section reviews the literature that discusses how IS can affect remote working, what type of threats and vulnerabilities are there and what needs attention for a remote worker in the software industry.

2.2.1. Information Security Challenges in Remote Working

Jilani, U., Ahimmat, A., Raso, A., Thorpe, D., & Tran, M. (2013) categorize the security risks associated with teleworking into three categories as:

- Physical risks,
- Technical risks and
- Document management risks.

The *Physical Risks* may include unauthorized access, theft, damage, tampering that are done to the device as well as getting the storage infected with malicious software. In addition to these, this category includes sensitive data theft in public places using computer forensic tools, shoulder surfing (i.e. information theft by looking at the screen over the employee’s shoulder) and eavesdropping.

They present the *Technical Risks* in different perspectives like user perspective and network perspective, listing some threats such as device configuration complexity, malware, password strength, eavesdropping (electronic) and network traffic analysis. According to them, the threats can be of specific characteristics with regard to the nature and the type of the business and can be targeted. Further, the personal use of the devices might also pose a threat because the users might disable security features for convenience and based on the misconception that they are secure enough.

The researchers highlight the importance of *Document Management Risks* as the documents such as projects, contracts and agreements as well as documents concerning the privacy of individuals are assets of an organization, which might be accessed by teleworkers for many purposes.

> An unauthorized issue of sensitive information which is normally stored in documents could not only damage the public's trust in an Ready, Steady Telework Information Security essentials for the teleworker 5 organization but also jeopardize the mission of an organization which may include harming individuals if their personal information has been released. The document management practices include physical and digital copies (Jilani et al. (2013)).

Their recommendations to overcome these challenges include making awareness on physical as well as technical risks that can be coming their way from the environment, public and private networks, applications and system, etc.. When it comes to document management, they need to be educated on the different policies that can have an influence on the different types of documents. For all this to happen, there should be proper policies in place. Their main target is on Security Awareness, Training and Awareness.

In a short article, Green, J. (2017) has highlighted some workarounds for the biggest security risks of telework. *Table 2.1: Workarounds for some of the security risks of telework* depicts these workarounds (the table continues in next page).

Table 2. 1: Workarounds for some of the security risks of telework.

Risk	**Workaround**
Unsecure and public Wi-Fi connections	Making awareness among employees to use only trusted networks when dealing with sensitive data
Losing information	Educating the employees as to never leave a laptop or other device used for telework unattended in a public place, car, hotel room, etc. Encrypting files when taking files from the workplace

Visual theft/ visual hacking	Ensuring that the confidential data in the screen is not visible to others
Negligent employees	Incorporating best practices for remote working into the Information Security Policy Making security awareness an ongoing practice Providing compliance training
Unsecured mobile apps	Including a list of approved apps (after making sure that the app makers have addressed security) in the Policy
Improper disposal of confidential information	Ensuring proper disposal of digital and paper media

These suggestions contain some of the ideas that can be included in an ISP as well as some good practices for the remote workers to take into account.

2.2.2. The Increasing Need for Information Security in Remote Working and The Trends in Remote Working Landscape

While embracing the trend of remote working – one of the trends that is rapidly taking over the global workforce – among the key actions that need to be taken, Information Security should also be included in order to maintain smooth operation of the company (Thudium, 2017). The remote workers accessing company information from anywhere using a laptop or other mobile device that they use to work is indicating that the security landscape now includes the individual computer systems, too. To take care of this, Thudium (2017) suggests a few actions that can be taken.

- Securing the workplace by making awareness on having a proper work area to conduct work at home and to take necessary actions such as choosing strong passwords and disconnecting users after a time-out of no activity, when using public areas to work,

- Restricting the usage of public wi-fi and educating the users on threats caused by accessing public wi-fi,

- To have a personal company VPN to enable a private and a controlled network,

- To encourage running the software updates on the employee personal computers that they use to work and keep them up-to-date to reduce vulnerabilities and

- To do remote worker monitoring so malicious activities are detected easily.

But, when it comes to the electronic monitoring of the employees, it is something that needs to be handled with care. According to Holland, Cooper and Hecker (2015), employee monitoring has a negative impact on their trust in the management. On one hand, it indeed is an effective tool to measure employee productivity, ensure security and be knowledgeable on what's happening in the organization when executed with caution but on the other hand this can make the employees feel uncomfortable, distrusted and demoralized, which can eventually tarnish the employment relationship as well as productivity and ultimately this can even lead to employees withdrawing themselves from the organization.

Another concept that goes hand in hand with remote working is Bring Your Own Device (BYOD). Some organizations allow their remote workers to plug their own device and plug it into the company network. As far as the two important aspects in this research – productivity and security – are considered, this can have a mixed impact.

Gajar, P.K., Ghosh, A., Rai, S. (2013) highlight many of these benefits and drawbacks. According to them an advantage for the company would be the considerable saving on procurement of the devices as well as training. More importantly, they believe that there is an increase in the productivity, efficiency and morale of the employees as a result of practising this concept along with remote work. On the contrary, this also carries challenges such as not having up-to-date anti-viruses, firmware, etc., high vulnerability to attacks due to the high level of connectivity, affecting the integrity of the data due to both personal and business data residing in the same computer and having less control over information security. Gajar, et al. (2013) list down some measures such as integrity control and compliance that could be taken to mitigate the risk, which in turn would affect the productivity negatively when considering the insights gained from literature in section 2.1 above.

Working remote nowadays is more like a synonym for working in the cloud. As the cloud is secured, end-point security is often a neglected topic. However, it should be noted that the security of an organization which is operating in a cloud environment is seriously dependent on endpoints. Proper integrations, restrictions and other settings should be in place with endpoint security in mind (Roemer, 2016).

Morrow, B. (2012) calls BYOD a phenomenon which is among the trends that can influence the degree of control over an organization's sensitive data availability. (According to Wikipedia, "the term phenomenon refers to any incident deserving of inquiry and investigation, especially events that are particularly unusual or of distinctive importance." ("Phenomenon", n.d.)). He mentions data leakage, data theft and regulatory compliance as the security implications contributed by BYOD as it drives the employees' increased access into the organization's sensitive data via devices over which the organization has less control. What he suggests to overcome these is to treat the devices that are corporately owned and that are not.

Internet of Things (IoT) is something that is rapidly trending in the present. With the increasing use of the internet, cloud computing, etc., Internet of Things (IoT) came into the scene and it has already become a major trend. Maddox, T. (2016) describes how it is posing threats to IT security in ways that people would not even imagine. She mentions excerpts from several security experts, mostly from the ideas gained from a roundtable-discussion done by TechRepublic.com. Even a vending machine which is connected to the company network via IoT, is vulnerable to security threats and any attacker who can exploit that, can reach so many other personal and corporate devices without much hassle as a number of devices are tightly connected. IoT security expert Dave Palmer (director of technology for Darktrace), sees the modern businesses as hives of connected objects. These tight connections enable the attackers to gain access to the core of the network.

In the roundtable-discussion, TechRepublic has involved a number of top-notch security experts holding responsible positions such as product managers, general managers, etc. from companies like Intel Security, Hewlett Packard Enterprise, etc.. Their ideas also echo with the ideas above and according to them, security in IoT is complex as the IoT connects not only the corporate devices but also the employees' personal devices. In fact, they identify security as the biggest barrier to the adoption of IoT. One idea shares the importance of knowing the agreements before connecting the device to the network and sharing data as a precaution. These same methods in a corporate office can be considered to be exposing avenues for the attackers no matter whether the employee is in his/ her home office or somewhere else connecting to the company network; one such method that may have a bigger impact is the unsecured/ not properly secured Wi-Fi connections. Another point raised in this discussion was that "there is a lack of awareness of the attack surface that the IoT systems present and a lack of due care in consumer deployments" (Maddox, 2016). Due to this, the corporate and home networks are inadvertently made open to the threats via IoT.

There are some suggestions from the experts in the discussion to overcome the challenges/ to reduce the effects of these threats to businesses (Maddox, 2016) which are mentioned in Table 2.2 (the table continues in next page).

Table 2. 2: Suggestions to businesses to overcome threats posed by IoT

Suggestion	**Target**
Involve security testing when building IoT applications	The developers of such applications

Have an “end-end, data-centric security approach” in IoT infrastructure, removing the space for a compromise of an IoT device	The organization which involves IoT infrastructure
Educate the employees	The organization
Create a proper policy with regard to device usage	The organization
Implement a good threat defense life cycle that includes measures to protect, detect and correct.	The organization
Putting necessary controls in place (e.g. network access controls, limiting access only to necessary information to perform the tasks, usage of VPN, usage of Privileged Account Management (PAM)	The organization
Keeping track of who is connecting, who should be connecting, etc.. Ensure that proper monitoring is in place.	The organization

Table 2.3 contains a list of suggestions given for the remote workers (Maddox, 2016) which is most relevant for this research (the table continues in next page):

Table 2. 3: Suggestions for users of IoT enabled devices to ensure information security

Suggestion	**Target**
Invest in commercial intrusion detection and network monitoring	Remote workers
Change default usernames and passwords of IoT devices, install a quality firewall, check with vendor on the internal security mechanisms	Consumers of IoT devices

To secure access to company data and network, install security software in the devices that are used to access company network. Keep them active and up-to-date.	Remote workers
Keep the devices locked when not in use. Require PINs, passwords or other biometric methods to unlock.	Remote workers
Use privacy/ blackout screens when on devices used to access company data when connecting from public locations.	Remote workers
Use end-to-end encrypted, password-enabled Wi-Fi. Use passwords that are unique and change them often. Connect via VPN.	Remote workers
Enable Bluetooth only when necessary.	Remote workers
Download apps only from official app stores. Consider security settings of the apps before downloading.	Remote workers

2.3. Existing Work on Remote Worker Productivity and Information Security Policies

When considering most of the literature mentioned in the sections above, they identify the security risks posed by remote working (e.g. Green, 2017; Jilani et al., 2013; Maddox, 2016; Thudium, 2017) but they have not looked at the problem in the remote worker’s perspective. Even though some of them indicate that the information security policies should be set up in a way that they do not disrupt the productivity of the businesses and the importance of using the right amount of security (Al-Mukahal & Alshare, 2015; Davis, 2011; Farrugia, 2009; Sun, Ahluwalia & Koong, 2011), they do not relate their studies/ articles with remote working which is a subset of online working.

Some dated but useful white papers from SANS Institute also provide guidelines/ best practices that can be helpful in setting up security policies.

Hirsch, J. L. (2000) concludes that, in order to meet the challenges resulted by granting remote access, the telecommuting solution should be created with the attention to information security; i.e. a sound security policy balancing financial and security considerations. She suggests identifying the telecommuters on the necessity and qualifications as the basis. When considering qualifications, she mentions that an important factor is the remote worker’s awareness of information security and the related risks in case a security incident occurs.

In his white paper, Jenkins, G. (2002) points out that security policy to be treated as a vital area in mitigating teleworking risks. The following, in particular, should be considered in an ISP with regards to remote working, according to him:

- Who may telework,
- Services available to teleworkers,
- Information restrictions,
- Identification/authentication/authorization,
- Equipment and software specifications,
- Maintaining integrity and confidentiality,
- Maintenance guidelines,
- User guidelines (User's role),
- User education.

While giving out some very good insights into policy-making, these whitepapers have not focused on the possible reasons resulted by the same which can lead to productivity drops of the employees who are into telecommuting.

Cisco white paper, Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior (n.d.) mentions, IT organizations must listen to their clients for better insight into how their users perceive security issues. Without an ongoing dialogue, IT will have only a limited view of how well teleworkers understand IS and apply best practices when working remotely (Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior (n.d.)).

Knowledge of how the remote worker sees the security policy can be useful to the security officers in order to implement sound security policies.

2.4. Summary

Information security and productivity, being integral parts of a business, must be balanced carefully. In the current context, the software industry provides more flexibility in exchange for more efficiency and creativity. Remote working/ telework/ telecommuting/ SOHO (Small Office – Home Office) is a concept that is arising as a result of the need for flexibility at work. Remote working has a number of information security threats associated with it. These need to be handled using security policies to ensure the integrity and confidentiality of information while making sure that following the policy does not become a burden or cause business disruption by leading to productivity hits. This may lead to inefficiencies as well as non-compliance. Existing literature proves these, makes suggestions and best practices, but few looks at the security policies in the remote working software professional's eye who is the end user.

Going by the reviewed literature and the researchers' observations, two factors that can be the main reasons for failures in the security policies in productivity perspective, in general, were identified; dissatisfaction of the employee towards the implemented security policies and the slowness of the systems and processes or the complexity caused by the security initiatives.

The contributing factors to these reasons are;

- The level of communication,
- Attitudes of the end-user of the policy,
- The amount of additional work caused by having to follow the security policies,
- The level of education provided by the organization on the security policy,
- Management and supervisory practices in information security,
- The perceived level of trust/ strength of the relationship between the employee and the organization
- Connectivity and other constraints.

3. RESEARCH METHODOLOGY

Learning about the perception that the remote-working software professionals have on the influence of the information security policies over their productivity is one of the aims of this research. This was done through a survey and the findings derived by analyzing the results of the same are the base for the other objective which is to make recommendations to the IT officers in improving the information security policies so that they do not pose a negative effect on the productivity of the remote workers in the software industry.

This chapter discusses the research methodology that was adopted to achieve the above aims. It details the conceptual framework, the target population, hypothesis development and how the data was collected.

3.1. Conceptual Framework

The conceptual framework links the Research Problem, Research Question and supports to drive the investigations in a clear direction in achieving the Research Objectives. It illustrates the various types of variables that are related and presents their relationships to better understand the rationale behind the study. The Conceptual framework is seen by researchers and students as representing the particular study's overview visually, communicating existing or own theories with regard to the study or a series of logical and sequential suggestions proving the importance of the study (Ravitch & Riggan, 2017).

The conceptual framework to be followed in this research is shown in Figure 3.1.

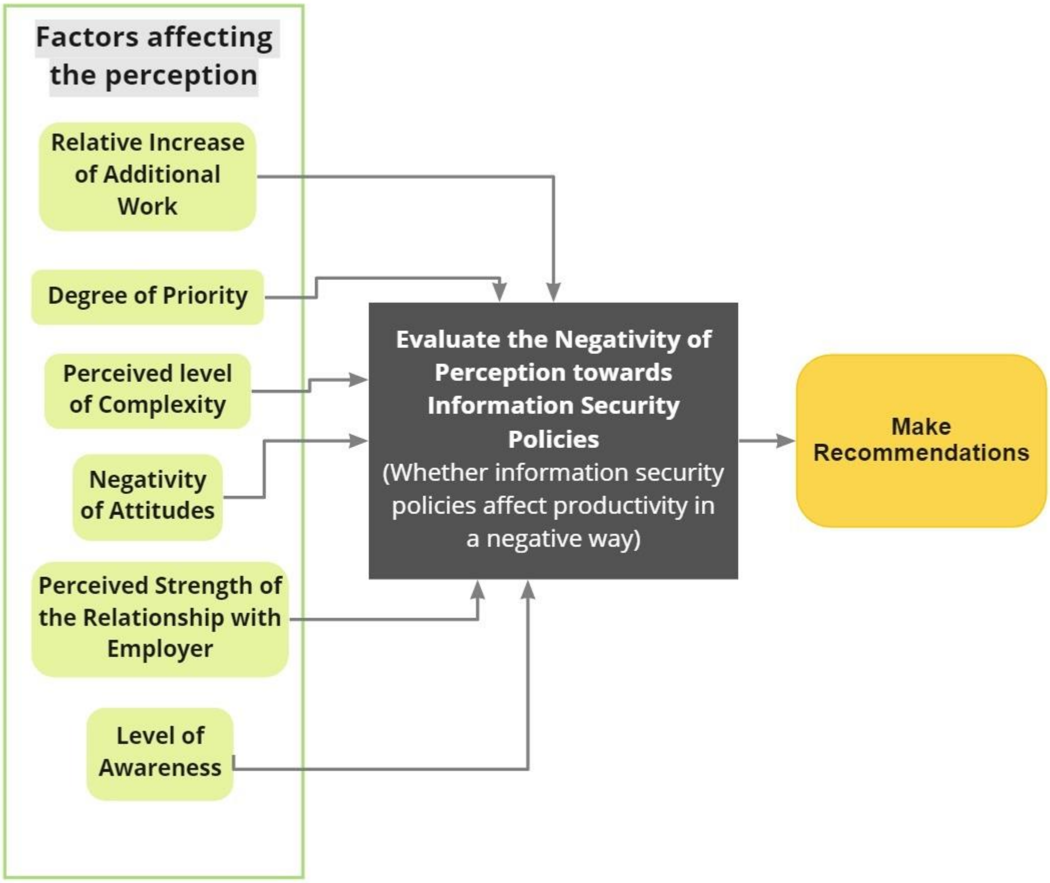

Factors affecting the perception
Relative Increase of Additional Work
Degree of Priority
Perceived level of Complexity
Negativity of Attitudes
Perceived Strength of the Relationship with Employer
Level of Awareness
Evaluate the Negativity of Perception towards Information Security Policies
(Whether information security policies affect productivity in a negative way)
Make Recommendations

Figure 3. 1: Conceptual Framework for the current study

3.1.1. Variables

The Dependent Variable in this study is the Perception of the remote working software professionals whether the information security policies affect their productivity. This reacts to the variations of the Independent Variables. The Mediating Variables explain the impact of some of the Independent Variables over the Dependent variable; i.e. how the perception is affected by the Independent Variables.

Table 3.1 defines the Dependent Variable and related literature.

Table 3. 1: Definition of the Dependent Variable

Variable	Definition	Related Literature

Negativity of Perception Towards Information Security Policies	In Psychology, perception is defined as "Mental processes by which intellectual, sensory, and emotional data are organized logically or meaningfully." – ("Perception (psychology)", n.d.).
	The extent of negativity of the remote working software professionals' perception when considering the influence of information security policies over their productivity is reflected here.
		Chan et al. (2014);
		Davis (2011);
		Guruswamy (2016)

The existing literature related to the Dependent Variable, especially the scholarly work, has little focus on the remote working community of the software industry.

The Independent Variables are defined in Table 3.2. The dependent variable is measured against these variables with respect to the effect the ISP has when comparing the situations where the ISP is followed and not (the table continues in next two pages).

Table 3. 2: Definition of the Independent Variables

Variable	Definition	Related Literature
Relative Increase of Additional Work	Additional tasks apart from the usual day-to-day work that the users have to carry out in order to adhere to Information Security Policy. By requiring to adhere to security policies, there can be additional activities created (e.g. changing passwords frequently, going through	Bacik (2011)

	special processes to get approvals, etc.) while connecting to the network, getting privileges, accessing sensitive data, etc.. The users may have to spend some extra effort beyond the actual expected effort to the tasks they are doing at work due to these, i.e. in order to meet the security requirements. This effort will ultimately be added to the daily output showing a productivity downturn.	
Degree of Priority	The degree of priority given to follow Information Security Policy by supervisory and management practices. The ISP may define the level of compliance and the team may perceive its outcome (whether it is affecting productivity or not) differently. When the immediate management's priorities (e.g. productivity) conflict with the organization-wide priorities (e.g. adhering to security policy), conflicts may occur.	Gilchrist (2016); Sun et al. (2011)
Perceived Level of Complexity	The complexity perceived by the remote worker in following the Information Security Policy while ensuring productivity when working remote.	Thudium (2017); Maddox (2016); Gajar et al. (2013); Farrugia (2009); Jenkins (2002); Hirsch (2000)
Negativity of Attitudes	The remote workers' attitudes towards the policy. These can be formed with partial involvement of past experience; most of the time, negative attitudes due to bad experiences that the users had to go through as a result of following security policies (for example, longer waiting times to obtain privileges, system slowness). Observations of instances in which actions that are taken to follow the ISP that affect productivity may contribute in setting up the nature of experience (good or	White (2016)

	bad) and thereby affecting attitudes.	
Perceived Strength of Relationship with Employer	The relationship between the employer and employee, looked at in employee's perspective. If a certain policy is put in place (e.g. monitoring the visited sites) where this relationship is weak in employee's eye, the employee may feel that the reason behind it is the fact that he/ she is not being trusted.	Bulgurcu et al. (2010)
Level of Awareness	The remote worker's common sense and general knowledge, awareness made by the relevant parties by communicating the details of the policy and training programs held by the company.	White (2016); Al-Mukahal and Alshare (2015); Sun, Ahluwalia and Koong (2011); Thudium (2017); Green (2016); Maddox (2016); Jilani et al. (2013); Morrow (2012); Jenkins (2002); Hirsch (2000)

Mediating variables given in Table 3.3 were considered initially, but dropped them later. Resistance coming from the organizational level and dissatisfaction coming from the individual's level can be affected by the independent variables in this study as factors but when digging into more details, it could be concluded that they do not have a significant effect that requires to be measured in this study.

Table 3.3 containing the Definitions of discarded Mediating Variables continues in next page.

Table 3. 3: Definitions of Mediating Variables

Variable	**Definition**	**Related Literature**
Degree of Resistance	Degree of resistance created by the security policy set up. A resistance usually builds up as a response when moving out of comfort zone or having to do something new is required. A resistance may form when the remote workers are unable to understand what the correct priority is; whether it is following the information security policy disregarding its effect on productivity or to ensure productivity even if the security policies are violated. This may result in decreased productivity of the employees.	Gilchrist (2016); Sun et al. (2011); Davis (2011) Schwochau et al. (1997) state that involvement of employee participation in policy changes resulted in better support from them for implementation of the policy changes.
Level of dissatisfaction	The level of dissatisfaction of the remote worker towards following the information security policy. A weak bond between the employee and the employer may result in	Gilchrist (2016); Davis (2011); Sun et al. (2011) According to Halkos &

	dissatisfaction. Having to follow a security policy may be seen as the employee as the company doubting in the employee's trustworthiness. The dissatisfaction may badly affect the employee's productivity.	Bousinakis (2010), increased job satisfaction results in increased productivity. Ye and King (2016) point out that the trust between the employee and management can help avoid the negative consequences on productivity generated by dissatisfaction.

3.1.2. Hypotheses Development

In order to evaluate the research question via a survey which is a quantitative method, hypothesis testing was used. "A hypothesis is a tentative statement about the relationship between two or more variables. It is a specific, testable prediction about what you expect to happen in a study." (Cherry, 2018).

Several hypotheses were developed based on the proposed conceptual framework and the previous related research outcome. These directly relate to the independent variables. By testing these hypotheses and measuring the probability of each hypothesis being true, it was expected that the speculated relationships between the independent and dependent variables could be assessed and thus come to conclusions based on those proven associations.

Let;

H_A – Alternate Hypothesis

H_0 – Null Hypothesis

Hypothesis 1:

H1$_A$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the relative increase of additional work/ tasks/ procedures created by the information security policy.

H1$_0$ – The additional work/ tasks/ procedures created by information security policy has no impact on the remote worker’s perception towards the information security policy’s influence over productivity in the software industry.

Hypothesis 2:

H2$_A$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the priorities set by supervisory and management practices with regard to productivity and information security policy, by creating resistance.

H2$_0$ – Priorities set by supervisory and management practices with regard to productivity and information security policy have no impact on the remote worker’s perception towards information security policy’s influence over productivity in the software industry.

Hypothesis 3:

H3$_A$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the perceived level of complexity of following the information security policy while working remotely.

