THE INFLUENCE OF DEMOGRAPHIC FACTORS ON THE CYBERSECURITY AWARENESS LEVEL OF INDIVIDUALS IN AN ACADEMIC ENVIRONMENT

Juan Carlos Barrera Vazquez

A THESIS SUBMITTED TO THE FACULTY OF GRADUATE STUDIES IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF ARTS

GRADUATE PROGRAM IN INFORMATION SYSTEMS AND TECHNOLOGY

YORK UNIVERSITY

TORONTO, ONTARIO

May, 2019

© Juan Carlos Barrera Vazquez 2019

Abstract

Nowadays the notion of cybersecurity has claimed center stage in the daily life of individuals and organizations. Losses incurred to cyber-attacks are the result of faulty human interactions with new information and communication technologies (ICT's) in the context of cyberspace. The fast pace of technology discoveries has surpassed the understating of most ICT users. Consequently, individuals become unaware of such changes in different ways.

This research examines differences and/or relationships in awareness level of individuals towards cybersecurity issues, considering four basic demographic factors: Gender, Age, Education, and Employment. The data set for this study originated from university students pursuing a bachelor's degree in information systems and/or information technology. Finally, the results from this study are not conclusive and cannot be generalized due to several natural research limitations. However, several observations found in this study may contribute to the general body of knowledge for cybersecurity, and to stimulate future research.

Acknowledgements

Henry Ward Beecher wrote once that: “The unthankful heart discovers no mercies; but let the thankful heart sweep through the day and as the magnet finds the iron, so it will find, in every hour, some heavenly blessings!” – Throughout my life I have experienced many unexpected blessings, moments of divine mercy, and I can certainly attest that we can always find something to be thankful for. Consequently, it is in light of profound gratitude that I want to thank first God in Jesus Christ for his mercy and blessings, and for the gift of inspiration throughout my life and all of my academic endeavors.

I also want to express my deepest gratitude to Dr. Jimmy Huang, for his guidance and support during my years of studies at York University. He has certainly influenced my career path and my future academic pursuits.

Finally, I am very grateful to my family and to Miss. Elizabeth Lanzo for their continued support of my professional and academic aspirations. This academic work would not be possible without all of them.

Thank you all!

Table of Contents

List of Tables

List of Figures

List of Abbreviated Terms

CNSS = The Committee on National Security Systems

DHS = Department of Homeland Security

DM = Data Mining

IaaS = Infrastructure as a Service

ICT = Information and Communication Technologies

IoT = Internet of Things

IP = Internet Protocol

IS = Information System

ISF = Information Security Forum

ISO = International Organization for Standardization

IT = Information Technology

ML = Machine Learning

NIST = National Institute of Standards and Technology

PaaS = Platform as a Service

SaaS = Software as a Service

SCADA = Supervisory Control and Data Acquisition

SETA = Security Education, Training and Awareness

SPSS = Statistical Package for the Social Sciences

UK = United Kingdom

USA = United States of America

List of Symbols

(α) = Alpha Coefficient

$\bar{c}$ = The average inter-item covariance among the items

H_0 = Null Hypothesis

H_1= Alternative Hypothesis

N = The number of items,

n = Sample size

n_c = Number of concordant pairs

n_d = Number of discordant pairs

% = Percentage

p-value = Probability value

R_i = Rank of the sample size

(*τ)* = Tau

(*τc)* = Tau c

(*τb)* = Tau b

U = Mann-Whitney U test

$\bar{v}$ = The average variance

≥ Greater than or equal to

≤ Less than or equal to

= Equal

Chapter One

Introduction and Motivation

1.1 Background

Nowadays individuals and business organizations are capitalizing on the benefits of easier access to information through innovative internet technologies and also through their scalable and cost-efficient infrastructures and devices. Subashini & Kavitha (2011) stated that small and medium size companies are now accessing online information at unprecedented levels, to optimize business applications and information asset utilization. Consequently, most service providers currently enjoy unique opportunities in the marketplace to develop, and to prolong the utilization of innovative information technologies as building blocks for all productive activities within commercial and non-commercial entities. However, despite all of the above-mentioned benefits, the unchartered ecosystem of data and information security is still an intimidating concern for everyone. Clavister (2009) pointed out that many executives hold back in terms of fully adopting new information technology services and applications due to their security concerns over the management of data in cyberspace.

De Bruijn & Janssen (2017) noted that cybersecurity is one of the most critical challenges for anyone who is connected to the internet today, and yet, visibility and public awareness towards this issue remains limited. Further, Arora, Nandkumar, & Telang (2006) stated

that individuals consider the internet to be a safe environment. Therefore, their behavior does not reflect a high level of security awareness when confronted with new cyber threats. Consequently, organizations continue to incur in higher operations costs associated with cybersecurity incidents, disaster recovery, and business continuity planning. These business-technology grievances might result in disruptions of information systems and data transfers.

1.2 Recent Events

In recent years, several technology discoveries have led the world to a higher level of interconnectivity of physical devices through the internet (Internet of Things – IoT) (Hernández-Ramos, Jara, Marın, & Skarmeta, 2013). These devices depend on complex communication networks and intertwined systems, that continue to populate all aspects of human space (Ten, Liu, & Manimaran, 2008). In these complex arrays of devices and networks, the greatest danger occurs when an unauthorized entity gains access to the administrator's security privileges to exert control on actions that may cause catastrophic damages (Ten et al., 2008), such as the recent case of Ukraine's power grid cyber-attack on December 23, 2015.

In addition, evidence of continuous unauthorized access to critical industrial systems is noted through recent attacks to Supervisory Control and Data Acquisition (SCADA) systems. These computerized real-time process control systems are geographically dispersed to satisfy continuous distribution operations from multiple industrial units. Zhu, Sastry & Joseph (2011) stated that SCADA systems are increasingly subject to serious

damage and disruption by cyber means due to their standardization, their connectivity to other networks, and due to human errors in their operations. However, general security awareness of cyber-threats to SCADA systems remains limited and insufficient. Therefore, there is little protection from the latest cyber threats.

Buczak & Guven (2016) noted that recent literature in the field of cybersecurity focuses more on machine learning (ML) and data mining (DM) methods for cyber analytics in support of intrusion detection and security improvement, rather than building security awareness for users in general. This remarked emphasis is due to the fact that such innovative methods rely less on user's awareness levels towards security, and more on the output produced from the latest information technologies that seek out more efficient outcomes.

1.3 Security and its Challenges

Data generated through new devices and transmitted at faster speeds than ever, has contributed to a large source of vulnerabilities for all users of data. Elmaghraby & Losavio (2014) noted that any quality of life improvements that result from sharing data seems to justify any new risk-taking in cyberspace. However, the vast amount of private data available about location, activities, preferences, hobbies, etc. is giving rise to new challenges in cybersecurity awareness (Arora et al., 2006), and within the modern legal frameworks, which have become ill to understand them and to legislate them accordingly (Gorham-Oscilowski & Jaeger, 2008).

Wang, Wang, & Ren (2009) affirmed that some of the current cybersecurity challenges are associated with accessibility vulnerabilities, virtualization vulnerabilities, new web applications, code injection and cross-site scripting, physical control of data, data verification, tampering, integrity, confidentiality, data loss and theft, data authentication, and IP spoofing, to mention just a few of them. Further, unforeseen threats to data security on ever growing workloads are only intensifying the security risks, and subsequently, fears from everyone (Seccombe, Hutton, Meise, Windel, & Mohammed, 2009)

Modern service environments (i.e. cloud and non-cloud) only add up to the current uncertainty of data security. Cloud computing utilizes three delivery forms for web services: 1) IaaS, 2) PaaS, and 3) SaaS, which provide infrastructure resources, application platform, and software as service to the consumer; respectively (Hassan, 2011). These forms of delivery also demand a different level of security requirements in the cloud environment and its networked clients, since inherited capabilities convey inherited security risks associated with data management.

The complexity of modern cybersecurity issues must be carefully studied from different angles, since computing and data transfer capabilities continue to evolve in new directions. Therefore, it is expected that industry and academia join efforts in the study of cybersecurity. Moreover, newly discovered vulnerabilities to cyber-attacks clearly indicate that complex innovations in information and communication technologies (ICT's) (Furnell, Bryant, & Phippen, 2007) will contribute to increase users' unawareness of the latest cybersecurity issues. Lastly, Sophos (2009) concluded that the vulnerability to information security is due to the fact that individuals are not aware of overall cybersecurity risks and threats.

1.4 The Importance of Security Awareness

Individuals and commercial entities have now become more dependent on the extensive use of information and computing systems, to complete essential activities, and to devise new forms of conducting their doings. Further, in an effort to increase productivity and efficiency, both entities need to keep their data and information assets secure. Bada & Sasse (2014) noted that to achieve the above-mentioned, technical measures and behavioral policies have been deployed extensively. However, there is ample evidence that compliance with policies regarding desirable behavior to handle information assets in a secure manner is always uncertain, since the correct behaviors remain unknown for most individuals (Caputo, Lawrence, Freeman, & Johnson, 2014).

Kirlappos & Sasse (2012) suggested that it is critical to move from awareness to tangible behaviors, to secure information assets and systems, and to further develop policies that specify appropriate behaviors for individuals towards security of information in cyberspace (Kirlappos, Parkin, & Sasse, 2014). Further, despite of continuous efforts to improve security, there is ample evidence that major cyber events will continue to occur everywhere. Training as currently conceived is not delivering the benefits expected, as manifested in recent cybersecurity statistics. Caputo et al., (2014) illustrated the above-mentioned, by having spear phishing as an example that showed that framing had no significant effect in security improvement. In addition, it was noted in the study that effective embedded training must take into account not only framing and security experience, but also perceived security support, information load, preferred notification method, individual awareness level and more (Kirlappos et al., 2014).

According to the National Institute of Standards and Technology (NIST), individuals know the answers to awareness questions but their actions do not reflect clear understanding of consequences (NIST Report, 2003). The primary purpose of security awareness is to render people amenable to change (Winkler & Manke, 2013). However, individuals do not just follow advice or instructions even if they come from a person of authority. Individuals exercise their own judgement as they rely on their own security education and learning over time (Roper, Fischer & Grau, 2006). Moreover, in many cases, individuals will have to overcome existing patterns in order to form new habits. If asked, “the conscious mind will invent stories to rationalize these things that the unconscious mind is telling them to do” (Hogan, 2005, p. 41). The desire to behave consistently will drive individuals to honor a previous commitment to an ideal or an activity (Cialdini, 2009). Consequently, as individuals begin to think of themselves as users who are security-conscious, they begin to act in accordance with this image (Hogan, 2005).