H3$_0$ – Perceived level of complexity of following the information security policy while working remote has no impact on the remote worker’s perception towards information security policy’s influence over productivity in the software industry.

Hypothesis 4:

$H4_A$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the attitudes towards following information security policy while working remotely.

$H4_0$ – Attitudes of the employee towards following the information security policy while working remote has no impact on the remote worker’s perception towards information security policy’s influence over productivity in the software industry.

Hypothesis 5:

$H5_A$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the employee’s perceived strength of relationship with their management by creating a dissatisfaction.

$H5_0$ – Perceived strength of the relationship of the employee with their management has no impact on the remote worker’s perception towards information security policy’s influence over productivity in the software industry.

Hypothesis 6:

$H6_A$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the level of awareness with regard to maintaining information security and following information security policy while working remotely.

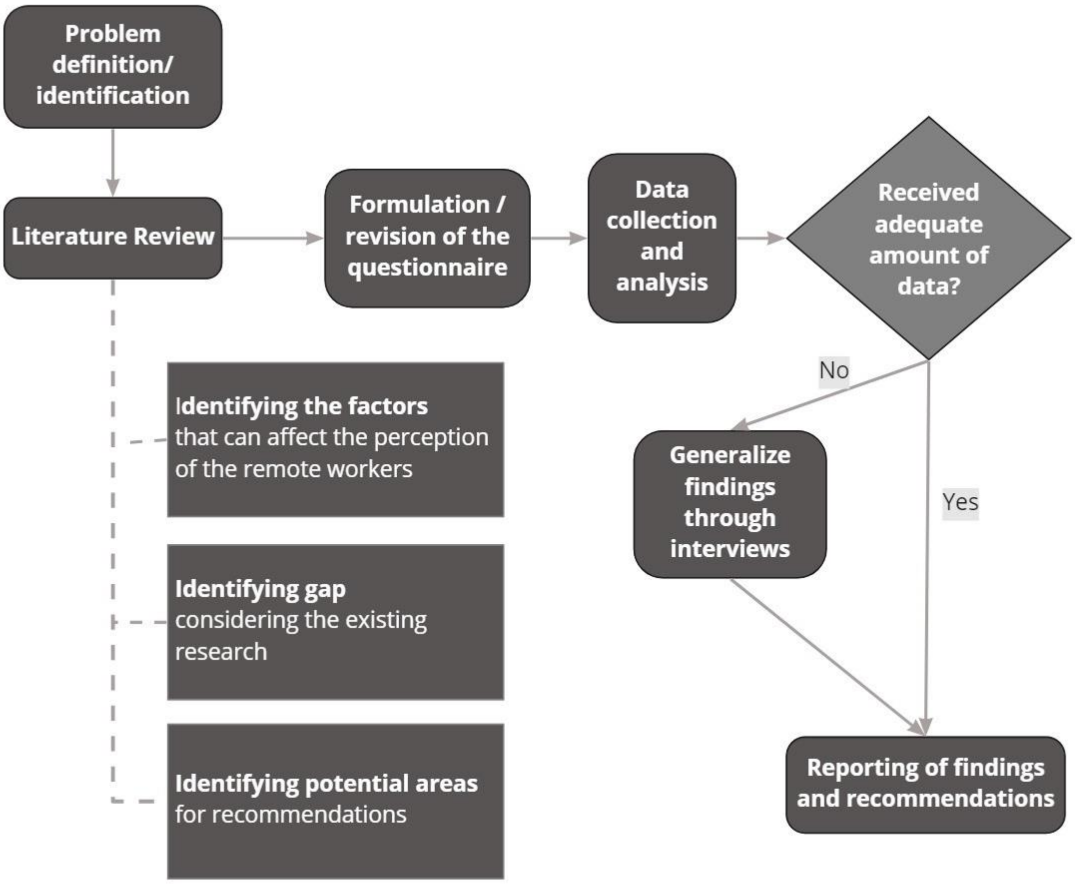
$H6_0$ – Level of awareness of the employee regarding the importance of following the information security policy while working remote has no impact on the remote worker’s perception towards information security policy’s influence over productivity in the software industry.

3.2. Research Method

Adopted a pragmatic method with the plan to initially assume a quantitative approach via a questionnaire (which is relatively convenient and economical than interviewing) and later on, if necessary, to take on a qualitative approach as a complement to or a verification on the results obtained via the quantitative approach.

Figure 3.2 depicts the flow of the research project; the actions that will be taken from the beginning until the end.

Figure 3. 2: Methodology of the current study


Problem definition/ identification
Literature Review
Formulation / revision of the questionnaire
Data collection and analysis
Received adequate amount of data?
No
Yes
Generalize findings through interviews
Reporting of findings and recommendations
Identifying the factors that can affect the perception of the remote workers
Identifying gap considering the existing research
Identifying potential areas for recommendations

Secondary data was collected with the help of a Literature Survey. Through this, the factors that can have an impact on the software professional's view were identified. These were then placed in the Conceptual Framework which aided in forming the hypotheses. The quantitative approach was supported by primary data collection via a questionnaire instrument which was set-up based on the developed hypotheses. It was distributed online via a google form among the targeted respondents.

3.3. Questionnaire Development

Following the hypotheses, a questionnaire instrument (Appendix A) was developed to measure the relationships between the independent variables and the dependent variable. The questionnaire consisted of 3 main sections/ categories. Section 1 was intended to capture the respondent's perception of how the information security policy is affecting their productivity. This was captured using a 6 point Likert scale having options Strongly Disagree, Disagree, Slightly Disagree, Slightly Agree, Agree and Strongly Agree. It was decided to use to opt for the 6 point Likert scale instead of using the commonly used 5 point Likert scale to get rid of the "neutral" opinions which does not add value for the study as most of the time the respondents tend to select Neutral when they do not want to put thought into the question. In other words, this forces the respondent to select a more proper assessment, resulting in better data. While Section 2 focused on the demographic information of the respondent, Section 3 was anticipated to capture how the individuals felt about some popular or highly available attributes of a potential information security policy along with an open-ended question to obtain the respondent's opinion, which would give guidance when doing recommendations.

Table 3.4 presents a summary of the measures that were used to test the above hypotheses. Appendix B contains more details by categorizing the questionnaire items into sections and then into variables that are being measured.

Table 3. 4: Measures of variables

Variable	Item Count	Scale
Relative Increase of Additional Work	3	6 point Likert scale
Degree of Priority	3	6 point Likert scale
Perceived Level of Complexity	3	6 point Likert scale
Positivity of Attitudes	3	6 point Likert scale
Perceived Strength of Relationship with Employer	3	6 point Likert scale
Level of Awareness	3	6 point Likert scale
Negativity of Perception Towards Information Security Policies	3	6 point Likert scale

3.4. Population and Sample Selection

The targeted population of respondents consisted of software professionals who were working in software or non-software organizations and who did telework part-time or full-time, globally. There was no reliable source of statistics available to determine the population size. Therefore, in order to come up with an acceptable sample size, a few methods were taken into account.

Cochran’s formula (Cochran, 1977) was considered as one method to determine the sample size as guided by Ishmael Mensah (2015):

$$\frac{n_0 = Z^2pq}{e^2}$$

Here, **n_0** represents the sample size where **Z** is the standard normal deviation at the desired confidence level, **p** is the estimated proportion/ percentage of the sample picking a choice or an attribute being present in the population, **q** is **1-p** and **e** is the desired confidence interval. When the values Z = 1.96 (Z value taken from an Z table for 95% confidence level), p = 0.5, q = 0.5 and e = 0.05 were applied to the formula, it gave an output of **384** as the sample. Also, according to Krejcie and Morgan (1970) as the population increases, it reaches a plateau starting from 100000 members in a population at 384 sample size and remains there.

Roscoe (1975) suggests as a “rule of thumb” that, taking a sample between 30 and 500 is favourable for most studies. Another popular method used by researchers to derive a sample size from populations of which the size is unknown, is to take a sample that is five times as the number of variables that are being analyzed, as a minimum. However, the ideal is said to have a minimum of ten times and sometimes even 20 observations for each of the variables (Hair et al., 2014). On a separate note, having too large sample supports a great amount of generalizability but on the other hand, it “can make the statistical tests overly sensitive” (Hair et al., 2014). When those concepts are applied to this study, it requires **120** respondents as a minimum sample to have a minimum of 20 observations per each variable, as the number of independent variables involved is 6.

Considering the above, it was decided to collect a minimum of **120** responses for the questionnaire instrument.

3.5. Data Collection

As mentioned above, the questionnaire instrument was distributed among the targeted population online via a google form. As it was difficult to reach the wide-spread population, Snowball sampling technique was used to collect the data. Snowball sampling is a non-probability sampling method in which, each respondent would introduce more potential respondents, i.e. accumulating responses (Rubin & Babbie, 2009) thus creating a growing snowball effect. Even though this method was adopted for this quantitative research due to the practical difficulties in locating and reaching the intended population, it is widely used for qualitative research. As the participants are mostly from the same community, there can be bias as well. But, on the other hand, it suited this study well as the purpose was to explore (which is a characteristic of snowball sampling) the opinions of the remote working professionals in the software industry.

4. DATA ANALYSIS

The observations, detailed analysis and a discussion based on those are presented in this chapter. Data preparation was done including reliability tests before the analysis. The descriptive analysis backed by a short qualitative analysis supported in giving some interesting insights into the sample's expectation in an ISP.

4.1. Data Preparation

The survey was kept open for approximately a month's time and by the time data collection was closed, 179 responses had been received. The minimum requirement of responses that was required to collect was 120, and therefore, the sample was sufficient in size to carry out the analysis. Microsoft Office Excel and its add-in "Data Analysis" were used as the main tool to analyze the data. Responses for the three sections in the questionnaire instrument were treated separately when preparing data. The column "Timestamp" was removed as it did not have a major impact on the analysis other than to know the timeline. One response row had to be removed as it just contained the timestamp and not any other data, reducing the sample to 178.

Data in the first section were collected mainly to test the hypotheses/ variables, and therefore, were measured on a 6 point Likert scale with options Strongly Disagree, Disagree, Slightly Disagree, Slightly Agree, Agree, and Strongly Agree. This section of the data set was coded so that those options were assigned values 1, 2, 3, 4, 5 and 6 respectively. When calculating certain statistics such as Cronbach's alpha, statistical significance and the likes, the average value for each variable considering related survey item responses was taken into account.

An open-ended optional question was added at the end of the survey to learn more about the perception of the respondents. This part was taken out while preparing data for initial analysis as some of the respondents had skipped it. It was referred to later while coming up with the recommendations. This portion of data was combined with the demographics for the qualitative analysis.

Two sets of data were prepared; one with section 1 (hypothesis related) and section 2 (demographics) data, and section 2 and section 3 (user's point of view) data so it would be convenient to carry out the analysis with reference to the respondents' demographics.

4.1.1. Reliability – Cronbach's Coefficient Alpha

It is important to understand how well the questionnaire instrument used in this study has measured what it is intended to measure. In other words, there needs to be some indicator of the consistency of the survey results. To get an idea about this, Internal Consistency Reliability was estimated using Cronbach's coefficient Alpha.

First, the data set which was on the Likert scale was considered as a whole as it measures the perception of the respondents on information security policies towards productivity. If the Cronbach's Alpha coefficient is greater than 0.7, the data set is believed to be reliable. The Cronbach's Alpha coefficient was found out to be **0.91** which reflects a high level of reliability.

Table 4.1 shows Cronbach's Alpha coefficient calculated for each independent variable.

Table 4. 1: Cronbach's Alpha coefficient for the independent variables

Variable	Cronbach's Alpha coefficient
Relative Increase of Additional Work	0.71
Degree of Priority	0.79
Perceived Level of Complexity	0.7
Negativity of Attitudes	0.7
Perceived Strength of Relationship with Employer	0.73
Level of Awareness	0.71

Table 4.2 shows Cronbach's Alpha coefficient value for the dependent variable.

Table 4. 2: Cronbach's Alpha coefficient for the dependent variable

Variable	Cronbach's Alpha coefficient
Negativity of Perception towards Information Security Policies	0.75

By looking at the values for Alpha coefficient, it could be decided that the results received for the survey are consistent enough to carry out the analysis further. However, there is another argument that higher the Alpha coefficient, more unacceptable is the reliability (Taber, 2018) and may suggest redundancies when it is greater than 0.91 (Tavakol and Dennik, 2011). Therefore, even though the overall value for Cronbach's Alpha coefficient is 0.91 for the received data, another reliability test - Inter-item correlation - which can complement Cronbach's Alpha, was also run.

4.1.2. Reliability – Inter-item Correlation

To assess the reliability and consistency between different questionnaire items that are testing the same variable or the hypothesis further, it was decided to look into the average inter-item correlation. This coefficient is said to be in ideal state if it falls between 0.15 – 0.5; when the value is below this range, they are said to be less associated and when it is above, the items that are measuring the same variable are believed to be repetitious (Clark and Watson, 1995; Glen, 2018).

Section 1 of the questionnaire instrument had 3 items per each variable (independent and dependent) and the average inter-item correlation derived for each of the variables can be found in Tables 4.3 – 4.9.

Table 4. 3: Inter-item correlation for Relative Increase of Additional Work

	Q2	*Q4*	*Q8*
Q2	1		
Q4	0.5	1	
Q8	0.4	0.5	1
Average Inter-item correlation			0.5

Table 4. 4: Inter-item correlation for Degree of Priority

	Q9	*Q16*	*Q21*
Q9	1		
Q16	0.6	1	
Q21	0.5	0.5	1
Average inter-item correlation			0.6

Table 4. 5: Inter-item correlation for Perceived Level of Complexity

	Q5	*Q7*	*Q18*
Q5	1		
Q7	0.4	1	
Q18	0.4	0.5	1
Average inter-item correlation			0.4

Table 4. 6: Inter-item correlation for Negativity of Attitudes

	Q1	*Q14*	*Q15*
Q1	1		
Q14	0.4	1	
Q15	0.4	0.6	1
Average inter-item correlation			0.5

Table 4. 7: Inter-item correlation for Perceived Strength of Relationship with Employer

	Q10	*Q17*	*Q20*
Q10	1		
Q17	0.5	1	
Q20	0.4	0.5	1
Average inter-item correlation			0.5

Table 4. 8: Inter-item correlation for Level of Awareness

	Q3	*Q6*	*Q11*
Q3	1		
Q6	0.5	1	
Q11	0.4	0.4	1
Average inter-item correlation			0.5

Table 4. 9: Inter-item correlation for Negativity of Perception towards Information Security Policies

	Q12	*Q13*	*Q19*
Q12	1		
Q13	0.6	1	
Q19	0.4	0.5	1
Average inter-item correlation			0.5

The values for average inter-item correlation for all the variables except for the variable Degree of Priority are falling in the ideal range. Although the value (0.6) is greater than 0.5, as it is not much deviated from the borderline and as the Cronbach's Alpha is also in a desirable level for the same variable (0.79), it was decided to proceed with the rest of the analysis concluding that the dataset is reliable enough.

4.2. Descriptive Analysis

This section describes and summarizes the data from the survey in a meaningful way. It identifies patterns and features of data while presenting the findings in tabular and graphical form. The most important findings are stated in this chapter; Appendix C contains additional data related to Descriptive Analysis.

4.2.1. Age

The set of respondents consisted of a majority of professionals who are middle-aged or close to middle age.

Figure 4.1 shows the age-wise composition of the sample. It shows that the majority of respondents are aged from 25 years to 40 years.

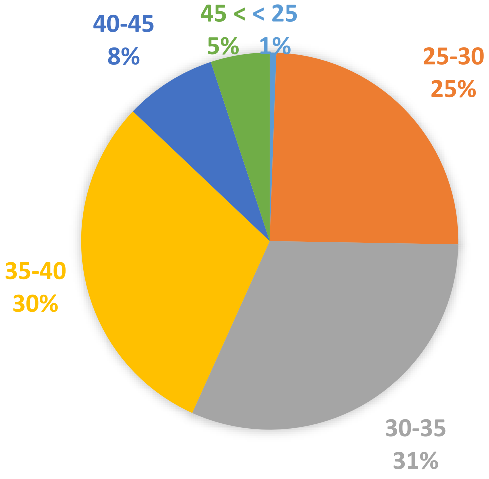


Figure 4. 1: Age-wise composition of the sample

The age distribution seems to be slightly right-skewed as seen in Figure 4.2; i.e. age-wise, the sample does not seem to have a normal distribution. But when the skewness was calculated, it turned out to be -0.01 suggesting a slight left (negative) skewness. This distribution has a sample mean of 35.4 and the median is 44, which corresponds to a respondent in 25-30 year category. Mode, which is 56 respondents falls in age category 30-35 years.

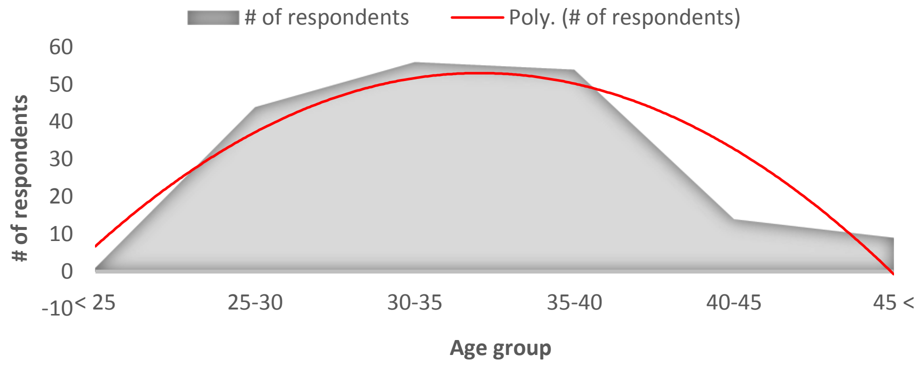


Figure 4. 2: Age-distribution of the sample

However, as age is not being considered as a factor affecting the perception, the distribution being asymmetrical does not have a major impact on the survey results. On the other hand, skewness between -2 and +2 is said to be acceptable to suggest a normal univariate distribution (George & Mallery, 2010; Gravetter & Wallnau, 2014; Trochim & Donnelly, 2006).

4.2.2. Geographical Location

When it comes to geographical location (Figure 4.3), Asian respondents contribute to the majority of the sample being 79% of them and African respondents have made the lowest contribution by being 1% of the sample. The geographical location may have an impact on the overall survey result as these locations can be using different technologies in information security controls, having divergent views on remote working and making judgements based on disparate cultural and attitudinal aspects. It could be argued that the sample is biased in a way. However, as this study focuses on a first generic look, there is room for future studies focusing on these geographical regions.

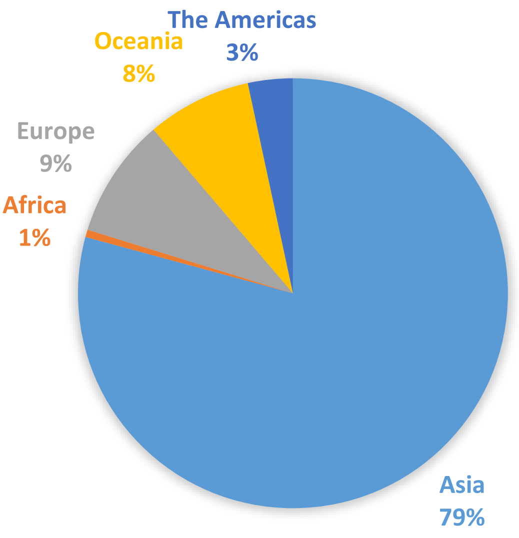


Figure 4. 3: Distribution of respondents according to geographical location

This was further analyzed taking the averages for each question per each area to understand the pattern. Figure 4.3.1 shows how the participants from different areas responded to each question.

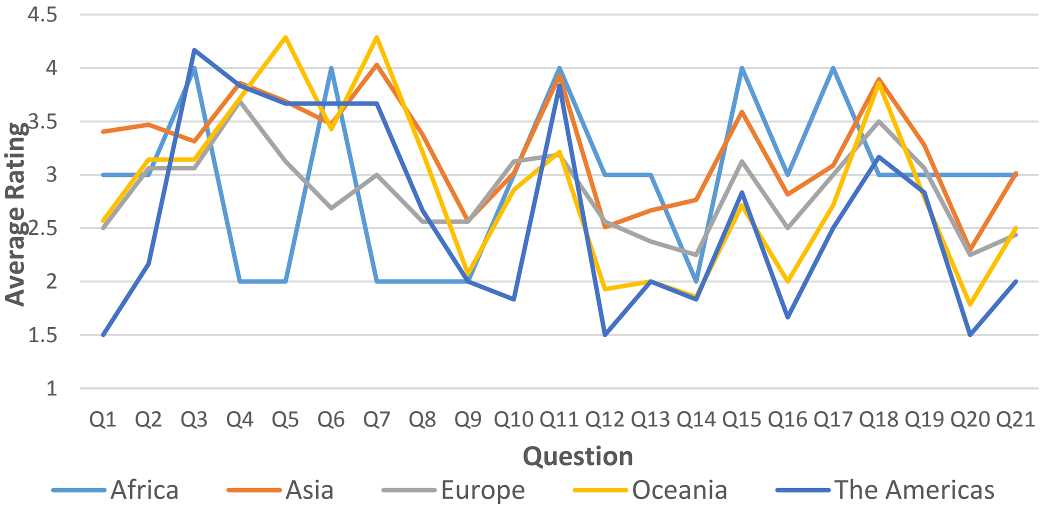


Figure 4.3. 1: Pattern of Responses for Each Question According to Region

The pattern of responding to questions seem to be consistent with a little variation in most cases as seen in Figure 4.3.1 with only a few variations mostly related to data from African and American regions which may be fallouts of lower volumes of responses or may be due to an effect of PESTEL factors. For example, Africa goes away from the pattern in questions 4, 5, 6, 7 and 8, and again at 7, 18 and 20; which account to the variables Relative Increase of Additional Work, Perceived Level of Complexity, Perceived Strength of Relationship with Employer and Level of Awareness. Oceania deviates in one instance at question 5 and The Americas deviate at question 10 which are related to Perceived Level of Complexity and Perceived Strength of Relationship with Employer, respectively. Europe deviates at question 9 and 13, which tested the variables Degree of Priority and Negativity of Perception towards Information Security Policies. However, the almost-consistent pattern suggests that the results may be able to be generalized globally although the results may be more relevant to Asia.

4.2.3. Nature of Service

Nature of Service of the participants of the survey was checked in three categories; the service category - to identify whether the respondents are performing managerial tasks or not, type of work – to see what type of work they are doing when working from remote locations and type of organization – to learn whether the respondents are working in private, government or semi-government companies.

Service Category

When considering the nature of the service provided by the respondents in the sample, the professionals who are performing managerial tasks contribute to one-third of it. Figure 4.4 shows the difference between the two categories.