1.5 Interpretation of Security

In current literature, there is a vast array of interpretations for cybersecurity and security awareness. Some definitions for the above-mentioned terms make a special emphasis on the security of data, others on the security of information, and some others on the security of information processes. Further, “Information Security” has claimed center stage in literature as the key leading concept in the definition for cybersecurity. However, Information security only focuses on protecting the confidentiality, integrity and availability of information (ISF, 2003). Consequently, information security awareness deals with the

use of security awareness programs to create and maintain security-positive behavior as a critical element in an effective information security environment (ISF, 2003). According to Hansche (2001) “the goal of a security awareness program is to heighten the importance of information systems security and the possible negative effects of a security breach or failure” (p. 14).

On one hand, differences in knowledge of information security is one of the main risks that individuals are exposed to in cyberspace. Further, when individuals lack the proper knowledge, they become unaware that they will fail to understand and/or be aware of future cyber risks that they could be exposed to in cyberspace, and that they are ultimately responsible for securing their own cyber environment (Furnell, Valleria, & Phippen, 2008). One of the main reasons for differences in knowledge of information security awareness is that there is no enforcement by a third party to ensure continuity of security practices (Kumar, Mohan, & Holowczak, 2008).

Conversely, business organizations rely solely on individuals’ knowledge and behaviors to keep abreast of security threats and current best practices (Kumar et al., 2008). However, despite the significant information security risks resulting from human factors, organizations have and continue to invest mostly in technology-based information security solutions (e.g. firewalls, antivirus software, machine learning tools, and intrusion detection systems) to defend organizational assets and infrastructure (Furnell et al., 2008). Indeed, the state-of-art technology-based security solutions provide a layer of protection. However, these solutions alone cannot supply the required security to defend organizational assets from a wide range of threats and attacks, since most critical issues of information security systems depend on the users, their decisions, and ultimately, their

informed or uninformed interactions in cyberspace (refer to Appendix I) (Kumaraguru, Rhee, Acquisti, Cranor, Hong, & Nunge, 2007).

1.6 Motivation

Cybersecurity is a new area of research for many experts in IT/IS in academia and in industry. There are different approaches to the study of this subject, as noted in the literature review. However, there is no general agreement on how to study awareness level of individuals towards security issues in cyberspace. Further, the purpose of becoming aware is to avoid cyber-incidents, as they relate to information losses and substantial damages for individuals and organizations.

The motivation of this study is to examine how the outcome of demographic factors affect the cybersecurity awareness level of individuals. Moreover, this study focuses on students currently enrolled in higher education. Particularly those individuals who pursue careers in the area of Information Systems (IS) and/or Information Technology (IT) at the bachelor's level. This is in direct response to the general belief that such backgrounds of study are conducive to higher and/or similar awareness level of security issues in cyberspace, since exposure to IT and/or IS subjects and best practices is more available.

1.7 Research Problems

In order to investigate the outcome of demographic factors in cybersecurity awareness level of individuals, it is imperative to narrow the scope of such factors to those of essential

nature. Further, in this case, this research focuses on four factors: 1) gender, 2) Age, 3) education, and 4) employment. Consequently, it examines:

1. The difference between the cybersecurity awareness level of individuals and their gender, if any.
2. The relationship between the cybersecurity awareness level of individuals and their age, if any.
3. The relationship between the cybersecurity awareness level of individuals and their education level completed, if any.
4. The relationship between the cybersecurity awareness level of individuals and their current employment status, if any.
5. The implications of the differences and/or relationships found through this study, in terms of the cybersecurity awareness level of individuals, if any.

1.8 Main Contributions

There are several aspects of this study that warrant an innovating character to its focus and approach to the study of cybersecurity awareness. First, it uses secondary data available to the study of cybersecurity awareness level of individuals. Second, the secondary data includes outcomes from individuals pursuing higher education at the bachelor's level in Information Systems and/or Information Technology. Third, it explores the outcomes of a specific group of demographic factors on cybersecurity awareness level, while delivering a series of outcome comparisons among groups of individuals

(participants in the study) located in three different geographic locations (Germany, The United Kingdom, and The United States of America). Lastly, it provides and overview of the implications of having security awareness or not, in individuals and in business organizations.

1.9 Summary

In this section, this research study provided a general introduction to the notion of cybersecurity awareness, through its conceptualization as information and data security awareness. It was also noted that some of the views towards cybersecurity referred to productivity effects on small and medium size enterprises, while identifying some deficits in the adoption of security awareness as an organizational goal. In addition, this section of the study illustrated some of the current views towards information security awareness, by evidencing the strong emphasis on investments in state-of-the-art technologies rather than user's security awareness programs.

This section also highlighted the importance of security awareness, which concluded that when individuals lack the proper security awareness knowledge (skills) they will fail to understand and/or be aware of the cyber risks and threats that they are exposed to in cyberspace (refer to Appendix H). Finally, the motivation and research problems are presented in a succinct style, in an effort to inform the readers about the purpose and scope of this study.

1.10 Thesis Structure

Next sections of this thesis are organized as follows: Chapter 2 provides an overview of literature in the field of cybersecurity and security awareness; Chapter 3 presents the data sets (from the sample) and methodology applied in this study; Chapter 4 discusses results from the study and it answers the research questions posted earlier in the methodology section; Chapter 5 presents conclusions and recommendations for future lines of research; Further, the appendix section shows additional tables of results; and finally, The references section lists all sources consulted to complete this research study.

Chapter Two

Literature Review

2.1 Current Perceptions of Cybersecurity

Recent cyber-attacks to business organizations and to government institutions have prompted everyone to think more seriously about security issues regarding cyberspace interactions (Arce, 2003). Business organizations consider now cybersecurity as a strategic risk, while governments consider cybersecurity as a national security matter. Further, “the extent to which users from all origins take precautionary actions against cyber risks is conditional upon how they perceive the value of information security relative to other important personal goals” (Nguyen, Rosoff, & John, 2017, p. 1). Indeed, one of the biggest challenges for all information users is to clearly define the extent to which everyone understands information security in the context of cyberspace (i.e. to accept a unified perspective of cybersecurity, risks, and threats). Diakun-Thibault (2014) stated that “the absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity potentially impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity, while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges” (p. 13).

Current literature continues to highlight the need for a multidisciplinary approach towards the conceptualization of cybersecurity. However, Chang (2012) noted that academic disciplines adopt themes according to self-interest to define cybersecurity. Computer science, electrical engineering, and mathematics are the leading disciplines in the quest for a definition of cybersecurity. Moreover, these disciplines have also struggled to agree on what the term ‘security’ means, and under what context is more relevant to apply it (Friedman & West, 2010; Cavelty, 2008). In addition, Cavelty (2010) stated that “there are multiple interlocking discourses around the field of cybersecurity. Consequently, the only way to understanding the true nature of this concept is by deconstructing it, and by looking at it from the domains of ‘cyber’ and ‘security’, as these domains may reveal some legacy definition issues” (p. 14) (Cavelty, 2008).

2.2 Defining Cybersecurity

The International Organization for Standardization (ISO) defines cybersecurity or cyberspace security “as the preservation of confidentiality, integrity and availability of information in the cyberspace” (ISO 27000). Moreover, The National Institute of Standards and Technology (NIST, 2003) defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks”.

The Committee on National Security Systems (CNSS-4009) defines cybersecurity as “the ability to protect or defend an enterprise’s use of cyberspace from an attack, conducted via cyberspace, for the purpose of: disrupting, disabling, destroying, or maliciously

controlling a computing environment/infrastructure; or, destroying the integrity of the data or stealing controlled information".

All these definitions consider different concepts, as they represent specific views, attributes, and/or interests from the entities defining the concept (refer to Appendix G). However, there are some common elements in the above-mentioned definitions for cybersecurity that might permeate across the literature, such as: purpose, means, and damages. Furthermore, other definitions focus more on capabilities, legal rights, and/or event occurrence. For instance, Lewis (2006) considered that cybersecurity entails the safeguarding of computer networks, and the information they contain from penetration, and from malicious damage and disruption. In addition, The US Department of Homeland Security in its 2014 report, conceptualized "cybersecurity as the activity or process, as ability or capability, or state, whereby information and communication systems and the information contain therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation". (DHS, 2014).

In most cybersecurity definition, users debate the trade-offs between the conceptualization of cybersecurity as information security and the critical attributes that they desire to maximize (Arce, 2003). Sasse, Brostoff, & Weirich (2001) further stated that humans are the weakest link in the cybersecurity chain. However, the security of any cyber infrastructure mostly depends on how users exercise self-protective information security behavior, and on how users understand the definition of cybersecurity in the context in which they operate (Furnell et al., 2007). Lastly, as Charles Leslie Stevenson (1908-1979) noted once, "to choose a definition is to plead a cause".

2.3 Information Security

The aim of information security is to ensure business continuity and to minimize business damage by preventing and minimizing the impact of security incidents (Von Solms, 1998). Further, according to Pfleeger & Pfleeger (2007), the critical attributes of information security are: Confidentiality, Integrity, and Availability (NIST, 2003). In this context, users involved in a security process need to possess the required knowledge about their security related roles and some form of education and/or training (Van Niekerk, 2005). In business organization, user-education or information security awareness programs are the most cost-effective initiatives against cyber-attacks. (Dhillon, 1999).

Tipton & Krause (2007) noted that technology alone cannot deal with all information security risks, and that people in organizations are the primary and most critical line of defense against cyber incidents and attacks (Tipton & Krause, 2007; IT Governance Institute, 2008). Further, “Any organization thinking of mitigating information security risks through purely technological countermeasures shall fail eventually” (Mitnick & Simon, 2003). This is due the fact that security threats continue to grow, as individuals rely more on internet technologies and applications for all their doings. Indeed, new risks or threats are usually associated with higher dependencies on new technologies, since many of the new technologies carry inherited vulnerabilities (Furnell, Bryant & Phippen, 2007).