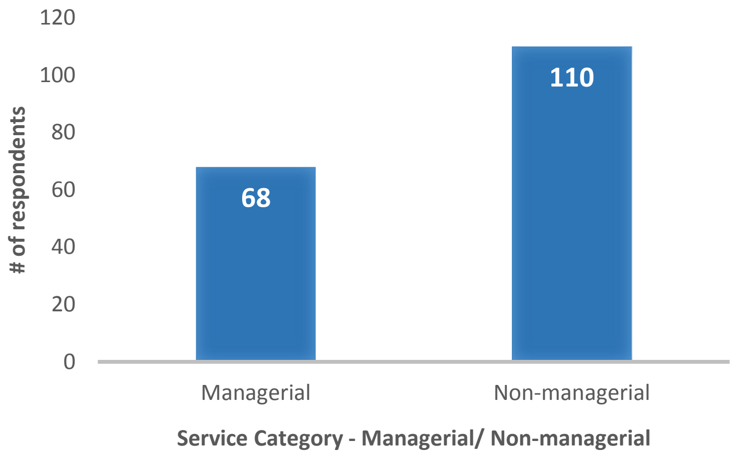


Figure 4. 4: Sample Composition according to Service Category

It is an obvious fact due to various considerations such as the cost differences, etc. that the organizational structure comes as a pyramid (organizational pyramid) according to Cassidy, Kreitner and VanHuss (2014) and managers are lesser in numbers when compared to the non-managerial workers; therefore, this sample can be considered as well-received from both the categories. The point of views of both these parties would be analyzed in a later section.

How these two categories have responded to various improvement-suggestions will be discussed under sub-section “4.2.5 Points for Improvement”.

Type of work

The sample comprised of various categories of the type of work/ tasks the professionals performed. Software development contributed to the majority with 41% whereas IT services and software quality assurance contributed in second place in equal portions (Figure 4.5). The mix of respondents with regard to Type of Work seems to be justifiable.

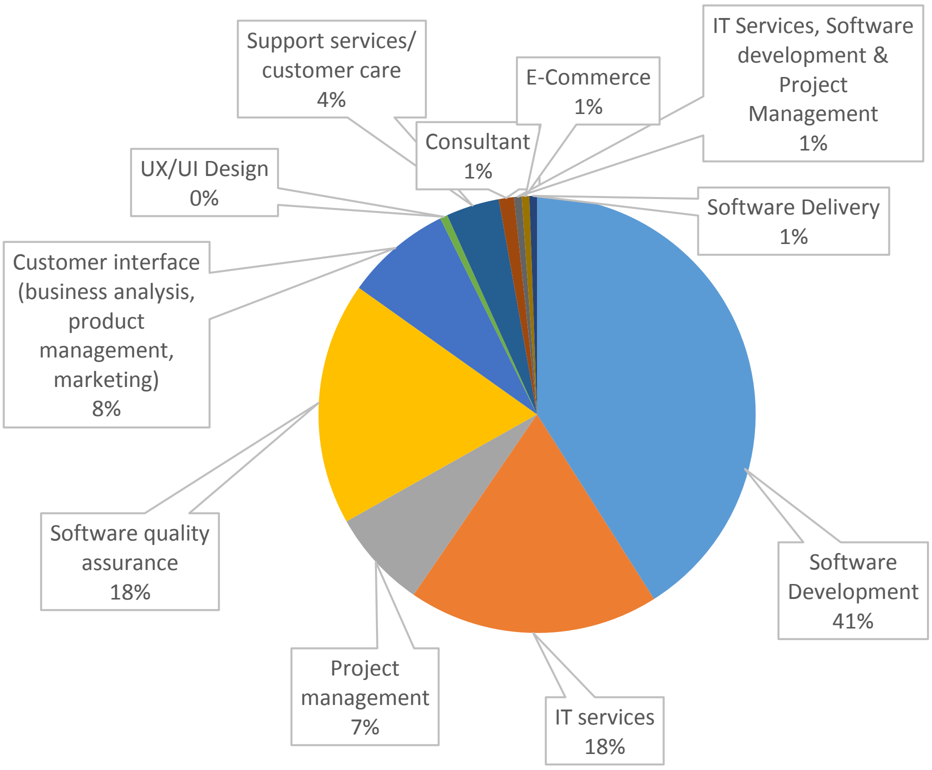


Figure 4. 5: Sample Composition according to Type of Work

Type of organization

It was measured to find out what the type of organization of the respondent is. The most part of the sample was consisting of private sector employees. Therefore, it could be concluded that there is room for future work considering the government and semi-government sector employees.

Figure 4.6 depicts the composition of the sample with regard to the type of organization.

The composition of the respondents is mainly coming from the private sector at 95%. Therefore, when it comes to generalizing the derived results, they can be mostly applied for the private sector.

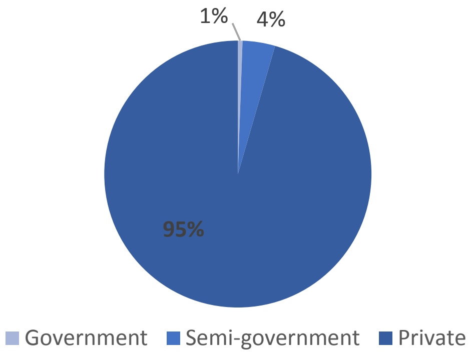


Figure 4. 6: Sample Composition according to Type of Organization

4.2.4. Remote-work Location

When it comes to the location from where the respondents in the sample used to work, some had mentioned that they use multiple types of locations. Therefore, data was processed to reflect the differences of numbers for each type of location. Figure 4.7 shows those variances in the location the sample use to work.

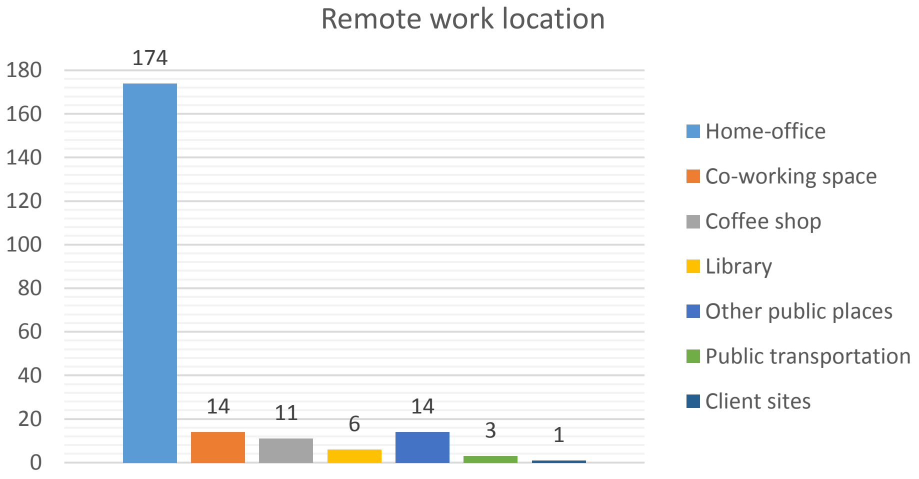


Figure 4. 7: Sample Composition according to Remote Work Locations

If the most-popular location – Home-office – is kept aside, then the popularity is distributed almost equally among co-working spaces, coffee shops and other public places. This important fact alerts to take necessary actions. These places are such that freedom is a basic and an essential element; being negligent on security may cause serious issues at such places.

4.2.5. Points for Improvement

A high-level test was done to learn more about how the respondents in the sample would accept some popular procedures to avoid information security breaches that take place when working from a remote location.

The following were included as the procedures:

- Having a proper, secured area for work when we work away from the company premises, helps to secure the sensitive information.

- Even though we have to log in from time to time, automatically disconnecting idle sessions after a time-out by the system makes it trouble-free when we work from a public area.

- When considering the security threats that connecting to a public Wi-Fi can pose, I think it is correct to restrict such when working remote. We should connect only via trusted Wi-Fi.

- A remote worker monitoring system would help to identify any malicious activities even though it monitors all our activities.

- We should be mindful to maintain up-to-date devices and software with regard to anti-viruses, firmware, etc. when we connect to company network from outside because it helps to reduce vulnerabilities.

- We should try to avoid connecting the devices we use to access company network to IoT devices at all times as we cannot make sure how vulnerable or not they are.

- In my opinion, our information security policy should have separate clauses to treat the devices we use to access company network that are company-owned and that are not (e.g. employee's own devices).

- Usage of mechanisms such as Data Leakage Prevention and Hashing to avoid information security breaches is an absolute necessity.

Figure 4.8 depicts the results on how the participants have responded to the question by selecting the given options.

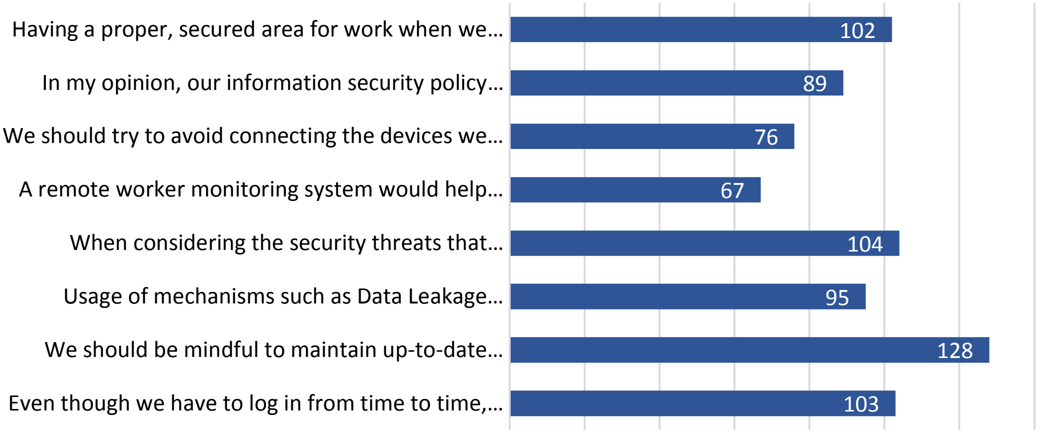


Figure 4. 8: How Respondents Approved of Points to Improve the ISP Suggested by the Researcher

The majority of the sample (71.9%) agrees that maintaining up-to-date software and devices is essential. Despite of the facts related to outside environment (avoiding connections with public Wi-Fi – 58.4%, using a proper secured area for remote work – 57.3%) and inside environment with regard to the systems (automatically disconnecting idle sessions – 57.9%, usage of certain mechanisms – 53.4%), surprisingly, more than one third of the sample (37.6%) is agreeing that there should be employee monitoring systems for remote workers. Generally, employees in the software industry perform diverse tasks rather than performing repetitive tasks. In such situations, employee monitoring can affect employee performance in a negative way (Stanton, 2000) creating resistance and it may lead to dissatisfaction. Therefore, the monitoring should be done at a tolerable level.

However, it was interesting to see that the majority of the respondents who agreed that employee monitoring is good to have when remote working was the participants who are in the non-managerial category. Figure 4.9 contains the related ratios which show that approximately two-thirds of the respondents are the remote workers who are not performing managerial tasks.

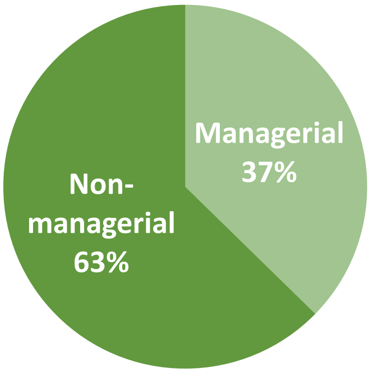


Figure 4. 9: Employee Monitoring Preference according to Service Category

4.2.6. Perception

Section 1 of the questionnaire contained questions to test each of the variables to capture the perception of the software professional on how the information security policies affecting their productivity. These questions were on a 6 point Likert scale from Strongly Disagree (value = 1) to Strongly Agree (value = 6). It was analyzed how the participants in the survey have responded to each question based on each variable.

Relative Increase of Additional Work

The variable "Relative Increase of Additional Work" was measured using questions 2, 4 and 8 in section 1 of the questionnaire instrument.

Question 2 was read as "*Information security policy forces us to follow so many procedures before getting a thing done when we work from outside no matter if the device we use is provided by the company. This keeps us waiting and our time is wasted.*" which received responses almost equally agreeing and disagreeing to the statement. 8.43% of the sample strongly disagreed to the statement while 31.46% disagreed being the majority, 8.99% slightly disagreed, 22.47% slightly agreed, 24.16% agreed and 4.49% strongly agreed. When looked at in another perspective, it was 48.88% disagreeing and 51.12% agreeing to the fact that there are additional procedures and work created by the ISP. The mean was 3.36 for this item which shows a tendency towards agreeing.

Question 4, "Having to follow the information security policy when working remote sometimes creates additional administrative procedures (e.g. going through certain procedures to gain privileges) to follow. This results in productivity drops." was responded with a mean of 3.82 and with 3.93% strongly disagreeing, 21.91% disagreeing, 8.99% slightly disagreeing, 23.03% slightly agreeing, 37.64% agreeing (majority) and 4.49% strongly agreeing. Altogether, that is 65.17% agreeing and 34.83% disagreeing that additional administrative procedures generated by the information security policy as a reason for productivity drops.

"My daily output is negatively affected while remote-working by having to stick to Information security policy, as it requires us to adhere to a lot of technical matter that take additional time apart from actual work such as using multi-factor authentication, using VPN to log in, resetting passwords frequently, limited usage of single sign-on capabilities, etc., even if I use my own PC." was Question 8 and it was focusing on additional work coming from information security policy in a technical aspect. When mean was considered, it came out as 3.26. The percentages of responses in the scale from Strongly Disagree to Strongly Agree to this question were 8.99%, 30.9%, 13.48%, 22.47%, 20.22% and 3.93% respectively. This shows a majority voting as disagreed. In total, 53.37% of the survey participants have disagreed on the fact that the technical actions taken as a part of the information security policy are creating a productivity hit while 46.63% have agreed on it. This makes almost equal proportions to agree and disagree with the statement.

Table 4.10 shows a summary of the details discussed above with regard to the questions that tested the variable Relative Increase of Additional Work.

Table 4. 10: Summary of Findings from Descriptive Statistics – Relative increase of additional work

Aspect	Q2 – policy creates additional work	Q4 – additional admin procedures	Q8 – additional technical actions
Majority's choice from the scale (Mode)	Disagree	Agree	Disagree
Collectively agreed/ disagreed?	2% of the sample agreeing than who are disagreeing	30% more participants agreeing than disagreeing	6% more participants disagreeing

The figures from Table 4.10 show that when it comes to additional work created by the information security policy, the sample agrees that policy creates additional work and admin procedures but disagrees that the additional technical actions are contributing to inefficiencies.

Degree of Priority

Questions 9, 16, 21 of section 1 of the questionnaire were used to test the independent variable *Degree of Priority*.

Observations for question 9 which was read as "My immediate management/ team leads/ supervisors instruct to increase productivity while working remote. Therefore, I take "shortcuts" and avoid the information security policy in situations when I feel that following it hits productivity badly.", collectively disagreed at 74% while the agreed percentage was 26% implying that the respondents do not take “shortcuts” to improve productivity while ignoring information security policy. This comprised 22.47% strongly disagreeing, 43.82% disagreeing, 7.3% slightly disagreeing, 14.61% slightly agreeing, 10.67 agreeing and 1.12% strongly agreeing. The mean was 2.5.

Question 16 was “Even though we’re supposed to adhere to the information security policy whenever we connect to the company network from outside, I sometimes ignore it to keep me productive.”. It received responses as strongly disagreed 17.98%, disagreed 41.01%, slightly disagreed 10.67%, slightly agreed 16.85%, agreed 11.8% and strongly agreed 1.69%. These amounts summed to 70% disagreeing and 30% agreeing. This shows that the respondents do not ignore adhering to the information security policy while connecting from remote locations.

“If the organization does not make it clear on what should be given more priority when remote working; whether it is following the information security policy or ensuring productivity, or to balance the both, I get confused. This only makes me struggle and being inefficient without knowing what to do.” was question 21. To this, 66% of the respondents disagreed while 34% agreed, making that composition by 12.92% strongly disagreeing, 39.89% disagreeing, 12.92% slightly disagreeing, 15.17% slightly agreeing, 17.98% agreeing and 1.12% strongly agreeing. The mean was 2.89. This hints that the organization’s priorities and directions do not have a major effect on making the participants in the survey inefficient. On the other hand, approximately one-quarter of the participants have the perception that the organizational and managerial priorities have a negative impact on productivity when working from remote locations.

A summary of the details discussed above is shown in Table 4.11 from which it is clear that the tendency is towards disagreeing.

This was further analyzed separately for participants involved in managerial and non-managerial work. The final outcome did not vary from the initial analysis, however, it could be observed that the managerial workers disagreed in larger proportions than the non-managerial workers to the statement that the priorities of the organization and management affected productivity when remote-working. Table 4.12 depicts those results that were retrieved from the above analysis.

Table 4. 11: Summary of Findings from Descriptive Statistics – Degree of priority

Aspect	Q9 – taking "shortcuts"	Q16 – ignoring policy	Q21 – confusion due to varying priorities
Majority's choice from the scale (Mode)	Disagree	Disagree	Disagree
Collectively agreed/ disagreed?	48% more of the sample disagreeing than who are agreeing	40% more participants disagreeing than agreeing	32% more participants disagreeing than agreeing

Table 4. 12: Descriptive Statistics of Degree of Priority according to Service Category

Question	Managerial			Non-managerial		
	Mean	Disagreeing	Agreeing	Mean	Disagreeing	Agreeing
Q9 – taking "shortcuts"	2.38	78%	22%	2.58	69%	31%
Q16 – ignoring policy	2.47	75%	25%	2.82	65%	35%
Q21 – confusion due to varying priorities	2.69	71%	29%	3	60%	40%

Perceived Level of Complexity

In order to test the independent variable *Perceived Level of Complexity*, questions 5, 7, 18 were included in questionnaire section 1.

Question 5, "I have to understand and acquire knowledge on certain technical and/or non-technical procedures (for example: using VPN to access the network) required by information security policy when connecting to the company network from a location away from office premises. This is tough at times resulting in inefficiencies." was responded by the sample by 58% collectively agreeing that having to gain prior knowledge to follow the procedures mentioned in the information security policy from remote locations causes inefficiencies and 42% collectively disagreeing. These figures were made up of 2.25% strongly disagreeing, 28.09% disagreeing, 11.24% slightly disagreeing, 21.91% slightly agreeing, 31.46% agreeing and 5.06% strongly agreeing. The mean was 3.67.

As for question 7, the respondents were asked their opinion on the statement, "I sometimes face difficulties when working remote due to the restrictions/ limitations/ procedures imposed by the information security policy.". The responses came out as 4.49% strongly disagreeing, 16.85% disagreeing, 8.43% slightly disagreeing, 29.21% slightly agreeing, 33.15% agreeing, 7.87% strongly agreeing; contributing to collective figures of 30% disagreeing and 70% agreeing to the fact that the limitations imposed by information security policy creating issues. The mean in this data set was 3.93.

Question 18 was "When working from a remote location, it is difficult to get problems solved quickly if we stick to the information security policy.". With this statement, 3.93% strongly disagreed, 20.22% disagreed, 10.67% slightly disagreed, 28.09% slightly agreed, 28.65% agreed, 8.43% strongly agreed, resulting in collective percentages of disagreed 35% and agreed 65% while having a mean of 3.83. In other words, the majority of the sample perceives that when adhering to information security policy, there is a waiting time to get problems solved.

Table 4.13 depicts a summary of the results received for questions related to independent variable Perceived Level of Complexity.

These figures indicate that there is a large contribution from the level of complexity of following an information security policy to perceive it as a factor affecting the productivity of people working from remote locations.

Table 4. 13: Summary of Findings from Descriptive Statistics – Perceived level of complexity

Aspect	Q5 – understanding procedures	Q7 – limitations	Q18 – time to solve problems
Majority's choice from the scale (Mode)	Agree	Agree	Agree
Collectively agreed/ disagreed?	6% more of the sample agreeing than who are disagreeing	40% more participants agreeing than disagreeing	30% more participants agreeing than disagreeing

Negativity of Attitudes

Questionnaire section 1 contained questions 1, 14, 15 to test the independent variable *Negativity of Attitudes*.

Question 1 was read as, "If productivity is a major concern, we should not be pressurized to follow policies, procedures and guidelines as they may cause serious productivity hits, especially when remote-working.". While 54% of the respondents disagreed with the statement showing a positive attitude, 46% agreed. The breakdown of these values was 15.17% strongly disagree, 28.09% disagree, 11.24% slightly disagree, 21.35% slightly agree, 16.29% agree and 7.87% strongly agree. The mean was 3.19.

Question 14, "In the past, information security policies have had affected in productivity losses. Because of that, I don't like to follow those when remote-working." received a mean of 3.61 with amalgamated figures of 75% disagreeing and 25% agreeing again showing a positive attitude and indicating that past experiences have less impact on creating a negative attitude towards following information security policy. When calculated separately according to the scale, there were 12.92% strongly disagreeing, 50.56% disagreeing, 11.24% slightly disagreeing while 14.61% slightly agreeing, 8.99% agreeing and 1.69% strongly agreeing.

Question 15 was, "Having to change the way we work according to the changes in information security policy all the time is something that I don't like.". While the mean was at 3.46, there were 6.18% strongly disagreeing, 29.78% disagreeing, 8.99% slightly disagreeing, 25.28% slightly agreeing, 26.97% agreeing, 2.81% strongly agreeing observations. When consolidated, the percentages went up to 45% disagreeing and 55% agreeing to the statement indicating that the effects of resistance to change can have a negative impact on the perception of information security policy.

Table 4.14 contains a summary of the results discussed above for the questions testing the independent variable Negativity of attitudes.

Table 4. 14: Summary of Findings from Descriptive Statistics – Negativity of attitudes

Aspect	Q1 – attitude towards policies	Q14 – past experience contributing to attitudes	Q15 – attitudes towards change
Majority's choice from the scale (Mode)	Disagree	Disagree	Disagree
Collectively agreed/ disagreed?	8% more of the sample disagreeing than who are agreeing	50% more participants disagreeing than agreeing	10% more participants agreeing than disagreeing

Surprisingly, the sample does not seem to have a negative perception towards ISP as a result of past experiences. However, the attitudes towards "change" can have an impact on perception.

Perceived strength of relationship with employer

The independent variable *Perceived strength of relationship with employer* was tested using questions 10, 17, 20 in section 1 of the questionnaire.

Question 10 in section 1 of the questionnaire was, "I sometimes have the suspicion that the organization sets up an information security policy just because the employees cannot be trusted when they are away from office.”. The sample had responded to this question with a mean value 2.97 as; 14.04% strongly disagreeing, 37.64% disagreeing, 10.67% slightly disagreeing, 15.17% slightly agreeing, 19.66% agreeing, 2.81% strongly agreeing, summing up to 62% disagreeing and 38% agreeing. This indicates that the majority of sample perceives that an information security policy is not set up just because the management cannot trust the employees who connect from remote locations.

Question 17 read, “The information security policy gives the impression that, the company doesn’t believe the fact that we’re taking necessary precautions to not to expose sensitive data when we work remotely.” and received a collective figure of 60% disagreeing while 40% agreed to it. This implies that the majority of the sample does not have a negative perception towards information security policy doubting about the trust they think their organization has on them. The breakdown of these amounts showed, strongly disagreed 12.36%, disagreed 35.96%, slightly disagreed 11.8%, slightly agreed 16.85%, agreed 21.91% and strongly agreed 1.12% with a mean value of 3.03.

“An information security policy is not required if the management has good faith in the employees.” was put forward as question 20, which observed a mean of 2.23 and 35.96% strongly disagreeing to the statement while 38.2% disagreeing, 7.87% slightly disagreeing, 6.18% slightly agreeing, 8.43% agreeing and 3.37% strongly agreeing. When these were summed up, 82% of the sample were disagreeing to the statement indicating that negative perception towards information security policy is less likely to be generated by issues in trust whereas 18% were agreeing.