Internet users are more vulnerable to cyber-attacks as a result of growing complexity of new information and communication technologies (ICT’s) (Furnell, Bryant & Phippen, 2007). Sophos (2009) stated that the vulnerability to information security is also attributed to the fact that individuals are not aware of overall cybersecurity risks. Nevertheless,

getting users to become aware and to participate in safe online behavior are only two of the most significant challenges today (Gandy, 2003). Internet users are very concerned about the privacy and security of their information. However, many of them are willing to overlook cybersecurity awareness best practices due to exchange for economic gain or because of difficulty to accept new risks (Finch, Furnell, & Dowland, 2003).

2.4 Cybersecurity Awareness

Several approaches have been proposed in the field of security awareness. However, there is no general consensus on what research streams should be considered as tenet in the production of new knowledge. For instance, Maseti & Pottas (2006) studied cybersecurity awareness in terms of the applicability of a role-based security awareness model in hospitals; Van Niekerk & Von Solms (2004) focused their efforts on outcome-based education in information security awareness, while Schlienger & Teufel (2003) analyzed socio cultural measures as a critical framework in the analysis of information security culture in business organizations.

Other research efforts have considered risk management approaches towards understanding information security in the context of situation awareness models (Whitman & Mattord, 2004). In addition, Siponen (2006) stated that information security management should be considered as process-oriented tasks, rather than content-oriented procedures. Further, Von Solms, (2010) noted that cybersecurity should be studied in the context of governance, as security awareness efforts require policy making

and proper governance structures to make it effective and to facilitate adoption and learning.

Shaw, Chen, Harris, & Huang (2009) noted in their study, that individuals learn more from information security awareness training that address higher information concerns because of self-interest. However, the study used a very extensive survey, designed to assess learning before and after the experiment, and not necessarily to measure acquired awareness level. Further, although results were not conclusive, the study certainly provided some direction on the application of surveys to assess information security awareness levels of individuals.

Surveys have been used as the primary instrument to assess awareness levels in recent studies. Dinev & Hu (2007) found that survey respondents who believed in the necessity of anti-spyware technology were more likely to use it. In addition, the study also concluded that the level of understanding of technology innovations has an impact on the adoption of such technology. Consequently, aversion to some technologies due to poor understanding will cause individuals to reject any learning that relates to them (Dinev & Hu, 2007).

Another approach to the study of cybersecurity awareness is situation awareness (SA). This awareness is commonly defined in terms of what information is important for a particular purpose or goal. The concept of situation awareness is frequently applied to operational situations, where specific reasons require individuals to have an identifiable awareness level for a specific context. Other situation awareness research in information systems has studied the privacy of internet users (Sim, Liginlal & Khansa, 2012); Some other studies have focused their efforts on information control in counterterrorism (Oh,

Agrawal, & Rao, 2011) (Abidi, Aragam, Yi, & Abidi, 2008), and automated systems in the detection of malware (Dube, Raines, Grimaila, Bauer, & Rogers, 2013).

Regardless of the approach applied to the study of cybersecurity awareness, *Information Security Awareness* (ISA) seems to represent it as the primary definition in current literature (Siponen, 2006). Further, Hoffer & Straub (1989) noted that information security is of critical importance, as information security techniques or procedures can be misused, misinterpreted or missed by end-users, (Goodhue & Straub, 1989; Ceraolo, 1996; Straub & Welke, 1998) causing mistakes and ultimately damages. Therefore, increased awareness should minimize user-related mistakes, and maximize the efficiency of security techniques (Straub & Welke, 1998). To this extent, Information security awareness can be defined as the level of comprehension that users have about the importance of information security best practices (Shaw et al., 2009).

Siponen (2000) stated that “to increase understanding of problems relating to awareness, two categories can be outlined, framework and content. Framework can be approached in a structural manner and by quantitative research, while content constitutes a more informal interdisciplinary field of study, and it should be approached using qualitative research methods” (p. 32). However, “the effective management of information security requires a different approach, and it may include improved awareness in tandem with updated technical knowledge” (p. 33). (Von Solms & Von Solms, 2004).

2.5 Issues in Security Awareness

Cyberattacks, hacks and security breaches are the most noticeable issues in cybersecurity today. Arora et al., (2006) noted that cyber incidents are more frequent than ever, and that concerns from individuals (users) focus more on visible incidents rather than the full spectrum of cyber-risks. Further, Doty (2015) stated that communication about cybersecurity issues is very difficult to achieve, since individuals tend to fictionalize cybersecurity risks as a way to deal with any fears, and/or the lack of awareness about the subject. Schlienger & Teufel (2003) suggested that security awareness is a dynamic process where individuals need to be informed continuously about changes. Consequently, any awareness program must be ongoing and an integral part of a culture of security in society and organizations. In addition, to become aware and to stay aware requires the support of cross-disciplinary assessment tools, where individual security awareness must be assessed and monitored continuously from different contexts.

Humaidi & Balakrishnan (2013) stated that "many individuals do not comply with expected behaviors for safety and security, while conducting their doings in cyberspace. This is because individuals are not aware of (or do not perceive) the risks or, they do not know (or fully understand) the appropriate behavior to follow while interacting in cyberspace" (p. 2). Consequently, any cyber security-awareness campaign should aim at influencing the adoption of secure behavior online. However, Rogers (1985) suggested that effective influencing requires more than simply informing individuals about the scope of their behaviors. It requires acknowledgement of fears and doubts (self-assessment),

acceptance of relevant information, and an appropriate response in tandem with expected behaviors (Witte, 1993).

The conceptualization of security awareness continues to change overtime, as evidenced by new trends in ICT's innovations. NIST (2003) stated that "awareness is not training, and that the purpose of awareness is simply to focus attention on security, while allowing individuals to recognize IT security concerns and to respond accordingly" (p. 4). To this end, behavioral science approaches have been applied to the notion of awareness. Dolan, Hallsworth, Halpern, King, & Vlaev, (2010) studied factors that are critical in influencing human response to concerns, while Hogan, Motivation, & Bolhuis (2005) recognized that individual knowledge, skills, and understanding of cybersecurity risks are informed by experiences, attitudes and beliefs, which translate into security awareness.

Security awareness is currently enforced through procedures and processes, and individuals easily become overwhelmed and fatigued by/through them. O'Donnell (2018) warned that It could be stressful to remain at a high level of vigilance and security awareness. This is because 'security fatigue', can be a hazardous endeavor for individuals, since there are no additional stimuli (Ahluwalia, 2000), beyond fear invocation that can lead to sustained appropriate behaviors in an ever-changing cyber-environment (ISF, 2014).

2.6 Related Approaches to the Study of Security

The study of security has been a main concern for many academic disciplines in recent years. Behavioral scientists have applied four main theories in the study of security: 1) Theory of Planned Behavior (TPB), 2) General Deterrence Theory (GDT), 3) Protection

Motivation Theory (PMT) and 4) Technology Acceptance Model (TAM). Further, these theories present an overview of determinants that have been proven to influence individuals' behavioral intention. However, the emphasis of these theories is predominantly on improving concrete training and awareness measures that can be developed in different environments.

This is indeed of great value for practitioners and consultants that undergo the process of designing Security Education, Training and Awareness (SETA) programs. However, in the area of information security, several studies have focused their efforts on policies and procedures, as a way to prevent incidents. Abraham (2011) noted that individuals (users) are the weakest link in the security chain. Therefore, education should be encouraged, in an effort to improve awareness (D'Arcy & Hovav, 2009). Moreover, theories from social psychology and criminology have also been adopted to IS literature (Mishra & Dhillon, 2005), to explain and predict individuals' security-related behavior and awareness level in organizations.

Despite the diverse approaches to security studies, there is still no up-to-date overview of dominant theories and main results that can unify and reconcile different views of security and awareness. In addition, one common denominator in the study of security is the dependency on self-reported information regarding the variables under study (i.e. awareness, literacy, behaviors, attitudes, etc.). Podsakoff & Organ (1986) stated that factors like individuals' intentions, attitudes, motivations or satisfaction are not verifiable by other means rather than self-reporting. However, the use of self-reports to measure security-related behavior might lack validity because self-reports are prone to the problems of common method variance, and restricted interpretation (Podsakoff & Organ,

1986). Lastly, Workmann, Bommer, & Straub, (2008) concluded that a single self-report is not sufficient predictor of employees' perceptions of security awareness. However, continuous studies through diverse self-reports might provide more insights regarding changes in behavior that might be desirable to improve security awareness.

2.7 Self-reported Awareness

The notion of self-awareness is relatively recent. According to Duval & Wicklund (1972), self-awareness is the study of the conditions which cause the consciousness to focus on the self as an object. In this theory, self-awareness has motivational properties deriving from social feedback and considered with relation to conformity, attitude-behavior discrepancies, and communication sets. Further, Fenigstein, Scheier, & Buss (1975) studied self-awareness through the development of a scale to assess individual differences in self-consciousness. In this study, it was included the construction of a scale with 38 initial items applied to 130 female and 82 male undergraduate students. However, the findings focused on identifying principal component factors, rather than determining differences in self-awareness level between male and female students.

Goleman (1995) stated that self-awareness is the key cornerstone to emotional intelligence, and that it also represents the ability to monitor our emotions and thoughts from moment to moment to understand and manage our thoughts, emotions, and behaviors. Conversely, Killingsworth & Gilbert (2010) found that almost half of the time we operate on "automatic pilot" or unconscious of what we are doing or how we feel, as our mind wanders to somewhere else other than here and now; rendering the notion of

self-awareness impractical. Further, Kahneman (2013) concluded that “how we feel about the experience in the moment and how we remember the experience can be very different and it share only 50% correlation”. It was noted that such “difference can have significant impact on the story we are telling ourselves, the way we relate to self and others, and the decision we make, even though we may not notice the difference most of the time”. Lastly, Govern & Marsch (2001) studied the manipulation and measurement of levels of situational self-focus, and found that there are differences in public and private self-awareness, and that both are sensitive to changes over time and across situations.

2.8 Other Methodologies in Cybersecurity Awareness

According to the SANS Institute (SANS, 2017), there are two general methodologies to studying cybersecurity awareness level of individuals. The first methodology focuses on assessment of any current security awareness program, with the purpose of determining current awareness level in an organization. Further, the second methodology focuses on quantifying the effect of a proposed awareness training on actual behavior of the trainees. In addition, Belaissaoui & Elkhannoubi (2015) stated that measuring current awareness levels and training effects are conducive to a better security posture. However, there is no agreement as to which methodology delivers more benefits. Nevertheless, both methodologies consider the existence of a training program and/or the implementation of a training program in a business organization.

Kruger & Kearney (2006) proposed the application of surveys in combination with models from social psychology to measure and analyze attitude, knowledge and behavior of

employees in several focus areas, each with its own weighting criteria. Parsons, McCormac, Pattinson, Butavicious, Zwaans, & Calic, (2014) suggested that standardized questionnaires with a focus on attitude, knowledge, and behavior are more appropriate to measure cybersecurity awareness level. Furthermore, other studies focused on specific security issues, rather than the overall awareness level. For instance: Stanton et al., (2005) proposed a study on password-related behaviors and training/awareness; Mylonas et al., (2012) conducted a study on security awareness in smartphone platforms; Furnell et al., (2006) completed a study on understanding the security features within an OS and specific applications; Dodge et al., (2007) focused on using phishing for user security awareness, while Khan et al., (2011) conducted a study on the effectiveness of information security awareness methods based on psychological theories.

2.9 Summary

Finally, this section of the study provided an overview of the literature in the field of cyber-security, information security, and security awareness. Several definitions for cybersecurity were provided, in an effort to illustrate the complexities of defining a concept that users should be aware of, as well as some of the benefits associated with perceived information security awareness. Further, several studies were mentioned to provide some context for the settings for this project, as described in the methodology section next. Finally, the term '*cybersecurity'* is inclusive to the term '*information security'*, since a review of the literature revealed that the latter is only a part of the comprehensive view, and a specific approach to the study of cybersecurity.

Chapter Three

Methodology

3.1 Importance of Monitoring Security Awareness

The number and frequency of cyber-attacks continue to increase in magnitude and level of sophistication (CIG Report, 2017). Most cyber-incidents are designed to take advantage of unsuspecting personnel and/or faulty security protocols. The significance of the human factor in cybersecurity is frequently understated. However, in order to counter cyber-attacks designed to exploit human factors in the information security chain, it is critical to assess cyber-risk awareness levels of individuals, as they continuously change over time (Halima, Shareeful, & Mohammad, 2018).

Abawajy & Kim (2010) stated that information security awareness must follow the objective of reducing information security risks that occur due to human related vulnerabilities. Therefore, security awareness levels must be monitored continuously, in an effort to ensure the cyber-safety of individuals and their information assets and processes (Halima et al., 2018). Further, many organizations have established information security awareness programs to ensure that their employees are informed and aware of security risks, protecting themselves and their integrity. However, in order for a cybersecurity awareness program to add value to an organization, while contributing

to the field of information security, it is necessary to have new methods to study and to measure cybersecurity awareness levels and their changes over time (Wilson & October, 2003).

Kruger & Kearny (2006) noted that cybersecurity awareness deals with the use of security awareness programs to create and maintain security-positive behavior as a critical element in an effective information security environment, while emphasizing the negative effects of a security breach or failure (Hansche, 2001). To this end, The Information Security Forum (ISF, 2003) defined information security awareness as the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly. Here is where a direct inquiry to the different security awareness levels of individuals warrants greater attention from researchers, in an effort to understand what variables might predict a relationship between security awareness levels and the individual itself, and/or what variables could have a direct influence on security awareness levels.

3.2 Purpose of the Study

The purpose of this study is to examine cybersecurity awareness levels of individuals currently enrolled in higher education. Particularly those individuals who pursue careers in the area of Information Systems (IS) and/or Information Technology (IT) at the bachelor's level. This is in response to the general belief that such backgrounds of study are conducive to higher and/or similar awareness level of security issues in cyberspace,

since exposure to IT and/or IS subjects and best practices is more available. Therefore, this study focuses on the influence of demographic factors, if any, on cybersecurity awareness level and any possible relationships associated with the background of individuals pursuing the above-mentioned careers.

3.3 Research Hypothesis

This study is limited to the academic environment of groups of students currently enrolled in a bachelor's degree program in Information Systems and/or Information Technology. Further, it is a general belief that individuals enrolled in higher education in such fields of study are more exposed to current information regarding cybersecurity (i.e. information and data security, cyber-threats, best practices, standards, etc.), and that they remain informed about the latest cybersecurity issues by exposure and/through individual interactions in academic settings.

The hypotheses seek to examine relationships, if any, between cybersecurity awareness level and the background of the participants, focusing specifically on four demographic variables: 1) Gender; 2) Age; 3) Education Level Completed; and 4) Current Employment Status.

Therefore:

H_0(a): There is no difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.

H_0(b): There is no relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.

H_0(c): There is no relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.

H_0(d): There is no relationship between the cybersecurity awareness level of individuals and their current employment status, in an academic setting in higher education.

Alternatively,

H_1(a): There is a difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.

H_1(b): There is a relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.

H_1(c): There is a relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.

H_1(d): There is a relationship between the cybersecurity awareness level of individuals and their current employment status. in an academic setting in higher education.

3.4 Research Questions

To further investigate cybersecurity awareness level of individuals in an academic setting, as stated in the research hypotheses; this study addresses the following research questions, as applicable to individuals who pursue careers in the area of Information Systems (IS) and/or Information Technology (IT) at the bachelor's level:

1. What is the difference between the cybersecurity awareness level of individuals and their gender, if any?

2. What is the relationship between the cybersecurity awareness level of individuals and their age, if any?
3. What is the relationship between the cybersecurity awareness level of individuals and their education level completed, if any?
4. What is the relationship between the cybersecurity awareness level of individuals and their current employment status, if any?
5. What are some of the implications of the differences and/or relationships found through this study, in terms of the cybersecurity awareness level of individuals, if any?

3.5 Survey

The survey that originated the data for this research study to address the hypotheses and research questions comes from the University of Louisville, KY, in the United States. Furthermore, the computer science department at this university developed this survey to assess cybersecurity awareness level of the staff and adjunct faculty, with the purpose of identifying training needs and cybersecurity literacy areas for improvement. A copy of the survey can be found in Appendix D.

The survey follows the Likert scale design, with a rating system from 1 to 5 (1= Very Unaware/Never; 2=Unaware; 3=Neutral; 4= Aware; 5=Very aware/Always), and there are 26 items in this survey. Further, the Likert scale is an ordinal psychometric measurement of attitudes, beliefs and opinions. In each question, a statement is presented in which a respondent must indicate a degree of agreement or disagreement in a multiple-choice

type format. Moreover, the survey does not require the participant to provide a simple and concrete yes or no answer, it does not force the participant to take a stand on a particular topic, but allows them to respond in a degree of agreement.

3.6 Data Set Collection

The Steinbeis University in Germany generated the data for this study and it administered the survey via electronic means to three groups of its student body across three different countries (i.e. United Kingdom, The United States, and Germany). Further, these groups of students fulfilled the sample characteristics required for this study (i.e. individuals who pursue careers in the area of Information Systems (IS) and/or Information Technology (IT) at the bachelor's level). In addition, the survey was also adapted to include some basic demographic elements (four), while avoiding the identification of the participants. Moreover, the survey was administered in English language (as originally developed by its author; The University of Louisville) to voluntary students, and no incentives were provided for the completion of the same.

The Steinbeis University followed its own research protocol involving human participants, and handled all logistics for the survey administration and data collection. Further, the researcher only received the results from the survey in an aggregate form, without any identifying information from the respondents to the survey. This is in full compliance with the confidentiality and anonymity protocols of The Steinbeis University. In addition, the researcher was never involved in the selection of the sample groups or the administration of the survey across countries.

The researcher has served at The Steinbeis University in different professional capacities; from delivering lectures to participating in consulting work projects during the past 10 years. Consequently, the researcher is well familiarized with the research protocols at this university, and the practical advantages that come with having access to its student body network, currently enrolled in different academic programs in Europe, USA, and other countries. Finally, the researcher has agreed to share the results of this study with The Steinbeis University, in an effort to promote future studies of cybersecurity awareness level of individuals, and to participate in the Steinbeis' Cybersecurity awareness project during 2019.

3.7 Reliability of the Survey

The author of the survey does not provide additional information about the reliability of this instrument. Consequently, before running a Cronbach's alpha or factor analysis on scale items, it's generally a good idea to reverse code items that are negatively worded so that a high value indicates the same type of response on every item. In the case of our survey, all items are worded in a positive manner, unifactorial. Therefore, data re codification is not necessary. In addition, the researcher completed the Cronbach's alpha test using the statistical software SPSS. This test is a measure of internal consistency, that is, how closely related a set of items are as a group, and it is considered to be a measure of scale reliability. In other words, the reliability of any given measurement refers to the extent to which it is a consistent measure of a concept, and Cronbach's alpha is one way of measuring the strength of that consistency (SPSS).

Cronbach's alpha can be written as a function of the number of test items and the average inter-correlation among the items (SPSS). The standardized Cronbach's alpha formula is:

$$\alpha = (N \cdot \bar{c}) / (\bar{v} + (N-1) \cdot \bar{c})$$

where N is equal to the number of items, $\bar{c}$ is the average inter-item covariance among the items and $\bar{v}$ equals the average variance. The results for this test are shown below.

	Cronbach's alpha Coefficient
No Adjustment	0.902

Table 1: Results for Cronbach's alpha Coefficient

The alpha (α) coefficient for all items from the survey is 0.902, suggesting that the survey items have relatively high internal consistency. As a general rule, reliability coefficients of 0.70 or higher are considered "acceptable" in most social science research situations. Alpha (α) coefficients that are less than 0.5 are usually unacceptable (SPSS Tutorial).

A common practice when testing for reliability of a survey is to test also individual correlations of all survey items. In some instances, some items might reveal higher or lower correlation levels. Consequently, the items must be deleted only one at a time, in an effort to determine their effect on the rest of the survey items. Further, two survey items (item # 1 and item # 9) presented slightly lower correlations when compared to the rest of the survey items. However, as indicated in the results for the adjusted Cronbach's alpha Coefficient (re-run reliability test), there is no significant effect (coefficient increment) from these two items on the rest of the survey items, Consequently, the researcher decided to keep all original 26 items of the survey.