Table 4.15 summarizes the facts discussed above in relation to the results received for tests on Perceived Strength of Relationship with the Employer.

By looking at the figures Table 4.15, it can be argued that the strength of the relationship between the employee and the organization does not seem to play a major role in creating a negative perception on the ISP.

Table 4. 15: Summary of Findings from Descriptive Statistics – Perceived strength of relationship with the employer

Aspect	Q10 – doubts due to weak relationship	Q17 – perceived trust on taking precautions	Q20 – perceived trust on the employees in general
Majority's choice from the scale (Mode)	Disagree	Disagree	Disagree
Collectively agreed/ disagreed?	24% more of the sample disagreeing than who are agreeing	20% more participants disagreeing than agreeing	64% more participants disagreeing than agreeing

Level of Awareness

Section 1 of the questionnaire contained questions 3, 6, 11 to test the independent variable *Level of Awareness*.

Question 3, "My organization doesn't clearly communicate the additions/ changes to the policies on time. Therefore, it's not easy to be productive while following the same because we don't have all the details about it." was observed as 52% disagreeing and 48% agreeing. The segregated figures show, strongly disagreed 8.99%, disagreed 30.9%, slightly disagreed 12.36%, slightly agreed 19.66%, agreed 24.16% and strongly agreed 3.93%. The mean was 3.31. The almost equal percentages who agreed and disagreed shows that on-time communications can have an impact on perception towards information security policy as a factor affecting productivity.

Question 6, "Because my organization doesn't provide adequate trainings/ instructions on preventive actions to safeguard information security when working from remote locations it is difficult and time-consuming to get rid of inefficiencies that are created by various limitations in the information security policy." was received as 6.18% strongly disagreeing, 28.65% disagreeing, 13.48% slightly disagreeing, 24.72% slightly agreeing, 23.6% agreeing, 3.37% strongly agreeing to make 48% of the sample disagreeing to the statement whereas 52% of the sample agreeing to it. This had a mean value of 3.41.

Question 11, "When I come to think of it, the fact that our company does not have trust on us even though we do not expose sensitive data when we remote-work, has created a disappointment in me and has resulted in decreasing my productivity." looked at the general awareness of the requirement of a security policy with 3.93% strongly disagreeing, 24.72% disagreeing, 6.18% slightly disagreeing, 23.6% slightly agreeing, 35.39% agreeing and 6.18% strongly agreeing with a mean 3.8. When consolidated, 35% of the sample was disagreeing to the statement while 65% was agreeing.

A summary of the figures discussed above with regard to descriptive statistics associated with the independent variable Level of Awareness is depicted in Table 4.16.

Table 4. 16: Summary of Findings from Descriptive Statistics – Level of awareness

Aspect	Q3 – on-time communication	Q6 – organization making awareness	Q11 – general awareness of the necessity
Majority's choice from the scale (Mode)	Disagree	Disagree	Agree
Collectively agreed/ disagreed?	4% more of the sample disagreeing than who are agreeing	4% more participants agreeing than disagreeing	35% more participants agreeing than disagreeing

The details direct to the conclusion that communication and awareness about the information security policy is an important factor in making remote workers perceive the policy as a trouble-maker when it comes to productivity.

Negativity of Perception towards Information Security Policies

The dependent variable "*Negativity of Perception towards Information Security Policies*" was measured using questions 12, 13, 19 in section 1 of the questionnaire.

Question 12 was read as, “I don’t see a justifiable reason to follow an information security policy when connecting to the company network from a remote location. It only makes life difficult.”. It was observed that 24.16% strongly disagreed to the statement whereas 44.38% disagreed, 8.43% slightly disagreed, 10.67% slightly agreed, 11.24% agreed and 1.12% strongly agreed to make the collective amounts as 77% disagreed and 23% agreed with a mean of 2.44.

Question 13, “The time-to-time changes in the information security policy are a headache and not communicating them properly affects productivity negatively as we don’t know all the specifics about the procedures.” received a mean value 2.57 along with 18.54% strongly disagree, 43.82% disagree, 11.8% slightly disagree, 15.17% slightly agree, 9.55% agree, 1.12% strongly agree, summing them up to 74% disagree and 26% agree.

“In my opinion, having to adhere to any policy causes delays, difficulties, etc.. Inefficiencies can emerge because of this.” was stated as question 19, to which the sample responded as 8.99% strongly disagreeing, 30.34% disagreeing, 17.98% slightly disagreeing, 19.1% slightly agreeing, 21.35% agreeing and 2.25% strongly agreeing. These amounts collectively contributed to 57% disagreeing and 43% agreeing. The mean was 3.2.

Table 4.17 illustrates a summary of the figures discussed above with regard to the questions corresponding to the dependent variable.

Table 4. 17: Summary of Findings from Descriptive Statistics – Negativity of Perception towards Information Security Policies

Aspect	Q12 – negative perception due to difficulties	Q13 – negative perception due to lack of awareness	Q19 – negative perception due to resistance to change
Majority’s choice from the scale (Mode)	Disagree	Disagree	Disagree
Collectively agreed/ disagreed?	54% more of the sample disagreeing than who are agreeing	48% more participants disagreeing than agreeing	14% more participants disagreeing than agreeing

The details do not show that the sample consisted of remote-working software professionals look at having to follow the information security policy as a factor that is affecting productivity inversely.

4.3. Inferential Analysis

For hypothesis testing, the Analysis Tool “Regression” of Data Analysis add-in in Microsoft Excel was used to get the required figures. The output of this test would return the statistical significance (p-value) as *Significance F*, Pearson’s Correlation Coefficient as *Multiple R* and Coefficient of Determination as *R square.* Important input values for the regression model were, values pertaining to dependent variable in Y range, averaged values for independent variables (average of the values for each questionnaire item per variable) as X range and 95% which is commonly used in the social sciences (Craparo, 2007) as Confidence level.

Statistical Significance

As a starting point to test the hypothesis, in order to assess if the statistics derived from the sample is good enough to represent the population as a whole and to determine whether relationships between the variables are results that were occurred out of mere chance, statistical significance was considered for each hypothesis. Here, the convention of considering a result as statistically significant when the p-value (the probability of making an erroneous inference) is less than or equal to the selected significance level (in this case 0.05) was followed.

Scatterplot, Pearson’s Correlation Coefficient and Coefficient of Determination

To determine the direction, as well as the tightness of the association between the independent variable and the dependent variable which are continuous variables, Pearson’s Product-moment Correlation Coefficient/ Pearson’s Correlation and Linear regression were used. Pearson’s Correlation Coefficient may vary from -1 to +1. A coefficient of -1 means a perfect negative correlation and a +1 indicates a perfect positive correlation. It is considered that there is no correlation between the variables if the coefficient equals to 0. In a negatively associated relationship, the value of the dependent variable decreases when the value of the independent variable increases and vice versa which can be explained by a scatterplot with a negative slope (i.e. an inverse relationship). On the other hand, when the correlation coefficient is positive, a scatterplot would contain a positive slope implying that the dependent variable increases when the independent variable increases and vice versa. The scatterplot comes in handy to see if the association is linear, making it an important factor as the correlation applies to linear relationships (Rumsey, 2011). The nature of the data is said to be playing a major role when weighing the strength of the association (Ragin & Amoroso, 2011). The closer the value is to +1 the relationship is reflected to be strong and the closer it is to 0, the correlation is said to be weak (Abbot, 2016). A coefficient between ±0.5 and ±1 is preferred (Rumsey, 2011) and said to indicate a strong association whereas a value between ±0.30 and ±0.49 is of medium strength. If the coefficient is a value below ±0.29, it is considered a weak relationship (Aczel & Sounderpandian, 2009). However, a weak correlation does not suggest zero association (Rumsey, 2011). The Coefficient of Determination denoted by *R square,* which is the proportionate variance of the dependent variable explained by the movements of the independent variable, was also used. This value can fall between 0 - 1 (0% - 100%) and being closer to 1 means that the observations are good enough to represent the population. When there are doubts in the assessments done with the correlation coefficient, coefficient of determination can bring more meaning (Taylor, 1990) to the outcomes.

4.3.1. Hypothesis 1

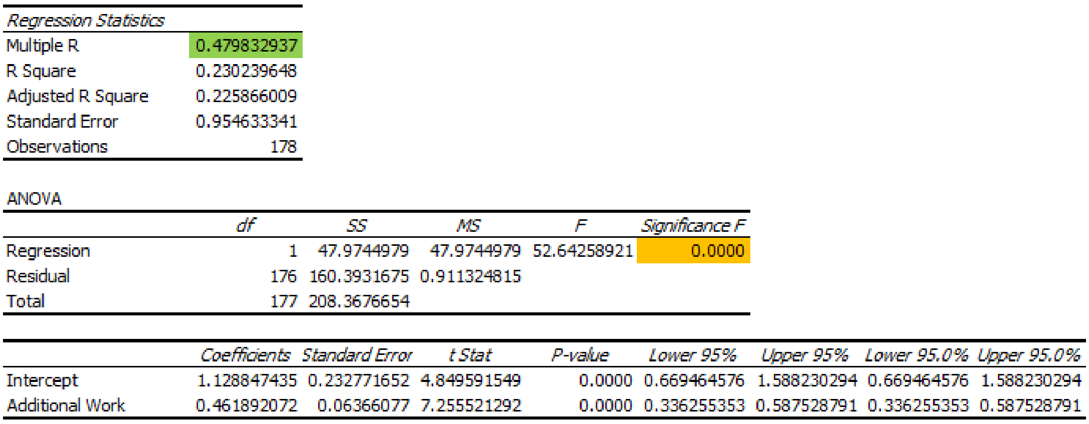
Hypothesis 1 was developed based on the relationship between the independent variable “Relative Increase of Additional Work” (Questions 2, 4, 8 from questionnaire section 1) and the dependent variable "Negativity of Perception towards Information Security Policies".

H1$_{A}$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the relative increase of additional work/ tasks/ procedures created by the information security policy.

H1$_{0}$ – The additional work/ tasks/ procedures created by information security policy has no impact on the remote worker's perception towards the information security policy's influence over productivity in the software industry.

Table 4.18 depicts the statistics derived using regression analysis from Excel when testing Hypothesis 1.

Table 4. 18: Results of the regression test - Hypothesis 1



Regression Statistics	
Multiple R	0.479832937
R Square	0.230239648
Adjusted R Square	0.225866009
Standard Error	0.954633341
Observations	178

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	47.9744979	47.9744979	52.64258921	0.0000
Residual	176	160.3931675	0.911324815		
Total	177	208.3676654			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	1.128847435	0.232771652	4.849591549	0.0000	0.669464576	1.588230294	0.669464576	1.588230294
Additional Work	0.461892072	0.06366077	7.255521292	0.0000	0.336255353	0.587528791	0.336255353	0.587528791

By looking at the reflected values in Table 4.18 it can be said that the relationship between *Relative Increase of Additional Work* and *Negativity of Perception towards Information Security Policies* is significant.

When the values were plotted in a scatter plot, the association could be seen as the Figure 4.10; illustrating that when the relative amount of additional work created by information security policy increases, the negativity of perception also increases, but not in very high proportions.

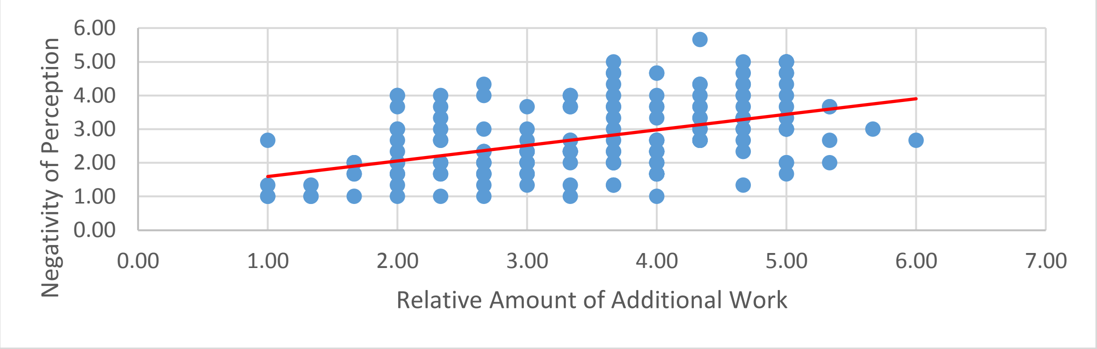


Figure 4. 10: Scatterplot of data points - Hypothesis 1

However, Pearson's Correlation Coefficient being at 0.48, it shows a positive but not very strong association. To further analyze this, Coefficient of Determination was considered. The difference of the independent variable explains a variation of 23% of the dependent variable which cannot be disregarded.

By looking at the above inferential statistics and considering practical significance by looking at the related descriptive statistics, the null hypothesis ($H1_0$) is rejected in favour of alternative hypothesis ($H1_A$). Therefore, it can be stated that the remote working software professional perceives that the relative increase of additional work/ tasks/ procedures created by the ISP as having a negative impact on their productivity.

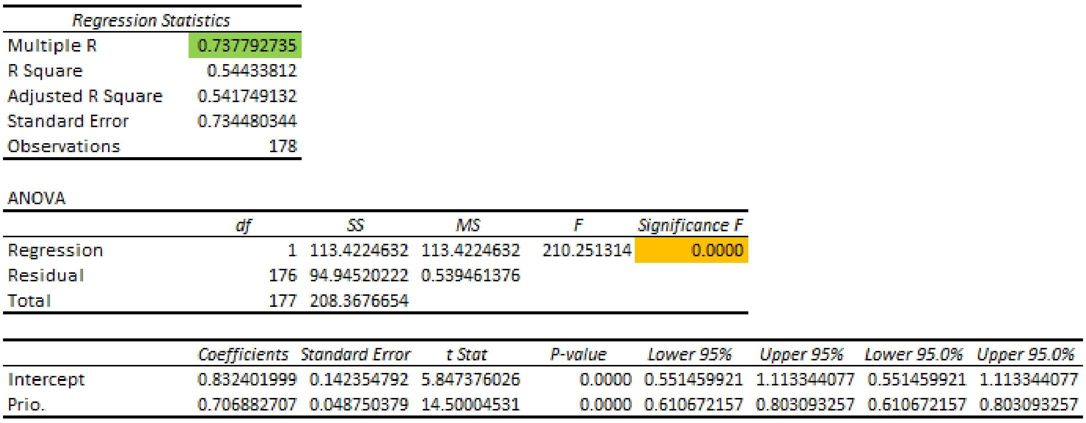
4.3.2. Hypothesis 2

The relationship between the independent variable "Degree of Priority" (Questions 9, 16, 21 of questionnaire section 1) and the dependent variable "Negativity of Perception towards Information Security Policies" was the basis for Hypothesis 2. Table 4.19 represents the regression statistics for this relationship.

H2A – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the priorities set by supervisory and management practices with regard to productivity and information security policy, by creating resistance.

H20 – Priorities set by supervisory and management practices with regard to productivity and information security policy have no impact on the remote worker's perception towards information security policy's influence over productivity in the software industry.

Table 4. 19: Results of the regression test - Hypothesis 2



Regression Statistics	
Multiple R	0.737792735
R Square	0.54433812
Adjusted R Square	0.541749132
Standard Error	0.734480344
Observations	178

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	113.4224632	113.4224632	210.251314	0.0000
Residual	176	94.94520222	0.539461376		
Total	177	208.3676654			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	0.832401999	0.142354792	5.847376026	0.0000	0.551459921	1.113344077	0.551459921	1.113344077
Prio.	0.706882707	0.048750379	14.50004531	0.0000	0.610672157	0.803093257	0.610672157	0.803093257

The statistics show that these two variables have a significant relationship.

The scatterplot for the observations looked like Figure 4.11. It shows a positive linear relationship.

As seen in Table 4.19, these variables display a strong positive correlation at 0.74 and an R squared at 54%.

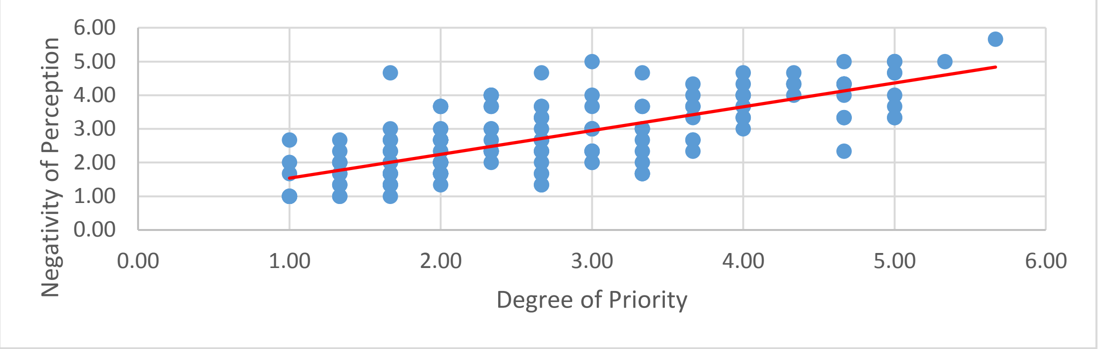


Figure 4. 11: Scatterplot of data points - Hypothesis 2

Considering the facts above, the null hypothesis ($H1_0$) is rejected and the alternative hypothesis ($H1_A$) is substantiated.

4.3.3. Hypothesis 3

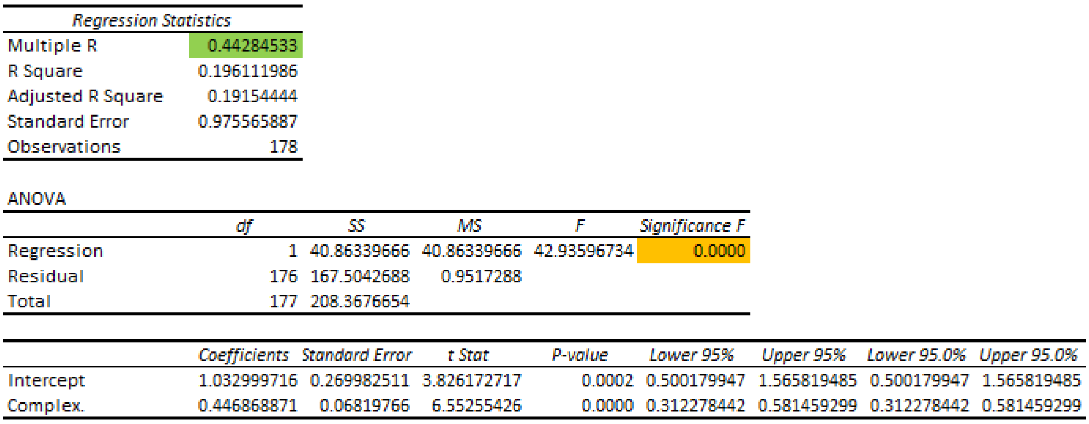
Based on the relationship between independent variable “Perceived Level of Complexity” (questions 5, 7 and 18 in section 1 of the questionnaire) and the dependent variable “Negativity of Perception towards Information Security Policies”, Hypothesis 3 was developed.

$H3_A$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the perceived level of complexity of following the information security policy while working remotely.

$H3_0$ – Perceived level of complexity of following the information security policy while working remote has no impact on the remote worker’s perception towards information security policy’s influence over productivity in the software industry.

Table 4.20 contains the results of the regression test for Hypothesis 3.

Table 4. 20: Results of the regression test - Hypothesis 3



Regression Statistics	
Multiple R	0.44284533
R Square	0.196111986
Adjusted R Square	0.19154444
Standard Error	0.975565887
Observations	178

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	40.86339666	40.86339666	42.93596734	0.0000
Residual	176	167.5042688	0.9517288		
Total	177	208.3676654			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	1.032999716	0.269982511	3.826172717	0.0002	0.500179947	1.565819485	0.500179947	1.565819485
Complex.	0.446868871	0.06819766	6.55255426	0.0000	0.312278442	0.581459299	0.312278442	0.581459299

The two variables considered here are statistically significant according to the details from the regression test.

A scatterplot created with the results is shown in Figure 4.12. It can be seen that the linear relationship is a positive relationship with the data points being dense towards the right side of the scale.

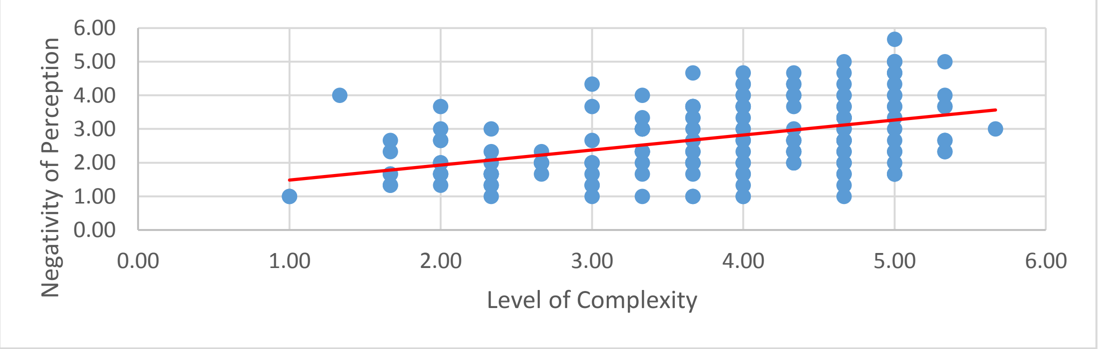


Figure 4. 12: Scatterplot of data points - Hypothesis 3

The regression results show that there is a positive correlation of 0.44 which is a medium strength value. As it is not a very weak relationship, the association of the variables cannot be ignored. On the other hand, Coefficient of determination is at 19.6% showing some variability of the dependent variable according to the movements of the independent variable.

Considering the above facts, the alternative hypothesis ($H3_A$) is substantiated and the null hypothesis ($H3_0$) is rejected.

4.3.4. Hypothesis 4

This hypothesis is based on the relationship between the independent variable "Negativity of Attitudes" (questions 1, 14 and 15 of section 1 in the questionnaire instrument) and the dependent variable "Negativity of Perception towards Information Security Policies".

$H4_A$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the attitudes towards following information security policy while working remotely.

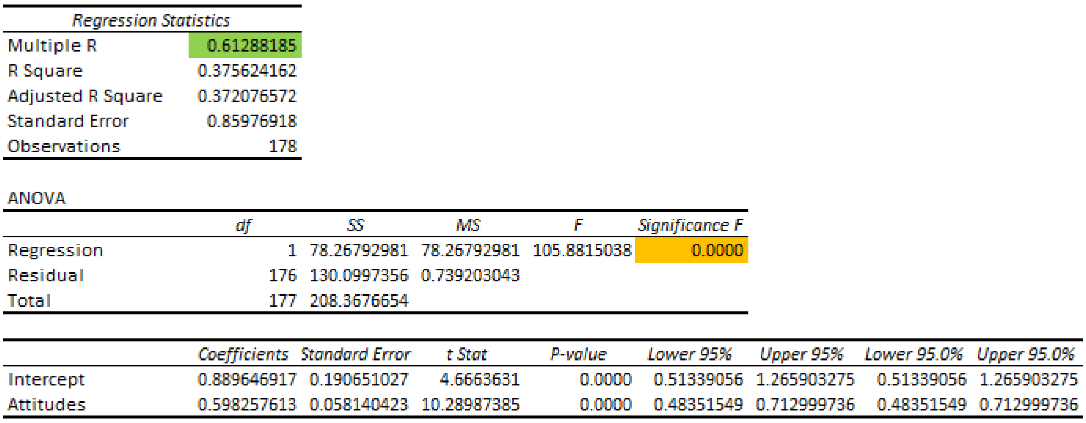
$H4_0$ – Attitudes of the employee towards following the information security policy while working remote has no impact on the remote worker's perception towards information security policy's influence over productivity in the software industry.

Results of the regression test are shown in Table 4.21. As it shows the relationship between the two variables is significant.

The scatterplot of the data points shows a positive linear association between the variables. It is shown in Figure 4.13.

The regression results contain a correlation coefficient of 0.6 and coefficient of determination at 37.6% showing a strong positive relationship.

Table 4. 21: Results of the regression test - Hypothesis 4



Regression Statistics	
Multiple R	0.61288185
R Square	0.375624162
Adjusted R Square	0.372076572
Standard Error	0.85976918
Observations	178

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	78.26792981	78.26792981	105.8815038	0.0000
Residual	176	130.0997356	0.739203043		
Total	177	208.3676654			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	0.889646917	0.190651027	4.6663631	0.0000	0.51339056	1.265903275	0.51339056	1.265903275
Attitudes	0.598257613	0.058140423	10.28987385	0.0000	0.48351549	0.712999736	0.48351549	0.712999736

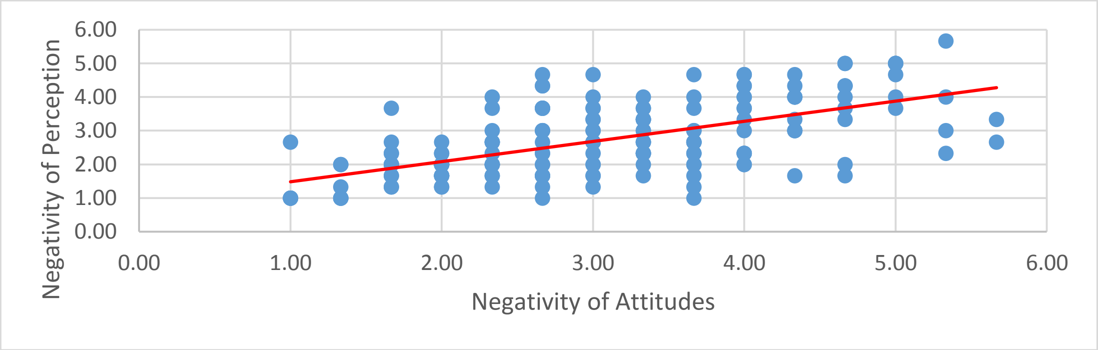


Figure 4. 13: Scatterplot of data points - Hypothesis 4

Taking the above details into account, the null hypothesis ($H4_0$) is rejected in favour of the alternative hypothesis ($H4_A$).

4.3.5. Hypothesis 5

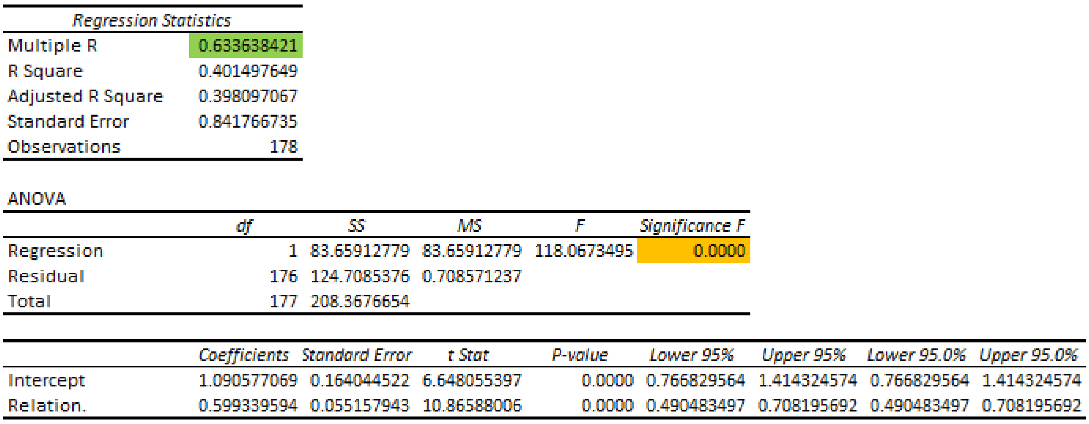
The relationship between the independent variable “Perceived strength of relationship with employer” (questions 10, 17 and 20 from section 1 of the questionnaire) and the dependent variable “Negativity of Perception towards Information Security Policies” was the basis for Hypothesis 5.

H5A – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the employee’s perceived strength of relationship with their management by creating a dissatisfaction.

H50 – Perceived strength of the relationship of the employee with their management has no impact on the remote worker’s perception towards information security policy’s influence over productivity in the software industry.

Results of the regression test for Hypothesis 5 are shown in Table 4.22.

Table 4. 22: Results of the regression test - Hypothesis 5



Regression Statistics	
Multiple R	0.633638421
R Square	0.401497649
Adjusted R Square	0.398097067
Standard Error	0.841766735
Observations	178

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	83.65912779	83.65912779	118.0673495	0.0000
Residual	176	124.7085376	0.708571237		
Total	177	208.3676654			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	1.090577069	0.164044522	6.648055397	0.0000	0.766829564	1.414324574	0.766829564	1.414324574
Relation.	0.599339594	0.055157943	10.86588006	0.0000	0.490483497	0.708195692	0.490483497	0.708195692

The regression results show that these variables have a statistically significant relationship.

Figure 4.14 illustrates the scatterplot of the data points of Negativity of Perception against Perceived Strength of relationship with the Employer which shows a positive linear relationship.

According to the results of the regression test, the relationship has a Pearson’s correlation coefficient of 0.63 which shows that it is a strong relationship and the coefficient of determination shows 40% of the variation of the dependent variable explained by the independent variable.

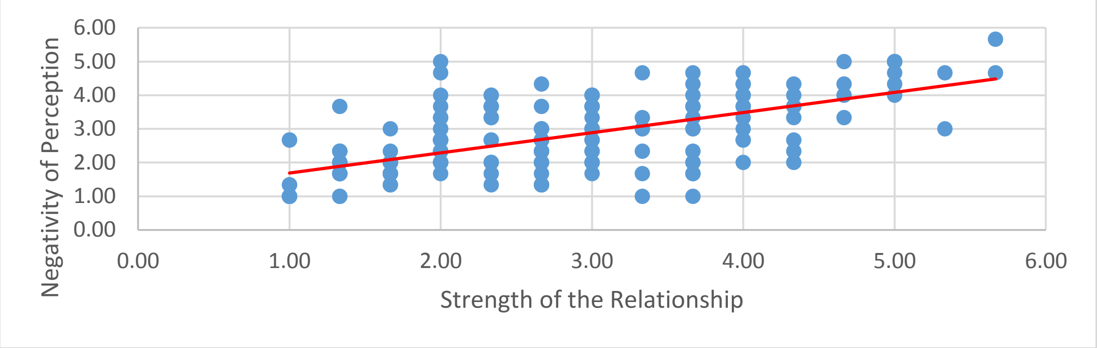


Figure 4. 14: Scatterplot of data points - Hypothesis 5

Due to the inferential statistics gathered, the null hypothesis (H5$_0$) is rejected while the alternative hypothesis (H5$_A$) is substantiated.

4.3.6. Hypothesis 6

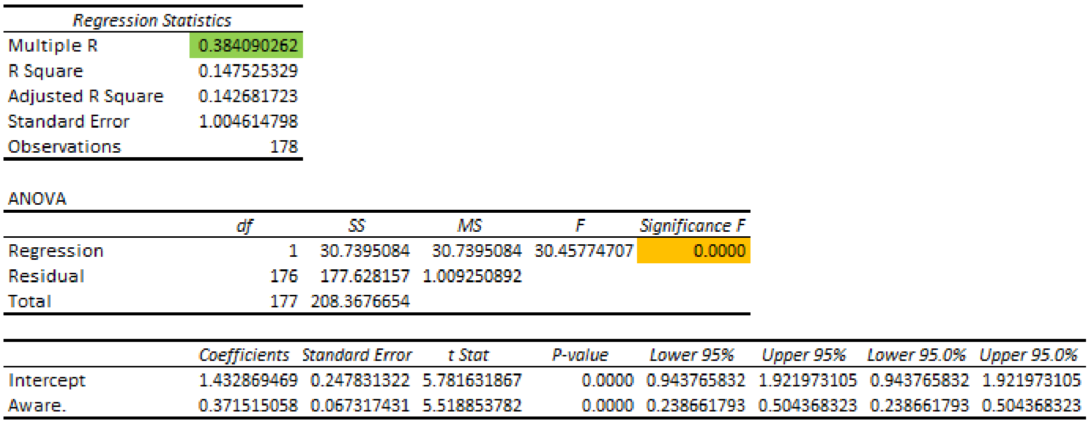
Hypothesis 6 was developed based on the relationship between the independent variable "Level of Awareness" (tested by questions 3, 6, 11) and the dependent variable "Negativity of Perception towards Information Security Policies".

H6$_A$ – Remote working software professional perceives that their productivity of day-to-day work is negatively influenced by the level of awareness with regard to maintaining information security and following information security policy while working remotely.

H6$_0$ – Level of awareness of the employee regarding the importance of following the information security policy while working remote has no impact on the remote worker's perception towards information security policy's influence over productivity in the software industry.

The results of the regression test for Hypothesis 6 are depicted in Table 4.23.

Table 4. 23: Results of the regression test - Hypothesis 6



Regression Statistics	
Multiple R	0.384090262
R Square	0.147525329
Adjusted R Square	0.142681723
Standard Error	1.004614798
Observations	178

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	30.7395084	30.7395084	30.45774707	0.0000
Residual	176	177.628157	1.009250892		
Total	177	208.3676654			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	1.432869469	0.247831322	5.781631867	0.0000	0.943765832	1.921973105	0.943765832	1.921973105
Aware.	0.371515058	0.067317431	5.518853782	0.0000	0.238661793	0.504368323	0.238661793	0.504368323

According to the regression test results, there is a statistically significant relationship between the two variables.

The scatterplot of the data points of the two variables, the dependent variable against the independent variable shows a positive linear relationship as shown in Figure 4.15.

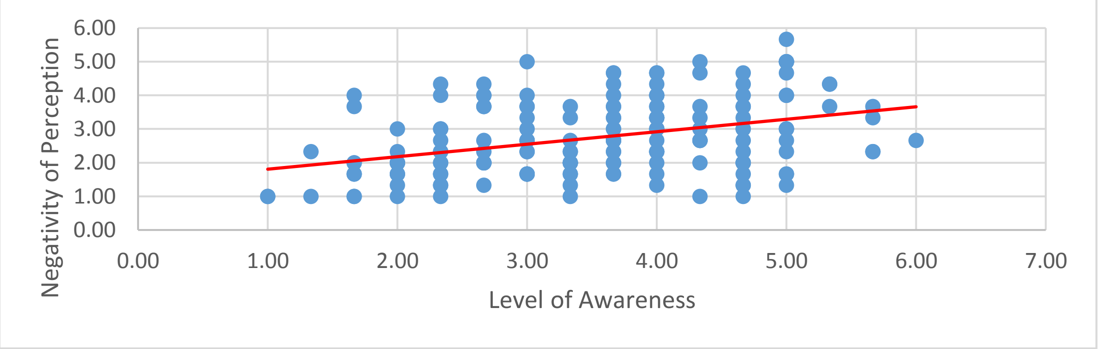


Figure 4. 15: Scatterplot of data points - Hypothesis 6

Having a correlation coefficient of 0.38 which displays an association of medium strength, having only 14.75% variability of dependent variable according to the independent variable, this relationship still can be accepted due to medium strength and practical significance.

Considering the results obtained, the null hypothesis ($H6_0$) is rejected in favour of the alternative hypothesis ($H6_A$).

4.4. Qualitative Analysis

An open-ended optional question was added to the questionnaire instrument to understand what area that the sample would prefer to have improvements in. Although the current study is a quantitative one, the qualitative method of open-coding was deployed to analyze the results received in this section. 62 out of 178 participants had responded to this question and the percentages presented were calculated based on the 62 respondents.

Through open-coding, a few important points were gathered. Table 4.24 depicts a summary of the results obtained by the qualitative analysis (note that the variable names are shortened for the convenience of the reader).

Table 4. 24: Summary of the results obtained by the qualitative analysis of comments given by the respondents

Suggestion derived through Open-coding	Number of Respondents	Matching variable in the present study
A clear, concise, straightforward, simplified policy is required	6	Additional work, Complexities
Organizational culture should be adapted to have mutual understanding within the organization	4	Priorities, Strength of Relationship
Should make awareness on importance, threats, vulnerabilities, best-practices, policy	23	Awareness
Process improvements are required in IT services team and workflows	11	Priorities
Proper policy design and implementation should take place	7	Complexities
Collaboration between the IT team and the remote workers to eliminate issues in policy	3	Complexities
Usage of proper tools/ procedures in securing information is required	16	Complexities

The results show that the majority’s focus has been put to making awareness by 37% out of 62 of the respondents who had made suggestions and the other important factors are the usage of proper tools/ procedures, process improvements and proper policy design and implementation. Figure 4.16 is a graphic representation of the results obtained from open-coding.

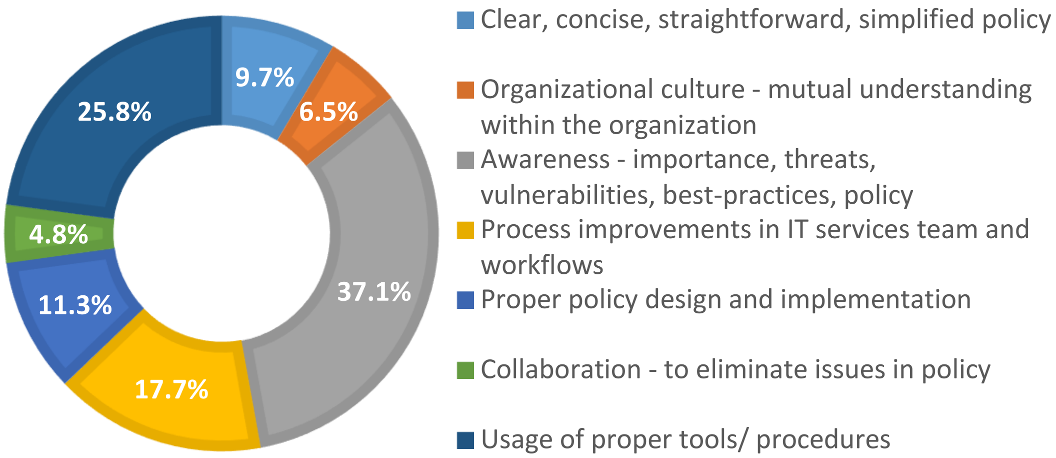


Figure 4. 16: Results Derived through Open-coding of the Comments of the Respondents

By looking at the outcome from qualitative analysis, the following findings can be drawn out:

- 37.1% of the respondents suggesting to take more action on making awareness of the policy, importance of IS, best practices, vulnerabilities and threats, is at the highest percentage. The other high ranking suggestion is optimizing the usage of proper tools and procedures for IS which contributes to 25.8%. This may be due to their opinion that it is more effective as a preventive action or because the organization they work at does not provide the necessary awareness and tools at present.

- A medium level interest has been shown to making process improvements in the IT team and related processes (17.7%), properly designing policy at the beginning and implementing it in proper ways (11.3%), and to creating/ updating a policy so it becomes clear, concise, straightforward and simple (9.7%) encouraging everyone to understand and follow. The respondents may have suggested this because they experience that individuals are not following the policy due to the issues in the processes and policy itself.

- Two human resource related suggestions contribute by lowest level here; creating an organizational culture where there is a mutual understanding between the management and the employees so any policy implementation would run smooth (6.5%) and collaboration between the teams to create an effective policy (4.8%). A lesser number of people may have suggested these may be because most of the respondents do not see the value and the role of the human factor here. All the respondents who have suggested that a mutual understanding should be there, are managers from different regions. The suggestion that got the least amount of voices was having collaboration between the IT team and the remote workers to eliminate issues in policy or to design a user-friendly policy. Only 4.8% of the respondents had suggested this, i.e. three respondents; two of them being in managerial positions and all three being middle-aged Asians (30-45 years), the suggestion cannot be regarded as something that might have done unconsciously.

4.5. Summary and Discussion

Some aspects that can influence the perception of the software professionals towards information security policies as a factor affecting their productivity when working from remote locations either part-time or full-time, were looked into in this study. The aspects considered here include priorities set by management and supervisory practices, attitudes of the employees, relationship between the organization and the employees, increase of additional work and procedures due to policy, complexities and issues in following the policy and awareness of the policy and information security in general. According to the research findings, when considering the correlation between the variables, all these seem to have a positive influence over the perception, some having strong and the rest having a medium effect. Among the aspects which are having strong correlation were, priorities set by management and supervisory practices, attitudes of the employees and relationship between the organization and the employees. Increase of additional work and procedures due to policy, complexities and issues in following the policy and awareness of the policy and information security in general, had a medium influence on perception. Despite having a lower number of responses from African and American regions, according to the identified pattern from which the said regions do not have a significant variance, the results may be able to be generalized across the regions.

However, in spite of having a medium effect according to inferential statistics, awareness was pointed out as one of the important aspects to look at as a response to the open-ended question in “Points for improvement” section (section 3) of the questionnaire by a majority of 37% of the respondents who answered the question.

When it comes to the additional work created by the information security policy, the technical procedures seemed to have less impact than the additional administrative procedures on creating a negative perception. It could be assumed that the respondents had been familiar with software and related technologies may have some degree of impact on steering this behaviour.

Although a majority of the survey participants have disagreed that the conflicts in management and supervisory practices as having a negative impact on productivity, the inferential statistics show a strong positive correlation as stated above. This is the same when it comes to the relationships between attitudes - perception as well as perceived strength of the relationship between the employee and the organization - perception.

It should be taken into account that, despite its medium-strength association with the perception on productivity, the complexity in the information security policy has been considered as a minus point by the respondents by agreeing that it creates productivity drops in all three questions representing the same.

The results in this study seem to be consistent with the outcomes of the studies done previously in productivity and security area which will be discussed more in section 5.1.

5. RECOMMENDATIONS AND CONCLUSION

This chapter foregrounds conclusions and recommendations based on the findings resulting from the statistical analysis of this study. Also, it brings the limitations of this research into light and puts forward future research directions.

5.1. Research Implications

The rapidly evolving technologies in today's world have opened doors to many new or updated concepts in work climates, such as remote working. As much as it is trending and embraced by the software professionals, it has its own downside when it comes to information security. While productivity is always a concern of the management that comes with remote working, securing company-owned data is also very important. However, there is a lack of formal research in research knowledge base combining these areas, information security and productivity, especially with regard to remote working. Therefore, this research was conducted in an attempt to fill the gap in this knowledge area.

The main aim of this study was to identify the factors that can affect the balance between productivity and information security of the software professionals who work part-time or full-time from remote locations. Initially, a literature survey was used to identify potential factors that may affect the balance between information security and productivity. This included the additional work created by the information security policy, priorities set by the management and supervisory practices on information security and productivity, attitudes of the employee, complexities and difficulties in following the security procedures, the strength of the relationship between the employer and employee and awareness of the employee on information security. These were placed in a conceptual framework which was used as the basis for the development of the hypotheses. A survey was deployed to look at the problem in the remote worker's eyes; i.e. their perception. This questionnaire instrument was set-up mostly looking at the problem against the information security policy of the organization, due to the fact that it acts as the controlling system in the area of concern. Despite the length of the questionnaire and difficulties the researcher faced to reach the sample, it was well-received meeting the required sample size; around 34% of the respondents had gone to the extent to answer to the open-ended question on suggestions as well, which is usually a rare observation in responding to surveys. However, in terms of the geographic dispersion and type-of-organization dispersion, the data received was not very promising. If geographical dispersion of the respondents is looked at, respondents from Asia contributed for 79% while the African respondents only contributed to 1%. When the type of organization of the respondents is considered, only 1% contributed from the government sector while 95% was filled by the respondents in the private sector. However, the study was not based on this demographic information, and therefore there is no sample bias. In fact, it makes these areas interesting to focus for future research. Data collected using the survey was then statistically analyzed in hypothesis testing using descriptive statistics, a regression model with Pearson’s correlation coefficient and Coefficient of determination analysis.

Descriptive statistics show that remote-working software professionals accept the fact that the information security policy creates additional work/ tasks/ procedures to follow. But, they also show that the most troubling aspect of it is the administrative procedures one has to go through due to this. This seems to get worsened by its time-consuming nature. A comment in the open-ended question suggested having online support from the system administrators to smoothen this out. The regression model shows a significant positive relationship between the additional work created by the policy and the perception, which is with an association of medium-strength. As 23% of the variation of perception on policy can be explained by variations in additional work created by the policy (Hypothesis 1), it can be said that the relative amount of additional work created by the policy has a positive impact on how the software professional looks at information security policy as having a negative impact on productivity as pointed out by Bacik (2011).

The respondents mostly disagreed that they try to avoid information security policy when there are conflicts of priorities between security and productivity created by managerial and supervisory practices. This may be due to the knowledge they have of the importance of information security as a software professional. The conflicts in priorities show a significant positive correlation of 0.73 towards the perception and 54.4% of perception's variation explained by conflict in priorities in regression test results (Hypothesis 2). This is consistent with the prior studies (Sun et al., 2011). When the same descriptive analysis was carried out for the managerial and non-managerial workers separately, the results showed approximately 10% of non-managerial workers had accepted that the giving priority to productivity over information security can cause productivity hits than the managerial workers. Also, it reflected that the confusion led by the conflicts in priorities are contributing more to the decreased productivity when considering the variable Degree of Priority into account having 40% in favour of it.

Even though it has a significant but moderate positive correlation of 0.44 with the perception of software professionals (Hypothesis 3), the degree of complexity in following the information security policy has been accepted by the participants in the survey sturdily as a contributing factor to productivity drops especially with regard to the limitations of the information security policy and the time consumption to get problems solved because of the policy. In other words, the complexities in understanding and following an information security policy is negatively affecting the remote-working software professional's productivity as suggested by Thudium (2017), Maddox (2016), Gajar et al. (2013), Farrugia (2009), Jenkins (2002), Hirsch (2000).

When considering the influence of attitudes, the descriptive statistics showed a mean which sat in the middle but leaning towards the scale's right side, i.e., towards agreeing that attitudes have an effect on the perception. Even though attitudes on the policies in general and the attitudes generated through past experience do not pose much weight on this, attitudes on change or resistance to change have a bigger impact. According to regression analysis (Hypothesis 4), attitudes have a significant positive association with the remote-worker's perception. While the correlation is at 0.61, attitudes can explain 37.5% of the variation of perception. This is consistent with what White (2016) has put forward with regard to attitudes, information security and productivity. The attitudes have an impact on the productivity of remote working software professionals when they have to follow information security policy.