	Cronbach's alpha Coefficient
With Adjustment	0.904

Table 2: Results for Adjusted Cronbach's alpha Coefficient

3.8 Experimental Settings

For the purpose of this study, the sample selection consisted of three matched groups of 31 students per group, randomly selected, for a total sample size of 93 students (*n*=93). Furthermore, all participants are currently pursuing careers in the area of Information Systems (IS) and/or Information Technology (IT) at the bachelor's level in three different geographic locations; Germany, United Kingdom, and the United States. In addition, due to The Steinbeis University's confidentiality and anonymity protocol, there is no additional information about these groups that could potentially identify them.

3.9 Data Set

The Steinbeis University followed its own research protocol involving human participants, and handled all logistics for the survey administration and data collection. Further, the researcher only received the results from the survey in an aggregate form, without any identifying information from the respondents to the survey. Appendix J shows the data sets coded for input on SPSS.

Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	61	65.6	65.6	65.6
	Female	32	34.4	34.4	100.0
	Total	93	100.0	100.0	

Table 3: Gender Composition – Total Sample

A visual inspection of this table immediately reveals that 65.6% of participants (61 participants) are males, and that 34.4% of participants (32 participants) are females. Although there is no conclusive evidence that gender plays a role in mediating factors that affect cybersecurity awareness and behaviors, Anward, He, Ash, Yuan, Li, & Xu, (2017) noted that gender has some effect in security self-efficacy. Further, it is noteworthy to highlight the gender composition of this sample.

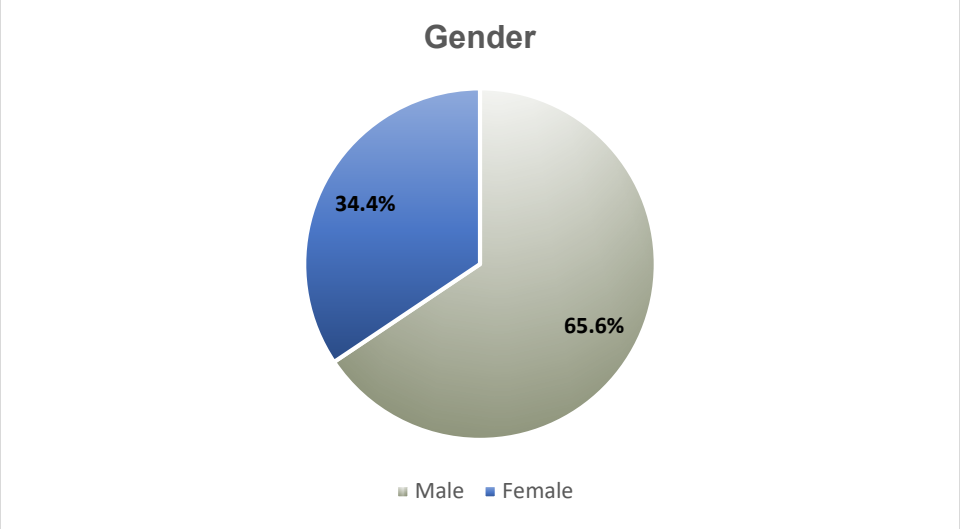


Figure 1: Gender Composition – Total Sample

Age range					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20 to 25	75	80.6	80.6	80.6
	26 to 30	11	11.8	11.8	92.5
	31 to 35	2	2.2	2.2	94.6
	36 to 40	5	5.4	5.4	100.0
	Total	93	100.0	100.0	

Table 4: Age range Composition – Total Sample

A visual inspection of this table immediately reveals that 80.6% of participants (75 participants) are between the ages of 20 to 25 years. This is the youngest group of participants in this study. Further, only 5.4% of participants (5 participants) self-reported being part of the oldest age group (36 to 40 years).

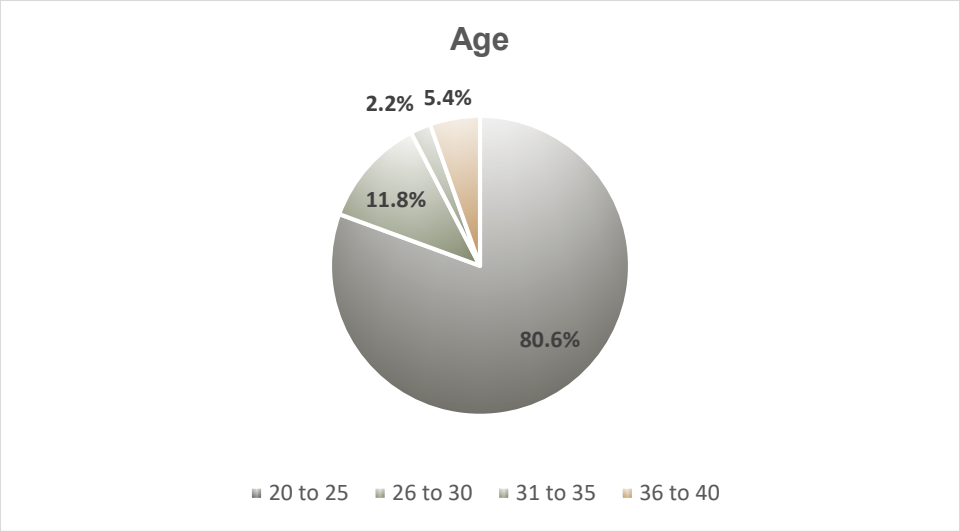


Figure 2: Age Composition – Total Sample

Education Level					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High School	14	15.1	15.1	15.1
	Technical and Professional degree (any degree)	12	12.9	12.9	28.0
	Some University Studies (not completed in full)	56	60.2	60.2	88.2
	University degree (any degree)	11	11.8	11.8	100.0
	Total	93	100.0	100.0	

Table 5: Education Level Composition – Total Sample

A visual inspection of this table immediately reveals that 15.1% of participants (14 participants) have completed high school education level only. Further, 12.9% of participants (12 participants) self-reported to hold a technical/professional degree. Only 11.8% of participants (11 participants) self-reported to have a university degree.

Although there is no conclusive evidence that education level affects cybersecurity awareness level of individuals, Dunkels (2008) stated that individuals at younger age and with lower education level would develop some strategies to treat cyber-threats unconsciously. However, these precautions are not sufficient to avoid harm from the latest cyber-threats. Further, Canbek & Sağıroğlu (2008) found that students have sufficient awareness level in terms of ethical issues. However, they have low awareness levels in terms of issues that require knowledge about rules and protocols. Finally, Tekerek & Tekerek (2013) claimed that information and computer security awareness education and related activities are insufficient.

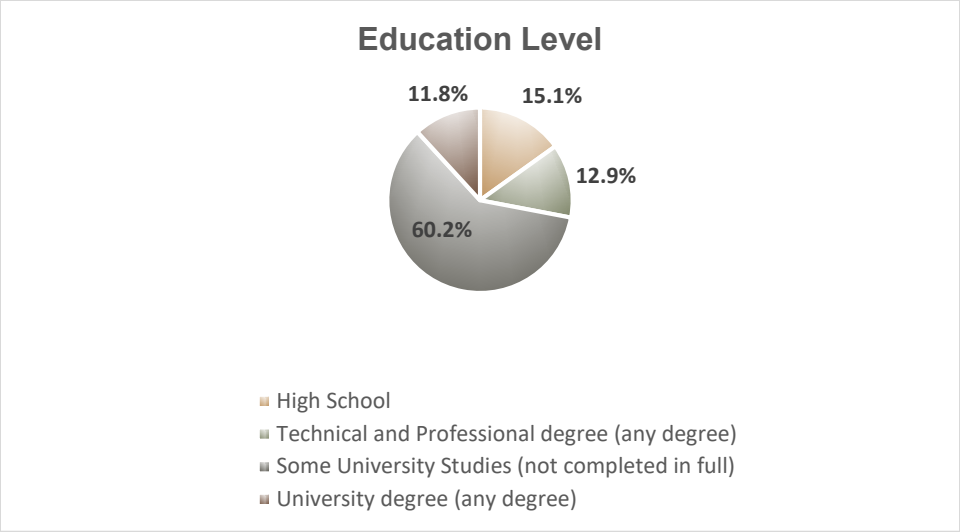


Figure 3: Education Level Composition – Total Sample

Employment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unemployed	12	12.9	12.9	12.9
	Part-time	34	36.6	36.6	49.5
	Full time	47	50.5	50.5	100.0
	Total	93	100.0	100.0	

Table 6: Employment Status Composition – Total Sample

A visual inspection of this table immediately reveals that 12.9% of participants (12 participants) are unemployed. Further, 50.5% of participants (47 participants) self-reported to be employed full time. Only 36.6% of participants (34 participants) self-reported being employed as part-time basis.

Figure 4: Employment Status Composition – Total Sample

3.10 Research Design and Analysis

The purpose of this study is to examine cybersecurity awareness levels of individuals currently enrolled in higher education. Particularly, those individuals who pursue careers in the area of Information Systems (IS) and/or Information Technology (IT) at the bachelor's level. Consequently, this study uses a survey (Cybersecurity Awareness Survey) to investigate all statements posted as null hypotheses, and to answer the research questions.

The variables for this study are:

DV = Awareness (*short for Cybersecurity Awareness*)

IV1 = Gender

IV2 = Age (*short for Age Range*)

IV3 = Education level (*short for Education Level Completed*)

IV4 = Employment status (*short for Current Employment Status*)

3.10.1 Proposed Methods

There are two statistical tests proposed for the analysis of the above-mentioned variables in this study. The first test is Mann-Whitman U test because the dependent variable (DV=Awareness) is ordinal (values range from 1 to 5 in the survey, as defined by its Likert scale design), and the independent variable (IV=Gender) is nominal, since it only takes two values (masculine-feminine, and there is no intrinsic order or hierarchy associated with them). Furthermore, the Mann-Whitney U test is the non-parametric test that is used to compare two sample means (for similar distribution shape) (refer to Appendix F) that come from the same population, and it is used to test whether two sample means are equal or not, when the dependent variable is either ordinal or continuous, but not normally distributed. Mann-Whitney U test is the non-parametric alternative test to the independent sample t-test, and it does not follow any assumptions related to the distribution of the scores. However, some basic assumptions must be observed:

1. The sample drawn from the population is random.
2. Independence within samples and mutual independence is assumed.
3. Ordinal measurement scale is assumed.