According to the descriptive statistics, the strength of the relationship between the employee and the organization seems to have a medium impact in making the remote workers disobey the information security policy. On the other hand, the inferential statistics (Hypothesis 5) show a significant positive correlation (0.6) between the organization-employee relationship and that the perception of policy's influence over productivity is in consistency with the previous study by Bulgurcu et al. (2010). This difference in results may have happened either due to some issue in presenting of the questions related to the strength of the relationship between the employee and the organization or an issue in the understanding of the same questions by the respondents. However, given the evidence from both descriptive and inferential analysis, it can be concluded that the strength of the relationship between the employee and the organization which has been created by the organizational culture has an impact on the perception which the remote working software professionals have towards information security policy as a factor affecting their productivity.

Both the descriptive statistics and the inferential statistics provide evidence in favour of the fact that the awareness on information security, as well as the policy, have some degree of influence over the way the remote workers of software industry see information security's effect on productivity. The regression results have shown that this relationship has a moderately strong positive correlation (Hypothesis 6). Out of the three questions that tested variable *Level of Awareness*, Question 11 in section 1 of the questionnaire tested the general awareness of information security proved that lack of awareness leads to dissatisfaction and ultimately resulting in decreased productivity. This has a major contribution in drawing the conclusion that awareness is a key factor that could affect balancing information security and productivity as

White (2016), Al-Mukahal and Alshare (2015), Sun, Ahluwalia and Koong (2011), Thudium (2017), Green (2016), Maddox (2016), Jilani et al. (2013), Morrow (2012), Jenkins (2002) and Hirsch (2000) have pointed out. The complementary qualitative study which was done to obtain the opinions of the respondents also shows that 37% which is the majority of the respondents who had answered the optional open-ended question are highlighting the importance on the level of awareness on information security and the related policy. Therefore, it can be concluded that the level of awareness may have an impact on the perception of the remote working software professional's perception of information security policy as a factor affecting productivity.

In summary, priorities set by management and supervisory practices, attitudes of the employees, relationship between the organization and the employees, increase of additional work and procedures due to policy, complexities and issues in following the policy and awareness of the policy and information security in general can be considered as affecting the software professional's perception towards information security as a factor affecting their productivity when they work from remote locations. This also disapproves of the current assumption of the non-managerial staff being counter-productive by showing that the managerial remote workers also need to improve themselves. As discussed in section 4.2.2, when the pattern of responding to questions considered, the results can be applied globally, although they may be most relevant to the Asian region. As far as the age and the remote work location are concerned, the results are applicable to all the age groups considered (section 4.2.1 and section 4.2.4). However, although results can be generalized for service category and service type, when it comes to the type of organization, they may be more relevant to remote working software professionals in the private sector.

5.2. Recommendations

One of the objectives of this study is making recommendations to the policy-makers of the organizations to consider when devising information security policy so that the productivity of the remote workers is assured. The findings of this study, derived from the detailed quantitative analysis as well as the short qualitative analysis of the comments given by the respondents, were used in coming up with these recommendations.

It is always better to keep all the users in the organization in general, aware of the importance of the information security and adhere to the relevant policies to protect the organization's data (section 4.3.6 contains the findings of quantitative analysis). The management of an organization has to take more weight on this. However, as the remote workers are a major vulnerability of an organization's information security, it is recommended to include separate clauses or it is even better to create a separate policy for them to follow (see sections 4.2.5 and 4.3.3 for more details on findings – complexities of the ISP should be eliminated). These clauses or policy should direct them to certain processes, procedures, actions and best practices that would act as precautions or self-defensive tactics. Some examples for these are to select a proper, secured area to work when working away from office, not to use public Wi-Fi, not to connect to IoT enabled devices to the devices that are used to connect to company network, to strictly use VPN, etc. when connecting to organization's network, taking necessary actions to avoid visual hacking when working from public places and properly disposing the confidential information.

Proper policy design and implementation followed by keeping it up-to-date is also highly recommended. Rather than setting up any policy blindly just using the widely-used standards, designing it with the end user in mind is a key point to consider (see findings in sections 4.3.1 and 4.3.3 – when the ISP creates additional work and complexities, they negatively affects productivity). Collaborating with the end users (in this case, the remote workers), via brainstorming, focus groups, etc. or even surveys would enable the policy-makers to get a better idea on the tasks that are going to be performed while teleworking, what level of access and privileges would they need, what would be the technical barriers, what can be the consequences on productivity if the proposed policy is implemented, etc.. Another aspect to look at is the level of sensitivity of data that needs to be protected and the context that the defenses are to be set up. These are essential to things in a prior analysis as they are the key elements that make the policy practical. In addition, with the technologies changing in no time, the threat landscape is also widening. Therefore, it is crucial to keep an eye on such changes and update the policy accordingly. These steps would help in reducing most of the inefficiencies of the policy (see sections 4.2.5 for quantitative analysis findings and 4.4 for qualitative analysis findings).

Even though it might create additional work to the end-user, the policy should enforce them to keep up-to-date software and devices. The IT services team is recommended to support the end-user in this regard by keeping them notified on updates, deploying patches and other extensions on a regular basis, etc. and be ready to provide support as and when necessary (based on findings in sections 4.3.3, 4.2.5 and 4.4).

To follow any policy properly, the users should be aware of it as well as its importance. Based on findings stated in sections 4.2.5, 4.2.6, 4.3.6 and 4.4, it is recommended to make awareness on the information security, its importance, vulnerabilities and threats, consequences of ignoring it and the details of the ISP. This can be achieved through discussions, training and periodic checks. By highlighting the value the ISP creates, it would be helpful to manage the resistance to change as well. Also, by making the policy straightforward and concise, it would be easy to get the user to go through it.

Better policy implementation can be achieved by improvements in the IT services team's processes as well as the related workflows. As an example of process improvements, the team can improve the process to monitor policy execution and review it as necessary from time-to-time. As examples for workflow improvements, the team can look into the ways to reduce the time taken to fix a technical issue (time-to-resolution), increase the ability to fix an issue when it occurs for the first time (first-time-resolution), simplifying approval paths, etc. (see related findings in sections 4.3.3 and 4.4).

Another recommendation to the organization is to allocate a dedicated team to maintain the policy and make them go through proper learning processes so they can contribute in designing policy effectively (based on findings in sections 4.3.1, 4.3.3 and 4.4 – there is a need to reduce the additional work created by and complexities of ISP).

When using tools, it is recommended to use a selection of tools which are capable of detecting and protecting from the various types of threats. However, it is not recommended to select these arbitrarily even if there is enough budget allocation to buy the industry’s best tools. The tool selection should be done consciously, after analyzing the requirement and the capabilities of the tools. It is better to have a few tools that are capable of handling the necessary focus areas such as security analytics capabilities and vulnerability management rather than having a number of tools for each area (see sections 4.2.5 and 4.3.1 for associated findings – incorporating every tool, every practice and procedure may make the policy to create additional work to the end user).

Employee electronic monitoring is also recommended given that it is used for security-related monitoring. This should be executed with caution as this could lead to dissatisfaction in the employees (Holland, Cooper and Hecker, 2015) (based on findings in sections 4.2.5, 4.3.4 and 4.3.5).

One of the most important recommendations is not targeting the policy, but targeting the organization as a whole is on managing the organizational behaviour. When there is a strong relationship between the employees and the organization, the mutual understanding tends to go up and the resistance to change is reduced (see associated findings in section 4.3.5) and the organization should have a clear vision on what aspects are considered important; may it be productivity, security, something else or a combination of aspects (see related findings in section 4.3.2). This makes it less troublesome to introduce change (Amarantou, Kazakopoulou, Chatzoudes & Chatzoglou, 2018; Crouzet, Parker & Pathak, 2014).

In summary, the following are the recommendations to consider when creating/ updating an ISP and to secure information of an organization:

- Including separate clauses or creating a separate policy for remote workers
- Including precautionary actions to take, best practices and other details to create awareness of information security related concerns
- Proper policy design and implementation keeping end user and their efficiency in mind
- To achieve proper policy design, collaborating with the end user and educating the IT team
- To achieve proper policy implementation, improving the internal processes as well as workflows of the IT team
- Keeping the policy up-to-date
- Considering the level of sensitivity of data when designing policy
- Improving the quality of support service of the IT team
- Creating awareness of information security, ISP, vulnerabilities, threats, etc. by training, discussions and other means
- Appointing responsible personnel to maintain the policy
- Optimizing the usage of tools
- Remote worker electronic monitoring in information security related areas
- Improving the organizational culture so the employees unanimously work towards securing information

5.3. Research Limitations and Future Research Directions

As a common case with most of the studies, this study is also subject to a few limitations that are possible to be addressed in future research. One such limitation was limited access to the sample in certain regions. For example, African respondents only contributed to 1% of the sample. Although the results were generalized taking the pattern in responding into account, this may have an impact on the findings at least in generalizing to that region. It is suggested to carry out a focused study on those regions. The same type of limitation also occurs with regard to the type of organization where the survey participants work. 95% of the respondents were from the private sector and therefore these findings may not be applicable to government/ public and semi-government sectors. Future research can focus on government and semi-government sectors to fill this gap. Moreover, as complementary actions to the current study, the following are suggested:

- qualitative research on the same problem,
- another study including freelancers to see how the freelancing companies would secure its buyers' information without hindering productivity and,
- how technical aspects can be integrated to make information secure while leaving the remote workers productive

5.4. Concluding Remarks

The main problem addressed in this research was that not knowing exactly what perception that the remote working software professionals have towards the security policies as a factor affecting the productivity in performing their day-to-day work as well as the related factors that may cause productivity drops, although the companies motivate the software developers to work more and more remotely.

It was intended to find what factors have impacted the productivity of the remote workers that are generated by the actions taken to safeguard information security which leads to specifically addressing the following research question:

> *"What considerations can be regarded as essential when devising information security policies to maximize the efficiency of remote workers in the software industry?"*

By finding an answer to the research question, the following objectives were expected to be served:

- *To identify and assess the factors affecting the perception of the remote workers in the software industry on how the security policies implemented by their organizations are affecting productivity.*

  As there was limited literature associating all the three aspects - information security, remote working and productivity - the literature survey was carried out to identify potential factors that are having an impact at least one of them and then connected them to the current study using a survey. Through the results, it was found out that the remote working software professionals see these identified factors as having an impact on their productivity. Therefore, this research objective has been proven successful by the current study.

- *To provide recommendations for devising effective information security policies to maintain a better balance between information security and remote worker productivity.*

  This study provides a number of recommendations to consider when devising information security policy backed by the analysis which gives insights into what would disturb the harmony between information security and productivity. Therefore, this objective can be considered as substantiated by this study.

- *To contribute to the research knowledge areas of information security and remote working.*

  The current research fills a gap in the research area that combines information security and productivity in remote working. As there was a lack of previous research, the present study collected many aspects from other related areas and expanded the landscape of this research area. Therefore, this objective is also supported.

REFERENCES

Abbot, M. L., (2016). Using Statistics in the Social and Health Sciences with SPSS and Excel. New Jersey: John Wiley & Sons.

Aczel, A. D., & Sounderpandian, J. (2009). Complete Business Statistics. McGraw-Hill/Irwin.

Adams, M. (2016), Are There Differences Between Working Remotely, Telecommuting, and Working from Home? – Telecommute and Remote Jobs – Career Tips, Retrieved November 8, 2017, from https://www.virtualvocations.com/blog/telecommuting-job-search-help/differences-working-remotely-telecommuting-working-home/

Al-Mukahal, H. M., Alshare, K. (2015) An examination of factors that influence the number of information security policy violations in Qatari organizations, *Information & Computer Security*, 23(1), 102-118. doi: 10.1108/ICS-03-2014-0018

Amarantou, V., Kazakopoulou, S., Chatzoudes, D., Chatzoglou, P., (2018), Resistance to change: an empirical investigation of its antecedents, *Journal of Organizational Change Management*, 31 (2), 426-450, DOI: 10.1108/JOCM-05-2017-0196

Bacik, S. (2011), Productivity vs. Security, Retrieved February 17, 2017, from http://www.infosectoday.com/Articles/Productivity_Security.htm

Bollen K.A. (1989). *Structural Equations with Latent Variables*. John Wiley & Sons, Inc., New York, NY

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010), Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly*, 34(3), 523-548.

Business Insider Netherlands (2019), Dit marketingbureau werkt een paar maanden per jaar vanuit Bali, Retrieved January 29, 2018, from https://www.businessinsider.nl/brandfirm-bali-werken/

Cassidy, C., Kreitner, R. & VanHuss, S. (2014). Administrative Management: Setting People Up for Success. 1st edition. Stamford. Cengage Learning.

*Census Bureau Report Shows Steady Increase in Home-Based Workers Since 1999 - Employment & Occupations - Newsroom - U.S. Census Bureau (*2012), Retrieved May 2, 2018 from https://www.census.gov/newsroom/releases/archives/employment_occupations/cb12-188.html

Chan, M., Woon, I. & Kankanhalli, A. (2014) Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior, *Journal of Information Privacy and Security*, 1(3), 18-41. doi: 10.1080/15536548.2005.10855772

Cherry, K. (2016), Forming a Good Hypothesis for Scientific Research, Retrieved December 2, 2018 from https://www.verywellmind.com/what-is-a-hypothesis-2795239

Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment,* 7(3), 309-319. http://dx.doi.org/10.1037/1040-3590.7.3.309

Cochran, W. G. (1977), *Sampling Techniques*, Retrieved from https://archive.org/details/Cochran1977SamplingTechniques_201703

Craparo, Robert M. (2007). "Significance level". In Salkind, Neil J. (Ed.). *Encyclopedia of Measurement and Statistics*. Thousand Oaks, CA: SAGE Publications.

Crouzet, B., Parker, D. W., Pathak, R., (2014), Preparing for productivity intervention initiatives, International Journal of Productivity and Performance Management, 63 (7), 946-959, DOI: 10.1108/IJPPM-10-2013-0175

CYBER RISK APPETITE:Defining and Understanding Risk in the Modern Enterprise. (2016). Retrieved from https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf

Davis, G. (2011), *The Zen of Risk: Seeking Balance between Security and Business Productivity,* Retrieved February 17, 2017, from http://www.securityweek.com/zen-risk-seeking-balance-between-security-and-business-productivity

Farrugia, C. (2009), *Security vs. Productivity in the Workplace*, Retrieved April 27, 2017 from https://techtalk.gfi.com/security-vs-productivity-in-the-workplace/

Gajar, P.K., Ghosh, A. & Rai, S. (2013), Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies, *Journal of Global Research in Computer Science*, 4 (4), 62-70

George, D., & Mallery, M. (2010). SPSS for Windows Step by Step: A Simple Guide and Reference, 17.0 update (10a ed.) Boston: Pearson.

Gilchrist, A. (2016), *IT choosing between productivity and security | ITProPortal*, Retrieved April 26, 2017 from http://www.itproportal.com/2016/03/17/choosing-productivity-security/

Glen, S. (2018, June 16). Average Inter-Item Correlation: Definition, Example. Retrieved from https://www.statisticshowto.datasciencecentral.com/average-inter-item-correlation/

Gravetter, F., & Wallnau, L. (2014). Essentials of statistics for the behavioral sciences (8th ed.). Belmont, CA: Wadsworth.

Green, J. (2016), *How to Avoid the Biggest Security Risks of Remote Working | Shred-it*, Retrieved January 13, 2018 from https://www.shredit.com/en-us/blog/securing-your-information/may-2016/how-to-avoid-the-biggest-security-risks-of-remote

Greenawald, E. (n. d.), WTF is a Workcation? (Hint: Something You Need Now), Retrieved November 30, 2018, from https://www.themuse.com/advice/wtf-is-a-workcation-hint-something-you-need-now

Guruswamy, K. (2016), *The Productivity vs. Risk Trade-Off in Enterprise Security*, Retrieved April 27, 2017 from https://www.menlosecurity.com/blog/the-productivity-vs.-risk-trade-off-in-enterprise-security

Hair, J. F., Black, W. C., Babin, B. J. and Anderson, R. E. (2014). *Multivariate Data Analysis*. 7th edition. Essex. Pearson Education Limited.

Halkos, G. & Bousinakis, D. (2010), The effect of stress and satisfaction on productivity, *International Journal of Productivity and Performance Management*, 59 (5), 415-431, https://doi.org/10.1108/17410401011052869

Hirsch, J. L. (2000), *Telecommuting: Security Policies and Procedures for the "WorkFrom-Anywhere" Workforce*, Retrieved June 4, 2018 from https://www.giac.org/paper/gsec/323/telecommuting-security-policies-procedures-work-from-anywhere-workforce/100918

Holland, P. J., Cooper, B. & Hecker, R. (2015), Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type, *Personnel Review*, 44 (1), 161-175, https://doi.org/10.1108/PR-11-2013-0211

Information Security Top-Down. (2004, December 1). Retrieved from https://www.securitymagazine.com/articles/76843-information-security-top-down-1

Ishmael Mensah. (2015). How can we determine the sample size from an unknown population?. [Blog comment]. Retrieved from https://www.researchgate.net/post/How_can_we_determine_the_sample_size_from_an_unknown_population

Jenkins, G. (2002), *Mitigating Teleworking Risks*, Retrieved June , 2018 from https://www.sans.org/reading-room/whitepapers/telecommunting/mitigating-teleworking-risks-314

Jilani, U., Ahimmat, A., Raso, A., Thorpe, D., & Tran, M. (2013). *Ready, steady telework: information security essentials for the teleworker*. Melbourne: The University of Melbourne

Jones, J. M. (2015), *In U.S., Telecommuting for Work Climbs to 37%*, Retrieved April 22, 2018 from http://news.gallup.com/poll/184649/telecommuting-work-climbs.aspx

Krejcie, R.V. & Morgan, D.W. (1970). Determining sample size for research activities. *Educational & Psychological Measurement*, 30 (3), 607-610.

Maddox, T. (2016), *IoT hidden security risks: How businesses and telecommuters can protect themselves – TechRepublic*, Retrieved March 18, 2018 from https://www.techrepublic.com/article/iot-hidden-security-risks-how-businesses-and-telecommuters-can-protect-themselves/

Mitchell, M. L. & Jolley, J. M., (2010). Research Design Explained. 7th Edition. Wadsworth. Cengage Learning.

Morrow, B. (2012), BYOD security challenges: control and protect your most sensitive data, Network Security, 2012 (12), 5-8, https://doi.org/10.1016/S1353-4858(12)70111-3

Perception (psychology), (n.d.) *McGraw-Hill Concise Dictionary of Modern Medicine*. (2002). Retrieved November 26 2018 from https://medical-dictionary.thefreedictionary.com/Perception+(psychology)

Phenomenon, (n.d.), In *Wikipedia*, Retrieved January 13, 2018 from https://en.wikipedia.org/wiki/Phenomenon

Ravitch, S. M. & Riggan M. (2017), *Reason & Rigor: How Conceptual Frameworks Guide Research* (2nd ed.), Thousand Oaks, CA: SAGE Publications, Inc

Roemer, K. (2016). Securing the cloud endpoint. Retrieved from https://www.networkworld.com/article/3138540/securing-the-cloud-endpoint.html

Roscoe, J.T. (1975). *Fundamental Research Statistics for the Behavioural Sciences*. 2nd edition. New York. Holt Rinehart & Winston.

Rubin, A. & Babbie, E. R. (2009). *Essential Research Methods for Social Work*. 2nd edition. Belmont. Cengage Learning.

Rumsey, D. J., (2011). Statistics for Dummies. New Jersey: John Wiley & Sons.

Schwochau, S., Delaney, J., Jarley, P. & Fiorito, J. (1997), Employee participation and assessments of support for organizational policy changes, *Journal of Labor Research*, 18 (3), 379-401, https://doi.org/10.1007/s12122-997-1046-z

Small office/home office, (n.d.), In *Wikipedia*, Retrieved June 05, 2018 from https://en.wikipedia.org/wiki/Small_office/home_office

Smalley, S. D. (1999). Policy Flexibility. Retrieved from https://www.cs.utah.edu/flux/papers/micro/node2.html

Springer, K. (2017), Digital nomad retreats: Work around the world | CNN Travel, Retrieved December 15, 2017 from https://edition.cnn.com/travel/article/workation-digital-nomad-retreats/index.html

Stackpole, B. (2016). How flexible should your infosec model be?. Retrieved from https://www.computerworld.com/article/3119745/how-flexible-should-your-infosec-model-be.html

Stanton, J. M., (2000) Reactions to Employee Performance Monitoring: Framework, Review, and Research Directions, *Human Performance*, 13 (1), 85-113, DOI: 10.1207/S15327043HUP1301_4

Sun, J., Ahluwalia, P. & Koong, K.S. (2011), The more secure the better? A study of information security readiness, *Industrial Management & Data Systems*, 111(4), 570-588. doi: 10.1108/02635571111133551

Ragin, C. C. & Amoroso, L. M., (2011). Constructing Social Research: The Unity and Diversity of Method (2nd ed). Thousand Oaks, CA: Pine Forge Press.

Taber, K. S., (2018). The Use of Cronbach’s Alpha When Developing and Reporting Research Instruments in Science Education, *Research in Science Education*, 48 (6), 1273-1296, DOI: 10.1007/s11165-016-9602-2

Tavakol, M. & Dennik, R., (2011). Making sense of Cronbach's alpha, International Journal of Medical Education, 2011 (2), 53-55, DOI: 10.5116/ijme.4dfb.8dfd

Taylor, R. (1990). Interpretation of the Correlation Coefficient: A Basic Review, *Journal of Diagnostic Medical Sonography*, 6 (1), 35-39, DOI: 10.1177/875647939000600106

Thudium, M. (2017), *Adopting Information Security to the Future of Remote Workers | IT Security Central*, Retrieved October 14, 2017 from https://itsecuritycentral.teramind.co/2017/08/04/the-rise-of-remote-workers-adopting-information-security-to-the-new-future/

Trochim, W. M., & Donnelly, J. P. (2006). The research methods knowledge base (3rd ed.). Cincinnati, OH:Atomic Dog.

Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior, (n.d.), Retrieved June 03, 2018 from https://www.cisco.com/c/dam/global/en_ca/assets/pdf/Understanding_Remote_Worker_Security_A_survery_of_User_Awareness_vs_Behaviour.pdf

White, S. K. (2016), *IT leaders pick productivity over security | CIO*, Retrieved April 27, 2017 from http://www.cio.com/article/3063738/security/it-leaders-pick-productivity-over-security.html

workcation, (n.d.), In *wiktionary*, Retrieved April 12, 2018 from https://en.wiktionary.org/wiki/workcation

Ye, J. & King, J., (2016), Managing the downside effect of a productivity orientation, *Journal of Services Marketing*, 30 (2), 238-254, doi: 10.1108/JSM-10-2014-0351

Yin and yang, (n.d.), In *Wikipedia*, Retrieved January 05, 2018 from https://en.wikipedia.org/wiki/Yin_and_yang

APPENDIX A: QUESTIONNAIRE

Effective Information Security Policies for Efficient Remote Working: Software Professionals' Perspective

Through this questionnaire, it is intended to find out what perception do the remote working (also called teleworking, work-from-home, etc.) professionals in the software industry have on *the security policies as a factor affecting their productivity* and what steps can be taken to avoid productivity downturns that may have caused by the same.

If you are a software professional working for a software or non-software company and working remotely full-time or part-time, you are most welcome to participate in this survey. Also, please be kind enough to forward it to your friends and colleagues who meet the above criteria.