Calculation of the Mann-Whitney U:

$$U = n_1 n_2 + \frac{n_2(n_2+1)}{2} - \sum_{i=n_1+1}^{n_2} R_i$$

Where:
U=Mann-Whitney U test
N_1 = sample size one
N_2= Sample size two
R_i = Rank of the sample size

The second test is the Kendall rank correlation coefficient. It measures the ordinal association between two measured quantities. A tau (τ) test is a non-parametric hypothesis test for statistical dependence based on the tau (τ) coefficient. For the rest of the independent variables (IV2, IV3, IV4 – All ordinal), tau-c (τ_c) test is more suitable than tau-b (τ_b) for the analysis of data, based on non-square (i.e. rectangular – Table 7) contingency tables and the monotonic relationship between two variables.

DV=Awareness	**IV2**=Age	**IV3**=Education Level	**IV4**=Employment Status
1=Very Unaware/Never **2**=Unaware **3**=Neutral **4**=Aware **5**=Very aware/Always	**1**=Category A (20-25) **2**=Category B (26-30) **3**=Category C (31-35) **4**=Category D (36-40)	**1**=High School **2**=Technical and Professional degree (any degree) **3**=Some University Studies **4**=University Degree	**1**= Unemployed **2**= Part time **3**= Full time
Contingency Table	Rectangular Table **5x4 (DV-IV2)** DV= Ordinal IV2= Ordinal	Rectangular Table **5x4 (DV-IV3)** DV= Ordinal IV3= Ordinal	Rectangular Table **5x3 (DV-IV4)** DV= Ordinal IV4= Ordinal

Table 7: Contingency Tables Summary for IV2, IV3, IV4

The Kendall's tau-c is a nonparametric measure of association for ordinal variables that ignores ties. The sign of the coefficient indicates the direction of the relationship, and its absolute value indicates the strength, with larger absolute values indicating stronger relationships. Possible values range from -1 to 1. However, a value of -1 or +1 can be obtained only from square tables.

The Kendall tau-c coefficient is defined as:

$$\tau c = 2(n_c - n_d) / n^2 (m-1)/m$$

Where:
n = Sample size
n_c = Number of concordant pairs

n_d = Number of discordant pairs
τ = Number of rows
c = Number of columns
m= min(τ,c)
Kendall's rank correlation provides a distribution free test of independence and a measure of the strength of dependence between two variables.

3.10.2 Metrics and Baselines

As mentioned earlier in this chapter, The Mann-Whitney U test is more broadly used to interpret whether there are differences in the "distributions" of two groups or differences in the "medians" of two groups. However, this is based on whether the distribution of scores (from the answers to the survey – Likert's scale from1 to 5) for both groups of the independent variable have the same shape or a different shape (refer to Appendix F). Furthermore, The Mann-Whitney U test works by ranking each score of the dependent variable (i.e., cybersecurity awareness), irrespective of the group it is in (i.e., males or females), according to its size, with the smallest rank assigned to the smallest value. The ranks obtained for males are then averaged, as are the female's ranks. This results in a mean rank for males and a mean rank for females. If the distributions are identical (there is no difference), which is the null hypothesis of the Mann-Whitney U test (with a baseline p-value set at 0.05 for this study, and a U value ≠ 0), the mean rank will be the same for both males and females. However, if one group (e.g., males) tends to have higher values than the other group, that group's scores will have been assigned higher ranks and will have a higher mean rank (and vice-versa for the group with lower scores). "U = 0 " or "close to 0" means that all values in one group are far greater compared to all the values

in the other group. When this occurs, the test must be rejected, since groups are very different.

It is this difference in mean rank that is tested by the Mann-Whitney U test for statistical significance. Using this approach, different distributions of scores can be accommodated by the Mann-Whitney U test when determining whether values (i.e., via mean ranks) are different between two groups. Moreover, regardless of similar or dissimilar distributions, the Mann-Whitney U test is used to determine whether awareness scores are higher or lower in males versus females based on the use of mean ranks to describe the group differences. However, it is also possible to describe the data using the more familiar median value, but it requires an additional assumption about the shapes of the distributions: to compare medians the distribution of awareness scores for males and females must have the same shape, including dispersion (refer to Appendix F).

As mentioned earlier in this chapter, Kendall's Tau is a non-parametric measure of relationships between columns of ranked data. The Tau correlation coefficient returns a baseline value of 0 to 1, where:

- 0 is no relationship,
- 1 is a perfect relationship.

A quirk of this test is that it can also produce negative values (i.e. from -1 to 0). Positive and/or negative signs indicate the direction for the relationship.

Several versions of Tau exist.

- Tau-A and Tau-B are usually used for square tables (with equal columns and rows). Tau-B will adjust for tied ranks.

- Tau-C is usually used for rectangular tables. For square tables, Tau-B and Tau-C are essentially the same (refer to Table 7).

3.11 Threats to Validity and Limitations

There are some limitations in this study that could pose a threat to the validity of the same. For instance:

a) Sample size is very small and it is not representative of any population, since the approach to sample selection was based on voluntary participation from The Steinbeis University's student body. Consequently, it is not possible to generalize conclusions based on the results from this study.

Some general guidelines to determine minimal sample size includes the following: First, knowing the population size. This is achievable by consulting government sources on students' statistics; Second, setting up a margin of error at 5% which is a general convention (i.e. 95% confidence level) that allows for smaller and more manageable sample sizes. For instance, for a population size of 26000 participants (the number of students currently pursuing and IT/IS bachelor's degree in the USA), the sample size at 5% margin of error (i.e. 95% confidence level) would be a minimum of 379 participants; whereas for the same population size and at a smaller margin of error of 1% (i.e. 99% confidence level) would be a minimum of 10127 participants.

b) The survey might become obsolete due to the fact that "cybersecurity awareness" as currently defined by different authors and/or organizations may change, to reflect new

technological innovations and discoveries that could affect the conceptualization of security awareness in cyberspace.

c) Convergent validity testing is suggested in future studies. Convergent Validity is a sub-type of construct validity. Construct validity means that a test designed to measure a particular construct is actually measuring that construct. Convergent validity takes two measures that are supposed to be measuring the same construct and shows that they are related. Conversely, discriminant validity shows that two measures that are not supposed to be related are in fact, unrelated. Both types of validity are a requirement for excellent construct validity (Campell & Fiske, 1959).

d) Attitudes of the population for one particular item might exist on a vast, multi-dimensional continuum. However, the Likert Scale is unidimensional and only gives 5 options of choice, and the space between each choice cannot possibly be equidistant. Therefore, it fails to measure the true attitudes of respondents.

e) Earlier questions might influence later answers to questions. It is not unlikely that individuals might concentrate on one response side (agree/disagree). Frequently, individuals avoid choosing the “extremes” options on the scale, because of the negative implications involved with “extremists”, even if an extreme choice would be the most accurate. In this case, a confirmatory factor analysis would be appropriate if the sample size n >200; This analysis is a multivariate statistical procedure that is used to test how well the measured variables represent the number of constructs.

f) A non-parametric statistical test is based on a model that specifies only very general conditions and none regarding the specific form of the distribution from which the sample was drawn.

Chapter Four

Discussion of Results

4.1 Responses Summary

Awareness Level					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Unaware	0	0	0	0
	Unaware	3	3.2	3.2	3.2
	Neutral	25	26.9	26.9	30.1
	Aware	50	53.8	53.8	83.9
	Very Aware / Always	15	16.1	16.1	100.0
	Total	93	100.0	100.0	

Table 8: Awareness Level Composition – Total Sample

Table 8 shows the SPSS output for all answers to the survey from the entire sample of participants (*n*=93) in this study. Further, a visual inspection of this table immediately reveals that 16.1% of participants (15 participants) self-reported being very aware of cybersecurity issues. In addition, 26.9% of participants (25 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.2% of participants (3 participants) self-reported being unaware of cybersecurity issues, as defined in the survey. (refer to Appendix B for all crosstabulations and E for frequency).

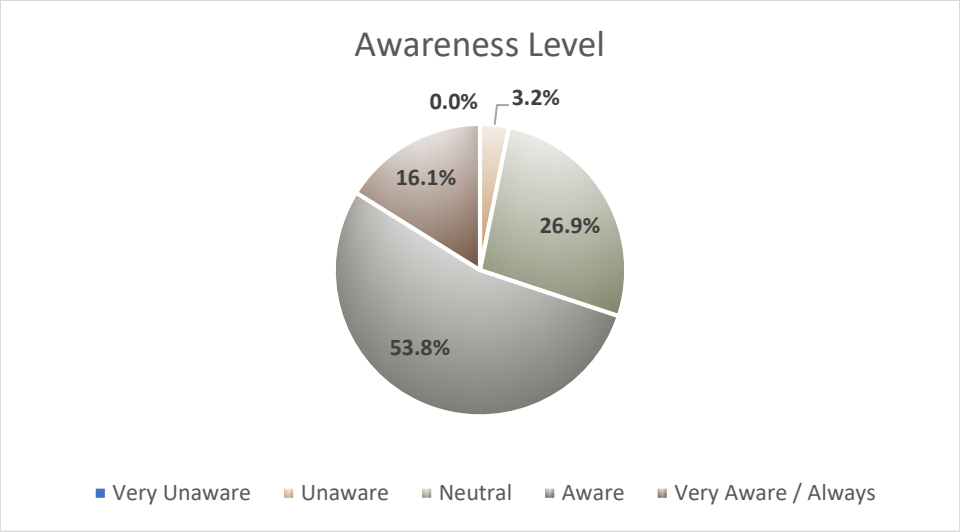


Figure 5: Awareness Level Composition – Total Sample

This section presents the SPSS output for all four crosstabulations; 1) Gender and Awareness Level, 2) Age range and Awareness Level, 3) Education Level and Awareness Level, and 4) Employment Status and Awareness Level.

The above-mentioned crosstabulations are organized as follows:

First, the total sample crosstabulation for Gender, Age range, Education Level, and Employment Status; followed by each of the geographic locations crosstabulation (i.e. Germany, United Kingdom (UK), and The United States (USA)).