Your frank and honest responses to the questions are much appreciated. This survey is conducted in relation to the post-graduate research "Effective Information Security Policies for Efficient Remote Working: Software Professionals' Perspective" as a partial fulfillment of MBA-IT course of University of Moratuwa, Sri Lanka. Your anonymity and confidentiality will be strictly protected and the information will be used only for academic purposes.

Thank you for your effort and willingness in participating in this survey.

Yours Sincerely,
Dileesha Amarasinghe Arachchi, PMP
MBA in IT (Final Year Student - University of Moratuwa)
Email: dileesha.17@cse.mrt.ac.lk

Section 1: The perception on information security policy (6 point Likert scale: Strongly Disagree/ Disagree/ Slightly Disagree/ Slightly Agree/ Agree/ Strongly Agree)

---

1. If productivity is a major concern, we should not be pressurized to follow policies, procedures and guidelines as they may cause serious productivity hits, especially when remote-working.
2. Information security policy forces us to follow so many procedures before getting a thing done when we work from outside no matter if the device we use is provided by the company. This keeps us waiting and our time is wasted.
3. My organization doesn’t clearly communicate the additions/ changes to the policies on time. Therefore, it’s not easy to be productive while following the same because we don’t have all the details about it.
4. Having to follow the information security policy when working remote sometimes creates additional administrative procedures (e.g. going through certain procedures to gain privileges) to follow. This results in productivity drops.
5. I have to understand and acquire knowledge on certain technical and/or non-technical procedures (for example: using VPN to access the network) required by information security policy when connecting to the company network from a location away from office premises. This is tough at times resulting in inefficiencies.
6. Because my organization doesn’t provide adequate trainings/ instructions on preventive actions to safeguard information security when working from remote locations it is difficult and time-consuming to get rid of inefficiencies that are created by various limitations in the information security policy.
7. I sometimes face difficulties when working remote due to the restrictions/ limitations/ procedures imposed by the information security policy.
8. My daily output is negatively affected while remote-working by having to stick to Information security policy, as it requires us to adhere to a lot of technical

matter that take additional time apart from actual work such as using multi-factor authentication, using VPN to log in, resetting passwords frequently, limited usage of single sign-on capabilities, etc., even if I use my own PC.

9. My immediate management/ team leads/ supervisors instruct to increase productivity while working remote. Therefore, I take "shortcuts" and avoid the information security policy in situations when I feel that following it hits productivity badly.
10. I sometimes have the suspicion that the organization sets up an information security policy just because the employees cannot be trusted when they are away from office.
11. When I come to think of it, the fact that our company does not have trust on us even though we do not expose sensitive data when we remote-work, has created a disappointment in me and has resulted in decreasing my productivity.
12. I don't see a justifiable reason to follow an information security policy when connecting to the company network from a remote location. It only makes life difficult.
13. The time-to-time changes in the information security policy are a headache and not communicating them properly affects productivity negatively as we don't know all the specifics about the procedures.
14. In the past, information security policies have had affected in productivity losses. Because of that, I don't like to follow those when remote-working.
15. Having to change the way we work according to the changes in information security policy all the time is something that I don't like.
16. Even though we're supposed to adhere to the information security policy whenever we connect to the company network from outside, I sometimes ignore it to keep me productive.
17. The information security policy gives the impression that, the company doesn't believe the fact that we're taking necessary precautions to not to expose sensitive data when we work remotely.
18. When working from a remote location, it is difficult to get problems solved quickly if we stick to the information security policy.

19. In my opinion, having to adhere to any policy causes delays, difficulties, etc.. Inefficiencies can emerge because of this.
20. An information security policy is not required if the management has good faith in the employees.
21. If the organization does not make it clear on what should be given more priority when remote working; whether it is following the information security policy or ensuring productivity, or to balance the both, I get confused. This only makes me struggle and being inefficient without knowing what to do.

Section 2: Demographics

1. Age range (dropdown):

   >25
   25 – 30
   30 – 35
   35 – 40
   40 – 45
   45<

2. Geographical location (dropdown):

   Asia
   Africa
   Europe
   The Americas
   Oceania

3. Nature of service (2 dropdowns):

- Managerial - Non-managerial	- IT services - Software development - Software quality assurance - Project management - Customer interface (business analysis, product management, marketing) - Support services/ customer care - Other	- Government - Semi-government - Private

4. Remote work is mostly carried from (multi-select):

□ Home-office

□ Coffee shop

□ Co-working space

□ Library

□ Public places (other than what is mentioned above)

□ Other

Section 3: Tips for improvement (A multi-select question and an open-ended question)

1. I think, one or more of the following should be considered when preparing an information security policy for remote workers to maintain high productivity levels while adhering to the policy (please select one or more):

□ Having a proper, secured area for work when we work away from the company premises, helps to secure the sensitive information.

□ Even though we have to log in from time to time, automatically disconnecting idle sessions after a time-out by the system makes it trouble-free when we work from a public area.

□ When considering the security threats that connecting to a public Wi-Fi can pose, I think it is correct to restrict such when working remote. We should connect only via trusted Wi-Fi.

□ A remote worker monitoring system would help to identify any malicious activities even though it monitors all our activities.

□ We should be mindful to maintain up-to-date devices and software with regard to anti-viruses, firmware, etc. when we connect to company network from outside because it helps to reduce vulnerabilities.

□ We should try to avoid connecting the devices we use to access company network to IoT devices at all times as we cannot make sure how vulnerable or not they are.

□ In my opinion, our information security policy should have separate clauses to treat the devices we use to access company network that are company-owned and that are not (e.g. employee’s own devices).

□ Usage of mechanisms such as Data Leakage Prevention and Hashing to avoid information security breaches is an absolute necessity.

2. My suggestions to improve the information security policy in order to ensure that it does not have any effect on our productivity when working from a remote location (in point form):

------------------------- You’ve reached the end. Thank you. ------------------------

APPENDIX B: QUESTIONNAIRE DEFINITION

The questionnaire instrument carried three sections; section 1 testing the independent and dependent variables is referred to as S1, section 2 related to demographics is referred to as S2 and section 3 on points for improvement is referred to as S3.

Table B. 1: Questionnaire items - to measure the variables in Conceptual Framework

Variable	Dimension	Scale	Questionnaire Item
Relative Increase of Additional Work	Extra steps, policies creating additional work	Ordinal	S1-Q2
	Administrative aspect	Ordinal	S1-Q4
	Technical aspect	Ordinal	S1-Q8
Degree of Priority	Organization-wide	Ordinal	S1-Q21
	Immediate reporting entity	Ordinal	S1-Q9
	Individual	Ordinal	S1-Q16
Perceived Level of Complexity		Ordinal	S1-Q5 S1-Q7 S1-Q18
Negativity of Attitudes	Specific to remote working and information security policy	Ordinal	S1-Q1 S1-Q14
	Attitude towards policies in general	Ordinal	S1-Q15
Perceived Strength of the Relationship with Employer		Ordinal	S1-Q10 S1-Q17 S1-Q20
Level of Awareness	Clarity, adequacy and timeliness of communications	Ordinal	S1-Q3 S1-Q11
	Adequacy of training	Ordinal	S1-Q6
Negativity of Perception Towards Information Security Policies		Ordinal	S1-Q12 S1-Q13 S1-Q19

Table B. 2: Questionnaire items - to measure the demographics and recommendations

Item	**Scale**	**Questionnaire Item**
Age	Ratio	S2-Q1
Geographical location	Nominal	S2-Q2
Nature of service	Nominal	S2-Q3
Remote-work location	Nominal	S2-Q4
Improvements to remote-work information security policy in employee’s opinion	Nominal	S3-Q1
Remote-worker’s own suggestions	Nominal	S3-Q2

APPENDIX C: DESCRIPTIVE STATISTICS

The additional details of the descriptive analysis are given here.

Table C. 1: Dispersion of the Respondents according to Age

Age	# of Respondents
< 25	1
25-30	44
30-35	56
35-40	54
40-45	14
45 <	9

Table C. 2: Dispersion of the Respondents according to Geographical Location

Location	# of Respondents
Asia	141
Africa	1
Europe	16
Oceania	14
The Americas	6

Table C. 3: Dispersion of the Respondents according to Service Category

Service Category	# of Respondents	%
Managerial	68	38.2
Non-managerial	110	61.8

Table C. 4: Type of work the respondents of the sample are performing

Type of work	# of Respondents
Software Development	73
IT services	33
Project management	13
Software quality assurance	32
Customer interface (business analysis, product management, marketing)	14
UX/UI Design	1
Support services/ customer care	7
Consultant	2
IT Services, Software development & Project Management	1
E-Commerce	1
Software Delivery	1

Table C. 5: Dispersion of the sample according to the Type of organization of the employer

Type of Organization	# of Respondents	%
Government	1	0.56
Semi-government	7	3.93
Private	170	95.51

Table C. 6: Dispersion according to remote work location

Location of Remote Work	# of Respondents
Home-office	174
Co-working space	14
Coffee shop	11
Library	6
Other public places	14
Public transportation	3
Client sites	1

Table C. 7: Preference for the Suggested Recommendations

Recommendation	# of Respondents	%
Even though we have to log in from time to time, automatically disconnecting idle sessions after a time-out by the system makes it trouble-free when we work from a public area.	103	57.9
We should be mindful to maintain up-to-date devices and software with regard to anti-viruses, firmware, etc. when we connect to company network from outside because it helps to reduce vulnerabilities.	128	71.9
Usage of mechanisms such as Data Leakage Prevention and Hashing to avoid information security breaches is an absolute necessity.	95	53.4
When considering the security threats that connecting to a public Wi-Fi can pose, I think it is correct to restrict such when working remote. We should connect only via trusted Wi-Fi.	104	58.4
A remote worker monitoring system would help to identify any malicious activities even though it monitors all our activities.	67	37.6
We should try to avoid connecting the devices we use to access company network to IoT devices at all times as we cannot make sure how vulnerable or not they are.	76	42.7
In my opinion, our information security policy should have separate clauses to treat the devices we use to access company network that are company-owned and that are not (e.g. employeeâ€™s own devices).	89	50.0
Having a proper, secured area for work when we work away from the company premises, helps to secure the sensitive information.	102	57.3

Table C. 8: Respondents who agree that employee monitoring is necessary according to service category

Service category	# of respondents	%
Managerial	25	37.31
Non-managerial	42	62.69

Table C. 9: Response frequencies for survey-section 1 Question 1

Response	Frequency	%	Cumulative %		Response Category	%
Strongly Disagree	27	15.17	15.17		Disagree	54.49
Disagree	50	28.09	43.26		Agree	45.51
Slightly Disagree	20	11.24	54.49			
Slightly Agree	38	21.35	75.84			
Agree	29	16.29	92.13			
Strongly Agree	14	7.87	100.00			
Total	178	100.00				

Table C. 10: Descriptive statistics for survey-section 1 Question 1

Q1	
Mean	3.191011
Standard Error	0.11703
Median	3
Mode	2
Standard Deviation	1.561373
Sample Variance	2.437885
Kurtosis	-1.16215
Skewness	0.200387
Range	5
Minimum	1
Maximum	6
Sum	568
Count	178
Confidence Level(95.0%)	0.230953

Table C. 11: Response frequencies for survey-section 1 Question 1

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	27	15.17	15.17		Disagree	54.49
Disagree	50	28.09	43.26		Agree	45.51
Slightly Disagree	20	11.24	54.49			
Slightly Agree	38	21.35	75.84			
Agree	29	16.29	92.13			
Strongly Agree	14	7.87	100.00			
Total	178	100.00				

Table C. 12: Descriptive statistics for survey-section 1 Question 1

Q1	
Mean	3.191011
Standard Error	0.11703
Median	3
Mode	2
Standard Deviation	1.561373
Sample Variance	2.437885
Kurtosis	-1.16215
Skewness	0.200387
Range	5
Minimum	1
Maximum	6
Sum	568
Count	178
Confidence Level(95.0%)	0.230953

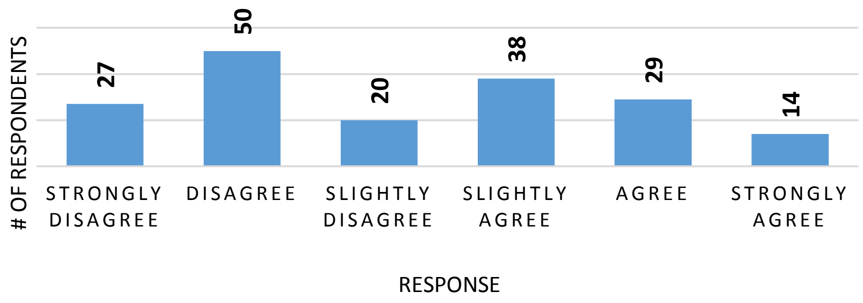


Figure C. 1: Response frequencies for survey-section 1 Question 1

Table C. 13: Response frequencies for survey-section 1 Question 2

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	15	8.43	8.43		Disagree	48.88
Disagree	56	31.46	39.89		Agree	51.12
Slightly Disagree	16	8.99	48.88			
Slightly Agree	40	22.47	71.35			
Agree	43	24.16	95.51			
Strongly Agree	8	4.49	100.00			
Total	178	100.00				

Table C. 14: Descriptive statistics for survey-section 1 Question 2

Q2	
Mean	3.359551
Standard Error	0.109387
Median	4
Mode	2
Standard Deviation	1.459411
Sample Variance	2.12988
Kurtosis	-1.29479
Skewness	0.016704
Range	5
Minimum	1
Maximum	6
Sum	598
Count	178
Confidence Level(95.0%)	0.215871

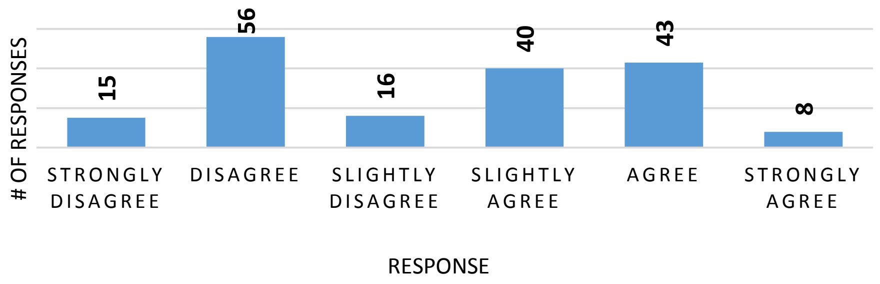


Figure C. 2: Response frequencies for survey-section 1 Question 2

Table C. 15: Response frequencies for survey-section 1 Question 3

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	16	8.99	8.99		Disagree	52.25
Disagree	55	30.90	39.89		Agree	47.75
Slightly Disagree	22	12.36	52.25			
Slightly Agree	35	19.66	71.91			
Agree	43	24.16	96.07			
Strongly Agree	7	3.93	100.00			
Total	178	100.00				

Table C. 16: Descriptive statistics for survey-section 1 Question 3

Q3	
Mean	3.308989
Standard Error	0.108662
Median	3
Mode	2
Standard Deviation	1.449733
Sample Variance	2.101727
Kurtosis	-1.27442
Skewness	0.065471
Range	5
Minimum	1
Maximum	6
Sum	589
Count	178
Confidence Level(95.0%)	0.21444

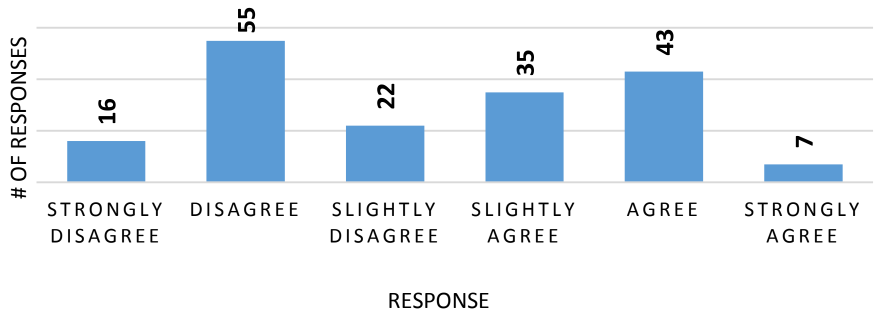


Figure C. 3: Response frequencies for survey-section 1 Question 3

Table C. 17: Response frequencies for survey-section 1 Question 4

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	7	3.93	3.93		Disagree	34.83
Disagree	39	21.91	25.84		Agree	65.17
Slightly Disagree	16	8.99	34.83			
Slightly Agree	41	23.03	57.87			
Agree	67	37.64	95.51			
Strongly Agree	8	4.49	100.00			
Total	178	100.00				

Table C. 18: Descriptive statistics for survey-section 1 Question 4

Q4	
Mean	3.820225
Standard Error	0.102071
Median	4
Mode	5
Standard Deviation	1.361802
Sample Variance	1.854504
Kurtosis	-1.03157
Skewness	-0.47045
Range	5
Minimum	1
Maximum	6
Sum	680
Count	178
Confidence Level(95.0%)	0.201433

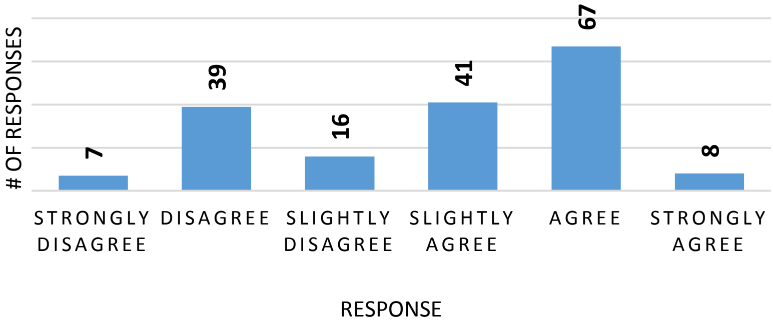


Figure C. 4: Response frequencies for survey-section 1 Question 4

Table C. 19: Response frequencies for survey-section 1 Question 5

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	4	2.25	2.25		Disagree	41.57
Disagree	50	28.09	30.34		Agree	58.43
Slightly Disagree	20	11.24	41.57			
Slightly Agree	39	21.91	63.48			
Agree	56	31.46	94.94			
Strongly Agree	9	5.06	100.00			
Total	178	100.00				

Table C. 20: Descriptive statistics for survey-section 1 Question 5

Q5	
Mean	3.674157
Standard Error	0.102204
Median	4
Mode	5
Standard Deviation	1.363572
Sample Variance	1.859328
Kurtosis	-1.29615
Skewness	-0.16258
Range	5
Minimum	1
Maximum	6
Sum	654
Count	178
Confidence Level(95.0%)	0.201695

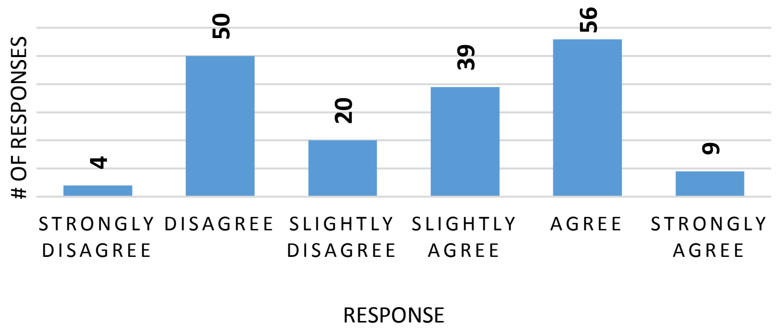


Figure C. 5: Response frequencies for survey-section 1 Question 5

Table C. 21: Response frequencies for survey-section 1 Question 6

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	11	6.18	6.18		Disagree	48.31
Disagree	51	28.65	34.83		Agree	51.69
Slightly Disagree	24	13.48	48.31			
Slightly Agree	44	24.72	73.03			
Agree	42	23.60	96.63			
Strongly Agree	6	3.37	100.00			
Total	178	100.00				

Table C. 22: Descriptive statistics for survey-section 1 Question 6

Q6	
Mean	3.410112
Standard Error	0.102508
Median	4
Mode	2
Standard Deviation	1.367628
Sample Variance	1.870406
Kurtosis	-1.18528
Skewness	-0.03707
Range	5
Minimum	1
Maximum	6
Sum	607
Count	178
Confidence Level(95.0%)	0.202295

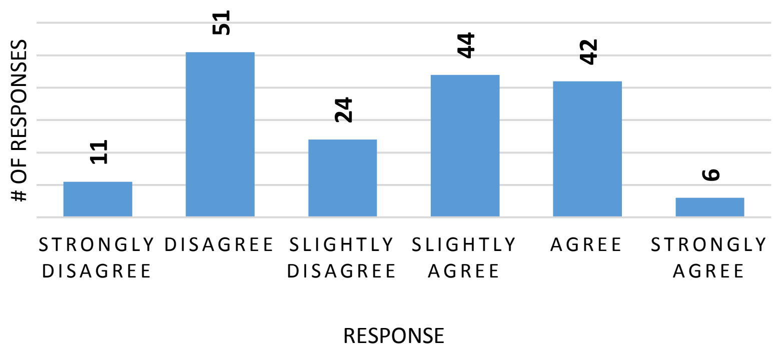


Figure C. 6: Response frequencies for survey-section 1 Question 6

Table C. 23: Response frequencies for survey-section 1 Question 7

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	8	4.49	4.49		Disagree	29.78
Disagree	30	16.85	21.35		Agree	70.22
Slightly Disagree	15	8.43	29.78			
Slightly Agree	52	29.21	58.99			
Agree	59	33.15	92.13			
Strongly Agree	14	7.87	100.00			
Total	178	100.00				

Table C. 24: Descriptive statistics for survey-section 1 Question 7

Q7	
Mean	3.932584
Standard Error	0.100968
Median	4
Mode	5
Standard Deviation	1.347085
Sample Variance	1.814638
Kurtosis	-0.64857
Skewness	-0.54928
Range	5
Minimum	1
Maximum	6
Sum	700
Count	178
Confidence Level(95.0%)	0.199257

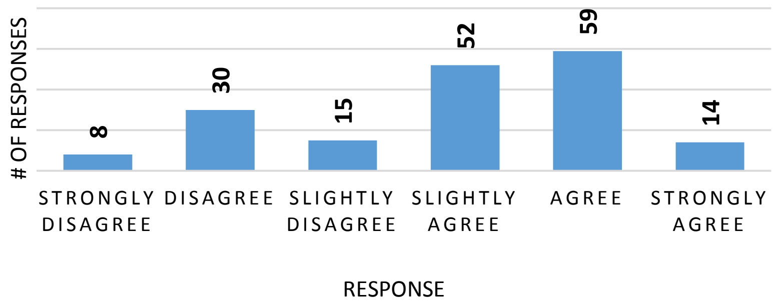


Figure C. 7: Response frequencies for survey-section 1 Question 7

Table C. 25: Response frequencies for survey-section 1 Question 8

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	16	8.99	8.99		Disagree	53.37
Disagree	55	30.90	39.89		Agree	46.63
Slightly Disagree	24	13.48	53.37			
Slightly Agree	40	22.47	75.84			
Agree	36	20.22	96.07			
Strongly Agree	7	3.93	100.00			
Total	178	100.00				

Table C. 26: Descriptive statistics for survey-section 1 Question 8

Q8	
Mean	3.258427
Standard Error	0.106017
Median	3
Mode	2
Standard Deviation	1.414438
Sample Variance	2.000635
Kurtosis	-1.16346
Skewness	0.113866
Range	5
Minimum	1
Maximum	6
Sum	580
Count	178
Confidence Level(95.0%)	0.209219

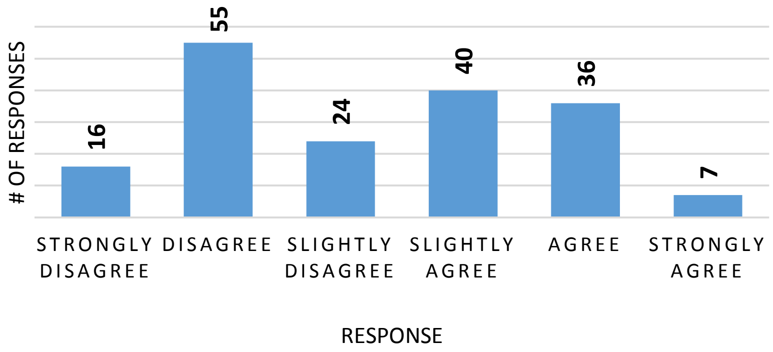


Figure C. 8: Response frequencies for survey-section 1 Question 8

Table C. 27: Response frequencies for survey-section 1 Question 9

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	40	22.47	22.47		Disagree	73.60
Disagree	78	43.82	66.29		Agree	26.40
Slightly Disagree	13	7.30	73.60			
Slightly Agree	26	14.61	88.20			
Agree	19	10.67	98.88			
Strongly Agree	2	1.12	100.00			
Total	178	100.00				

Table C. 28: Descriptive statistics for survey-section 1 Question 9

Q9	
Mean	2.505618
Standard Error	0.09991
Median	2
Mode	2
Standard Deviation	1.332968
Sample Variance	1.776804
Kurtosis	-0.50634
Skewness	0.776716
Range	5
Minimum	1
Maximum	6
Sum	446
Count	178
Confidence Level(95.0%)	0.197168

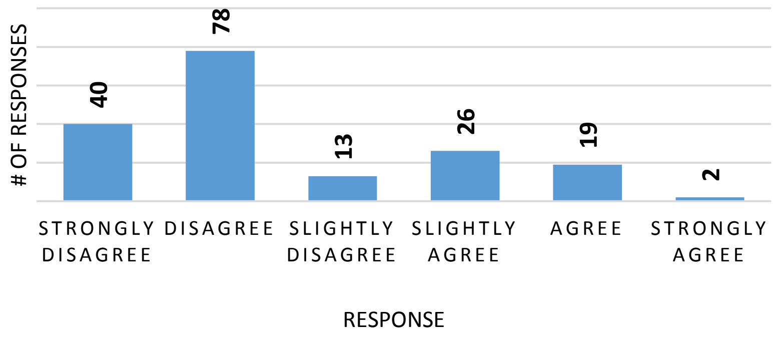


Figure C. 9: Response frequencies for survey-section 1 Question 9

Table C. 29: Response frequencies for survey-section 1 Question 10

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	25	14.04	14.04		Disagree	62.36
Disagree	67	37.64	51.69		Agree	37.64
Slightly Disagree	19	10.67	62.36			
Slightly Agree	27	15.17	77.53			
Agree	35	19.66	97.19			
Strongly Agree	5	2.81	100.00			
Total	178	100.00				

Table C. 30: Descriptive statistics for survey-section 1 Question 10

	Q10
Mean	2.97191
Standard Error	0.109659
Median	2
Mode	2
Standard Deviation	1.463027
Sample Variance	2.140449
Kurtosis	-1.16295
Skewness	0.377573
Range	5
Minimum	1
Maximum	6
Sum	529
Count	178
Confidence Level(95.0%)	0.216406

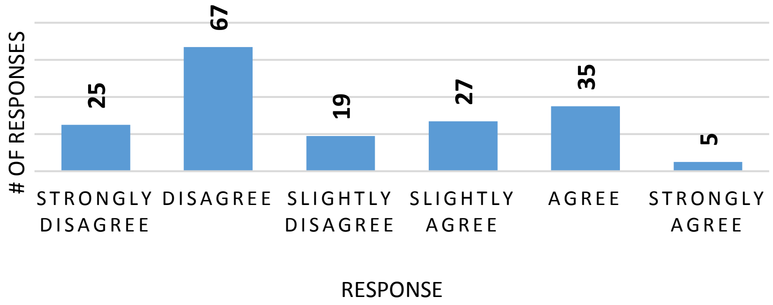


Figure C. 10: Response frequencies for survey-section 1 Question 10

Table C. 31: Response frequencies for survey-section 1 Question 11

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	7	3.93	3.93		Disagree	34.83
Disagree	44	24.72	28.65		Agree	65.17
Slightly Disagree	11	6.18	34.83			
Slightly Agree	42	23.60	58.43			
Agree	63	35.39	93.82			
Strongly Agree	11	6.18	100.00			
Total	178	100.00				

Table C. 32: Descriptive statistics for survey-section 1 Question 11

Q11	
Mean	3.803371
Standard Error	0.105417
Median	4
Mode	5
Standard Deviation	1.406438
Sample Variance	1.978068
Kurtosis	-1.12819
Skewness	-0.39664
Range	5
Minimum	1
Maximum	6
Sum	677
Count	178
Confidence Level(95.0%)	0.208036

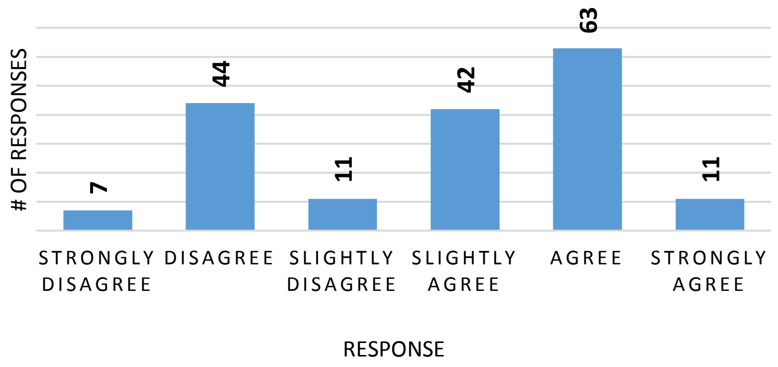


Figure C. 11: Response frequencies for survey-section 1 Question 11

Table C. 33: Response frequencies for survey-section 1 Question 12

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	43	24.16	24.16		Disagree	76.97
Disagree	79	44.38	68.54		Agree	23.03
Slightly Disagree	15	8.43	76.97			
Slightly Agree	19	10.67	87.64			
Agree	20	11.24	98.88			
Strongly Agree	2	1.12	100.00			
Total	178	100.00				

Table C. 34: Descriptive statistics for survey-section 1 Question 12

Q12	
Mean	2.438202
Standard Error	0.099485
Median	2
Mode	2
Standard Deviation	1.327289
Sample Variance	1.761696
Kurtosis	-0.25556
Skewness	0.897064
Range	5
Minimum	1
Maximum	6
Sum	434
Count	178
Confidence Level(95.0%)	0.196328

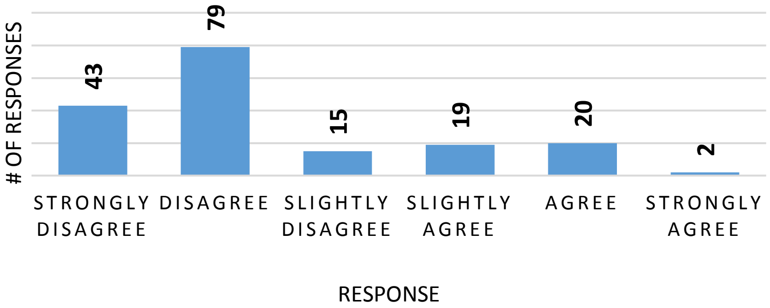


Figure C. 12: Response frequencies for survey-section 1 Question 12

Table C. 35: Response frequencies for survey-section 1 Question 13

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	33	18.54	18.54		Disagree	74.16
Disagree	78	43.82	62.36		Agree	25.84
Slightly Disagree	21	11.80	74.16			
Slightly Agree	27	15.17	89.33			
Agree	17	9.55	98.88			
Strongly Agree	2	1.12	100.00			
Total	178	100.00				

Table C. 36: Descriptive statistics for survey-section 1 Question 13

Q13	
Mean	2.567416
Standard Error	0.095889
Median	2
Mode	2
Standard Deviation	1.279325
Sample Variance	1.636672
Kurtosis	-0.44494
Skewness	0.724137
Range	5
Minimum	1
Maximum	6
Sum	457
Count	178
Confidence Level(95.0%)	0.189234

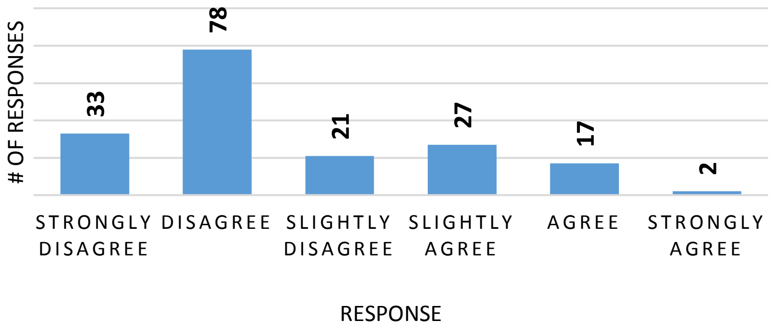


Figure C. 13: Response frequencies for survey-section 1 Question 13

Table C. 37: Response frequencies for survey-section 1 Question 14

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	23	12.92	12.92		Disagree	74.72
Disagree	90	50.56	63.48		Agree	25.28
Slightly Disagree	20	11.24	74.72			
Slightly Agree	26	14.61	89.33			
Agree	16	8.99	98.31			
Strongly Agree	3	1.69	100.00			
Total	178	100.00				

Table C. 38: Descriptive statistics for survey-section 1 Question 14

	Q14
Mean	2.61236
Standard Error	0.092959
Median	2
Mode	2
Standard Deviation	1.240222
Sample Variance	1.538151
Kurtosis	-0.13645
Skewness	0.862567
Range	5
Minimum	1
Maximum	6
Sum	465
Count	178
Confidence Level(95.0%)	0.18345

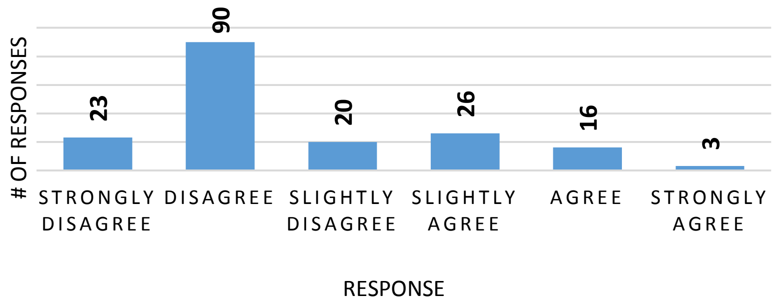


Figure C. 14: Response frequencies for survey-section 1 Question 14

Table C. 39: Response frequencies for survey-section 1 Question 15

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	11	6.18	6.18		Disagree	44.94
Disagree	53	29.78	35.96		Agree	55.06
Slightly Disagree	16	8.99	44.94			
Slightly Agree	45	25.28	70.22			
Agree	48	26.97	97.19			
Strongly Agree	5	2.81	100.00			
Total	178	100.00				

Table C. 40: Descriptive statistics for survey-section 1 Question 15

Q15	
Mean	3.455056
Standard Error	0.104209
Median	4
Mode	2
Standard Deviation	1.390323
Sample Variance	1.932997
Kurtosis	-1.29176
Skewness	-0.12938
Range	5
Minimum	1
Maximum	6
Sum	615
Count	178
Confidence Level(95.0%)	0.205652

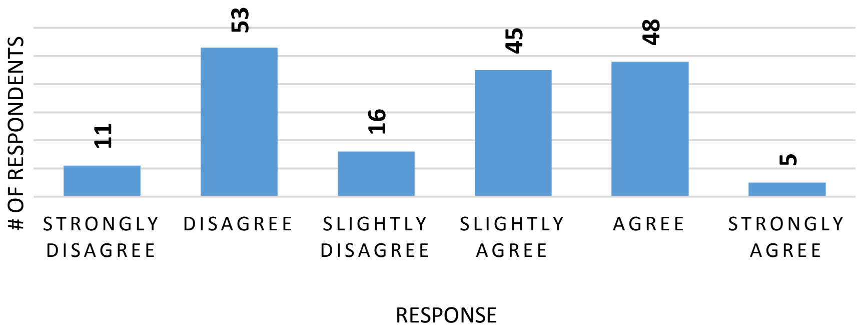


Figure C. 15: Response frequencies for survey-section 1 Question 15

Table C. 41: Response frequencies for survey-section 1 Question 16

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	32	17.98	17.98		Disagree	69.66
Disagree	73	41.01	58.99		Agree	30.34
Slightly Disagree	19	10.67	69.66			
Slightly Agree	30	16.85	86.52			
Agree	21	11.80	98.31			
Strongly Agree	3	1.69	100.00			
Total	178	100.00				

Table C. 42: Descriptive statistics for survey-section 1 Question 16

Q16	
Mean	2.685393
Standard Error	0.101469
Median	2
Mode	2
Standard Deviation	1.35376
Sample Variance	1.832667
Kurtosis	-0.73898
Skewness	0.602718
Range	5
Minimum	1
Maximum	6
Sum	478
Count	178
Confidence Level(95.0%)	0.200244

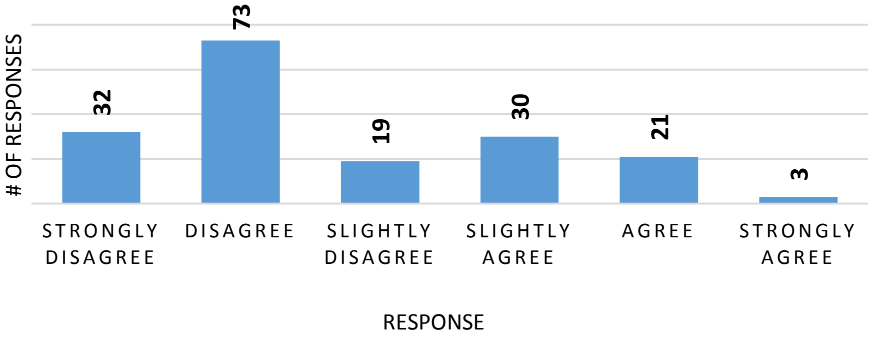


Figure C. 16: Response frequencies for survey-section 1 Question 16

Table C. 43: Response frequencies for survey-section 1 Question 17

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	22	12.36	12.36		Disagree	60.11
Disagree	64	35.96	48.31		Agree	39.89
Slightly Disagree	21	11.80	60.11			
Slightly Agree	30	16.85	76.97			
Agree	39	21.91	98.88			
Strongly Agree	2	1.12	100.00			
Total	178	100.00				

Table C. 44: Descriptive statistics for survey-section 1 Question 17

Q17	
Mean	3.033708
Standard Error	0.106269
Median	3
Mode	2
Standard Deviation	1.4178
Sample Variance	2.010157
Kurtosis	-1.29647
Skewness	0.240613
Range	5
Minimum	1
Maximum	6
Sum	540
Count	178
Confidence Level(95.0%)	0.209717

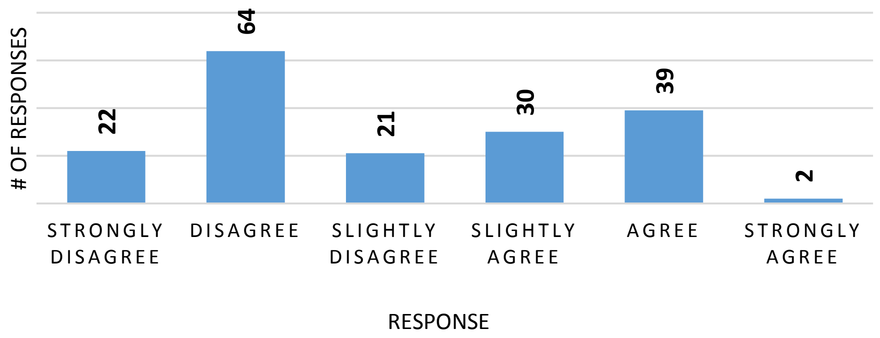


Figure C. 17: Response frequencies for survey-section 1 Question 17

Table C. 45: Response frequencies for survey-section 1 Question 18

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	7	3.93	3.93		Disagree	34.83
Disagree	36	20.22	24.16		Agree	65.17
Slightly Disagree	19	10.67	34.83			
Slightly Agree	50	28.09	62.92			
Agree	51	28.65	91.57			
Strongly Agree	15	8.43	100.00			
Total	178	100.00				

Table C. 46: Descriptive statistics for survey-section 1 Question 18

Q18	
Mean	3.825843
Standard Error	0.102591
Median	4
Mode	5
Standard Deviation	1.368741
Sample Variance	1.873453
Kurtosis	-0.90771
Skewness	-0.33604
Range	5
Minimum	1
Maximum	6
Sum	681
Count	178
Confidence Level(95.0%)	0.20246

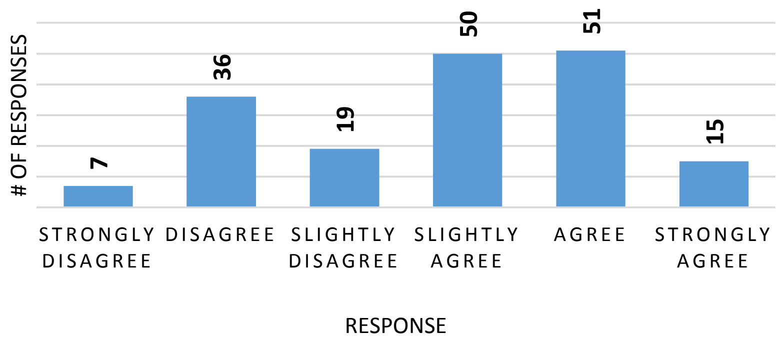


Figure C. 18: Response frequencies for survey-section 1 Question 18

Table C. 47: Response frequencies for survey-section 1 Question 19

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	16	8.99	8.99		Disagree	57.30
Disagree	54	30.34	39.33		Agree	42.70
Slightly Disagree	32	17.98	57.30			
Slightly Agree	34	19.10	76.40			
Agree	38	21.35	97.75			
Strongly Agree	4	2.25	100.00			
Total	178	100.00				

Table C. 48: Descriptive statistics for survey-section 1 Question 19

Q19	
Mean	3.202247
Standard Error	0.102764
Median	3
Mode	2
Standard Deviation	1.371047
Sample Variance	1.879769
Kurtosis	-1.15771
Skewness	0.134471
Range	5
Minimum	1
Maximum	6
Sum	570
Count	178
Confidence Level(95.0%)	0.202801

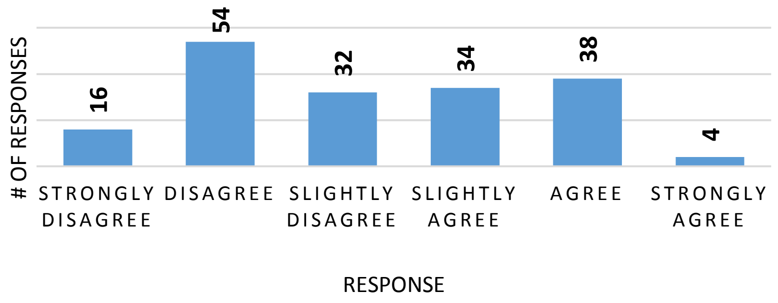


Figure C. 19: Response frequencies for survey-section 1 Question 19

Table C. 49: Response frequencies for survey-section 1 Question 20

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	64	35.96	35.96		Disagree	82.02
Disagree	68	38.20	74.16		Agree	17.98
Slightly Disagree	14	7.87	82.02			
Slightly Agree	11	6.18	88.20			
Agree	15	8.43	96.63			
Strongly Agree	6	3.37	100.00			
Total	178	100.00				

Table C. 50: Descriptive statistics for survey-section 1 Question 20

Q20	
Mean	2.230337
Standard Error	0.104424
Median	2
Mode	2
Standard Deviation	1.393196
Sample Variance	1.940995
Kurtosis	0.600135
Skewness	1.24122
Range	5
Minimum	1
Maximum	6
Sum	397
Count	178
Confidence Level(95.0%)	0.206077

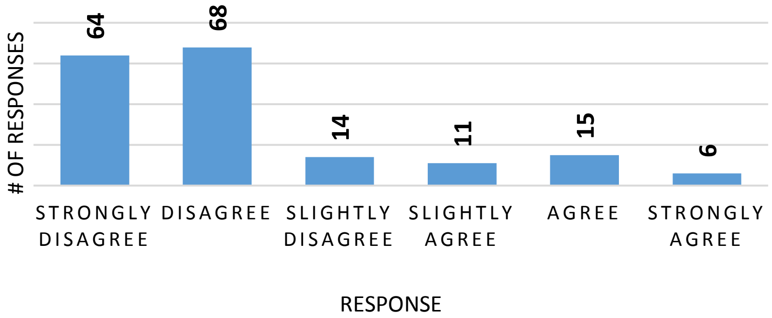


Figure C. 20: Response frequencies for survey-section 1 Question 20

Table C. 51: Response frequencies for survey-section 1 Question 21

Response	**Frequency**	**%**	**Cumulative %**		**Response Category**	**%**
Strongly Disagree	23	12.92	12.92		Disagree	65.73
Disagree	71	39.89	52.81		Agree	34.27
Slightly Disagree	23	12.92	65.73			
Slightly Agree	27	15.17	80.90			
Agree	32	17.98	98.88			
Strongly Agree	2	1.12	100.00			
Total	178	100.00				

Table C. 52: Descriptive statistics for survey-section 1 Question 21

	Q21
Mean	2.88764
Standard Error	0.102924
Median	2
Mode	2
Standard Deviation	1.373175
Sample Variance	1.885609
Kurtosis	-1.07533
Skewness	0.429776
Range	5
Minimum	1
Maximum	6
Sum	514
Count	178
Confidence Level(95.0%)	0.203116

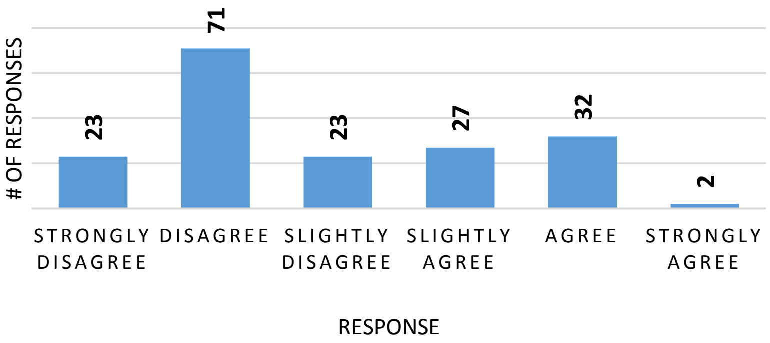


Figure C. 21: Response frequencies for survey-section 1 Question 21