Gender and Awareness Level Crosstabulation (Total Sample)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Gender:	Male	0	2	14	32	13	61
	Female	0	1	11	18	2	32
Total		0	3	25	50	15	93

Table 9: Gender and Awareness Level – Total Sample

Table 9 shows a crosstabulation between Gender and Awareness Level for the total sample size *n*=93. A visual inspection of this table immediately reveals that 65.59% of participants are males (61 participants), From this sample, only 16.12% of participants (15 participants) self-reported being very aware. In addition, 26.88% of participants (25 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.22% of participants (3 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

Gender and Awareness Level Crosstabulation (GERMANY)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Gender:	Male	0	2	2	8	4	16
	Female	0	0	5	9	1	15
Total		0	2	7	17	5	31

Table 10: Gender and Awareness Level by Location – Germany

Table 10 shows a crosstabulation between Gender and Awareness Level by location. The group size of participants from Germany is *n*=31. A visual inspection of this table immediately reveals similar participation from both genders (16 males vs 15 females), From this group, only 16.12% of participants (5 participants) self-reported being very aware, for this location. In addition, 22.58% of participants (7 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 6.45% of participants (2 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

Gender and Awareness Level Crosstabulation (UK)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Gender:	Male	0	0	4	15	6	25
	Female	0	0	2	3	1	6
Total		0	0	6	18	7	31

Table 11: Gender and Awareness Level by Location – UK

Table 11 shows a crosstabulation between Gender and Awareness Level by location. The group size of participants from United Kingdom (UK) is *n*=31. A visual inspection of this table immediately reveals that 80.64% of participants are males (25 participants). From this group, only 22.58% of participants (7 participants) self-reported being very aware, for this location. In addition, 19.35% of participants (6 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, none of the participants (0 participants) in this group self-reported being unaware of cybersecurity issues, as defined in the survey.

Gender and Awareness Level Crosstabulation (USA)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Gender:	Male	0	0	8	9	3	20
	Female	0	1	4	6	0	11
Total		0	1	12	15	3	31

Table 12: Gender and Awareness Level by Location – USA

Table 12 shows a crosstabulation between Gender and Awareness Level by location. The group size of participants from The United States (USA) is *n*=31. A visual inspection of this table immediately reveals that 64.51% of participants are males (20 participants).

From this group, only 9.67% of participants (3 participants) self-reported being very aware, for this location. In addition, 38.70% of participants (12 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.22% of participants (1 participant) self-reported being unaware of cybersecurity issues, as defined in the survey.

Age range and Awareness Level Crosstabulation (Total Sample)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Age range:	20 to 25	0	2	20	41	12	75
	26 to 30	0	1	3	5	2	11
	31 to 35	0	0	1	1	0	2
	36 to 40	0	0	1	3	1	5
Total		0	3	25	50	15	93

Table 13: Age range and Awareness Level – Total Sample

Table 13 shows a crosstabulation between Age range and Awareness Level for the total sample size *n*=93. A visual inspection of this table immediately reveals that 80.64% of participants are between the age range of 20 to 25 years (75 participants), which is the youngest group in this study. From this sample, only 16.12% of participants (15 participants) self-reported being very aware. In addition, 26.88% of participants (25 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.22% which included the two youngest age range groups (3 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

Age range and Awareness Level Crosstabulation (GERMANY)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Age range:	20 to 25	0	1	6	11	5	23
	26 to 30	0	1	1	3	0	5
	31 to 35	0	0	0	1	0	1
	36 to 40	0	0	0	2	0	2
Total		0	2	7	17	5	31

Table 14: Age range and Awareness Level by Location – Germany

Table 14 shows a crosstabulation between Age range and Awareness Level by location. The group size of participants from Germany is *n*=31. A visual inspection of this table immediately reveals that 74.19% of participants (23 participants) are between the age range of 20 to 25 years. From this group, only 16.12% of participants (5 participants) self-reported being very aware, for this location. In addition, 22.58% of participants (7 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 6.45% of participants, which included the two youngest age range groups (2 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

Age range and Awareness Level Crosstabulation (UK)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Age range:	20 to 25	0	0	2	15	4	21
	26 to 30	0	0	2	2	2	6
	31 to 35	0	0	1	0	0	1
	36 to 40	0	0	1	1	1	3
Total		0	0	6	18	7	31

Table 15: Age range and Awareness Level by Location – UK

Table 15 shows a crosstabulation between Age range and Awareness Level by location. The group size of participants from United Kingdom (UK) is *n*=31. A visual inspection of this table immediately reveals that 67.74% of participants (21 participants) are between the age range of 20 to 25 years. From this group, only 22.58% of participants (7 participants) self-reported being very aware, for this location. In addition, 19.35% of participants (6 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, none of the participants in this group self-reported being unaware of cybersecurity issues, as defined in the survey.

Age range and Awareness Level Crosstabulation (USA)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Age range:	20 to 25	0	1	12	15	3	31
	26 to 30	0	0	0	0	0	0
	31 to 35	0	0	0	0	0	0
	36 to 40	0	0	0	0	0	0
Total		0	1	12	15	3	31

Table 16: Age range and Awareness Level by Location – USA

Table 16 shows a crosstabulation between Age range and Awareness Level by location. The group size of participants from The United States (USA) is *n*=31. A visual inspection of this table immediately reveals that 100% of participants (31 participants) are between the age range of 20 to 25 years. From this group, only 9.67% of participants (3 participants) self-reported being very aware, for this location. In addition, 38.70% of participants (12 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.22% of participants (1 participant) self-reported being unaware of cybersecurity issues, as defined in the survey.

Education Level and Awareness Level Crosstabulation (Total Sample)

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Education level:	High School	0	0	2	10	2	14
	Technical and Professional degree (any degree)	0	0	1	7	4	12
	Some University Studies (not completed in full)	0	2	20	28	6	56
	University degree (any degree)	0	1	2	5	3	11
Total		0	3	25	50	15	93

Table 17: Education Level and Awareness Level – Total Sample

Table 17 shows a crosstabulation between Education Level and Awareness Level for the total sample size *n*=93. A visual inspection of this table immediately reveals that 72.04% of participants (67 participants) self-reported higher education studies (completed or in progress). From this sample, only 16.12% of participants (15 participants) self-reported being very aware. In addition, 26.88% of participants (25 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.22% of participants (3 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

Education Level and Awareness Level Crosstabulation (GERMANY)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Education level:	High School	0	0	0	0	0	0
	Technical and Professional degree (any degree)	0	0	0	4	0	4
	Some University Studies (not completed in full)	0	1	7	11	3	22
	University degree (any degree)	0	1	0	2	2	5
Total		0	2	7	17	5	31

Table 18: Education Level and Awareness Level by Location – Germany

Table 18 shows a crosstabulation between Education Level and Awareness Level by location. The group size of participants from Germany is *n*=31. A visual inspection of this table immediately reveals that 87.09% of participants (27 participants) self-reported higher education studies (completed or in progress). From this group, only 16.12% of participants (5 participants) self-reported being very aware, for this location. In addition, 22.58% of participants (7 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 6.45% of participants (2 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

Education Level and Awareness Level Crosstabulation (UK)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Education level:	High School	0	0	0	4	1	5
	Technical and Professional degree (any degree)	0	0	1	3	4	8
	Some University Studies (not completed in full)	0	0	4	9	2	15
	University degree (any degree)	0	0	1	2	0	3
Total		0	0	`6	18	7	31

Table 19: Education Level and Awareness Level by Location – UK

Table 19 shows a crosstabulation between Education Level and Awareness Level by location. The group size of participants from United Kingdom (UK) is *n*=31. A visual inspection of this table immediately reveals that 58.06% of participants (18 participants) self-reported higher education studies (completed or in progress). From this group, only 22.58% of participants (7 participants) self-reported being very aware, for this location. In addition, 19.35% of participants (6 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, none of the participants self-reported being unaware of cybersecurity issues, as defined in the survey.

Education Level and Awareness Level Crosstabulation (USA)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Education level:	High School	0	0	2	6	1	9
	Technical and Professional degree (any degree)	0	0	0	0	0	0
	Some University Studies (not completed in full)	0	1	9	8	1	19
	University degree (any degree)	0	0	1	1	1	3
Total		0	1	12	15	3	31

Table 20: Education Level and Awareness Level by Location – USA

Table 20 shows a crosstabulation between Education Level and Awareness Level by location. The group size of participants from The United States (USA) is *n*=31. A visual inspection of this table immediately reveals that 70.96% of participants (22 participants) self-reported higher education studies (completed or in progress). From this group, only 9.67% of participants (3 participants) self-reported being very aware, for this location. In addition, 38.70% of participants (12 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.22% of participants (1 participant) self-reported being unaware of cybersecurity issues, as defined in the survey.

Employment Status and Awareness Level Crosstabulation (Total Sample)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Employment:	Unemployed	0	0	5	6	1	12
	Part-time	0	2	11	14	7	34
	Full time	0	1	9	30	7	47
Total		0	3	25	50	15	93

Table 21: Employment Status and Awareness Level – Total Sample

Table 21 shows a crosstabulation between Employment Status and Awareness Level for the total sample size *n*=93. A visual inspection of this table immediately reveals that 50.53% of participants (47 participants) self-reported being employed full time. From this sample, only 16.12% of participants (15 participants) self-reported being very aware. In addition, 26.88% of participants (25 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.22% of participants (3 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

Employment Status and Awareness Level Crosstabulation (GERMANY)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Employment:	Unemployed	0	0	1	0	0	1
	Part-time	0	1	5	6	5	17
	Full time	0	1	1	11	0	13
Total		0	2	7	17	5	31

Table 22: Employment Status and Awareness Level by Location – Germany

Table 22 shows a crosstabulation between Employment Status and Awareness Level by location. The group size of participants from Germany is *n*=31. A visual inspection of this

table immediately reveals that 41.93% of participants (13 participants) self-reported being employed full time. From this group, only 16.12% of participants (5 participants) self-reported being very aware, for this location. In addition, 22.58% of participants (7 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 6.45% of participants (2 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

Employment Status and Awareness Level Crosstabulation (UK)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Employment:	Unemployed	0	0	1	0	0	1
	Part-time	0	0	0	1	1	2
	Full time	0	0	5	17	6	28
Total		0	0	6	18	7	31

Table 23: Employment Status and Awareness Level by Location – UK

Table 23 shows a crosstabulation between Employment Status and Awareness Level by location. The group size of participants from United Kingdom (UK) is *n*=31. A visual inspection of this table immediately reveals that 90.32% of participants (28 participants) self-reported being employed full time. From this group, only 22.58% of participants (7 participants) self-reported being very aware, for this location. In addition, 19.35% of participants (6 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, none of the participants self-reported being unaware of cybersecurity issues, as defined in the survey.

Employment Status and Awareness Level Crosstabulation (USA)

Count

		Awareness Level					
		Very Unaware	Unaware	Neutral	Aware	Very Aware / Always	Total
Employment:	Unemployed	0	0	3	6	1	10
	Part-time	0	1	6	7	1	15
	Full time	0	0	3	2	1	6
Total		0	1	12	15	3	31

Table 24: Employment Status and Awareness Level by Location – USA

Table 24 shows a crosstabulation between Employment Status and Awareness Level by location. The group size of participants from The United States (USA) is *n*=31. A visual inspection of this table immediately reveals that 19.35% of participants (6 participants) self-reported being employed full time. From this group, only 9.67% of participants (3 participants) self-reported being very aware, for this location. In addition, 38.70% of participants (12 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.22% of participants (1 participant) self-reported being unaware of cybersecurity issues, as defined in the survey.

4.2 Answer to Research Questions

1. What is the difference between the cybersecurity awareness levels of individuals and their gender, if any?

Gender and Awareness Level (*n*=93)					
H_0(a)	There is no difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.				
H_1(a)	There is a difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.				
Test:	Mann-Whitney U	**Value (U):**	785.0	**p-value:**	0.088
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(a). Therefore, there is no evidence against the null hypothesis.				

Table 25: Gender and Awareness Level Difference

2. What is the relationship between the cybersecurity awareness levels of individuals and their age, if any?

Age range and Awareness Level (*n*=93)					
H_0(b)	There is no relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.				
H_1(b)	There is a relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	-0.0201	**p-value:**	0.833
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(b). Therefore, there is no evidence against the null hypothesis.				

Table 26: Age range and Awareness Level Relationship

3. What is the relationship between the cybersecurity awareness levels of individuals and their education level completed, if any?

Education Level and Awareness (*n*=93)					
H_0(c)	There is no relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
H_1(c)	There is a relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	-0.109	**p-value:**	0.133
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(c). Therefore, there is no evidence against the null hypothesis.				

Table 27: Education Level and Awareness Level Relationship

4. What is the relationship between the cybersecurity awareness levels of individuals and their current employment status, if any?

Employment Status and Awareness Level (*n*=93)					
H_0(d)	There is no relationship between the cybersecurity awareness level of individuals and their current employment status, in an academic setting in higher education.				
H_1(d)	There is a relationship between the cybersecurity awareness level of individuals and their current employment status. in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	0.111	**p-value:**	0.170
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(d). Therefore, there is no evidence against the null hypothesis.				

Table 28: Employment Status and Awareness Level Relationship

5. What are some of the implications of the differences and/or relationships found through this study, in terms of the cybersecurity awareness levels of individuals, if any?

Education Level and Awareness Level (Location UK; *n*=31)					
H_0(c)	There is no relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
H_1(c)	There is a relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	-0.272	**p-value:**	**0.017**
Interpretation:	When p-value ≤ 0.05 the null hypothesis H_0(c) is rejected. Therefore, there is evidence against the null hypothesis.				

Table 29: Education Level and Awareness Level Relationship – UK

Table 29 shows the SPSS output for the group of participants located in UK (refer to Appendix C for all locations tables). This is the only group for which the null hypothesis was rejected. Therefore, there is evidence against the null hypothesis. The results from the Tau-c test showed a negative correlation between Education Level and Awareness Level which was statistically significant for the UK group. Appendix B and Appendix C provide more information about the SPSS output for the three specific locations of participants, Germany, United Kingdom (UK), and The United States (USA).

In sum, cybersecurity awareness is consistently intertwined with the notion of information security awareness. Increased security awareness can contribute to minimize user related mistakes, and to maximize the efficiency of security techniques (Straub & Welke, 1998). Further, getting users to become aware and to participate in safe online behavior

is a significant challenge (Gandy, 2003). It requires new methods and instruments of assessment associated to specific goals to improve results from assessments.

Awareness is frequently associated to operational situations, where specific reasons require individuals to have an identifiable awareness level for a specific context. Therefore, individuals and business organizations benefit from higher levels of security awareness, which ultimately reflects higher literacy levels and learning. Lastly, business continuity depends on how individuals respond to various situations, exercise caution in their decisions, and ultimately, how aware they are about current and future security risks in their doings.

4.3 A Comparison Note to Other Studies

One common denominator in the comparison among cybersecurity studies is the orientation towards specific missions or intentions, rather than building consensus among approaches towards a unified view for the study of cybersecurity awareness. For instance: several studies chose organizations to conduct their assessments. Maseti & Pottas (2006) focused on healthcare, since information contained in patients' records is quite sensitive, and it requires to be accessed by multiple parties (i.e. doctors, nurses, administrators, etc.). Further, Schlienger & Teufel (2003) conducted their study in the banking sector, and focused their analysis on the impact of cultural differences on cybersecurity awareness. In this approach, it is evident that the information security triad (Confidentiality, Integrity, Availability) is the specific mission of awareness, since the information contained in banking records is extremely important for the organization.

Moreover, Whitman & Mattord (2004) studied ways to make users mindful of Information Technology (IT) security. The focus of this study was on government offices, and the mission (purpose) included the confirmation that security awareness programs ensure that employees understand the importance of security and the adverse consequences of its failure.

In the education sector, many studies focus on the risk of daily operations conducted in schools, such as: retrieving information from websites; accessing videos; chatting; being social, etc. In the United States, the National Cyber Security Alliance (2017) conducted a study on school awareness towards common cyber incident, and found out that schools are ill prepared to teach students the basics of online safety, online security, and online ethics (Geer, 2015). Kritzinger, Bada, & Nurse (2017) studied the cybersecurity awareness initiatives for school learners in South Africa and the UK, which are supported by government, industry and academia. Furthermore, this study provided an overview of similarities and differences between initiatives across countries, and explored some of the reasons why they may exist. This research focused on presenting recommendations for both countries to improve school cybersecurity initiatives.

Lester & Dalat-Ward (2019) focused on curriculum development, while Bicak, Liu, & Murphy (2015) noted that cybersecurity is so broad that education needs to be more specialized. Moreover, regardless of the settings for the study, current literature reveals that specific missions (purpose) drive the study of cybersecurity awareness, since deficits in security awareness are perceived in different forms by different stakeholders.

Finally, higher education institutions embrace a common mission to understating cybersecurity awareness through curriculum development initiatives, as it is the case of

The Steinbeis University's preliminary report "Internal Planning Presentation" (Lamprecht, 2018). The focus of this report was on presenting results regarding data distribution (frequencies) and cross tabulations, in an effort to develop key goals for program, curriculum and training development. No other studies were sought with the data sets provided for this study, besides this master's thesis.

4.4 Related Cases

Cybersecurity awareness has been studied under different contexts and settings. As mentioned earlier in this study, mission (i.e. specific purpose) determine the direction of the research. Syed, Padia, Finin, Mathews, & Joshi (2016) examined the effect of user computer self-efficacy (CSE), cybersecurity countermeasures awareness (CCA), and cybersecurity skills (CS) on users' computer misuse intention (CMI) at a government agency. This study concluded that CSE, CCA and CS contribute to CMI. In addition, it was noted that cybersecurity policy is a significant contributor to cybersecurity action skills, and that personal factors, such as age and gender affect intentions.

Although demographic variables were not the focus of this study. It was noted the importance of personal characteristics (demographic factors) in the findings of this study. Rahim, Hamid, Mat Kiah, Shamshirband, & Furnell (2015) presented a systematic review of approaches to assessing cybersecurity awareness. This study was conducted to identify any gaps in the cybersecurity awareness assessment research, in an effort to unify the direction of future work. However, the study concluded that no previous research was conducted in the assessment of the cybersecurity awareness using a program

evaluation technique. Further, in this case, a program evaluation is a systematic method for collecting, analyzing, and using information to answer questions about status quo, projects, policies and programs, particularly about their effectiveness and efficiency. Lastly, it was also found that few studies focused on youngsters and on the issue of safeguarding personal information.

Torten, Reaiche, & Boyle (2018) studied the relationship between threat awareness and countermeasure awareness on IT professionals' compliance with desktop security behaviors. A model (originally developed by Hanus & Wu (2016)) was tested on a population of 400 IT professionals across a broad range of IT roles and company sizes in the United States. The overall findings show that 61.2% of the variability in desktop security behavior can be explained by threat awareness and countermeasure awareness. Furthermore, the research concluded that there is a relationship between threat awareness and countermeasure awareness with the five elements of protective motivation theory (PMT): perceived severity; perceived vulnerability; self-efficacy; response efficacy; and response cost.

Tekerek & Tekerek (2013) conducted a study in school settings. In this study, the researchers developed a scale to measure Information and Computer Security Awareness. The survey was applied to 2449 students in the schools in the center of Kahramanmaraş City, in addition to towns, and other villages of this province. Furthermore, the study found that students have sufficient awareness level in terms of ethical issues. However, they have low awareness levels in terms of issues that require knowledge about rules. Lastly, the study provided some observations and

recommendation as to what curriculum changes are necessary to improve the current outcome.

Parsons, et al., (2017) conducted a study to further establish the validity of the Human Aspects of Information Security Questionnaire (HAIS-Q), as an effective instrument for measuring information security awareness (ISA). In this study, 2 groups were used to establish the construct validity of the questionnaire. The first group consisted of 112 university students, and the second group consisted of 505 working adults. Both groups located in Australia. The results of a factor analysis and other statistical techniques provided evidence for the validity of the HAIS-Q as a robust measure of ISA. Lastly, the study also provided some practical recommendation for information security practitioners.

Chapter Five

Conclusion and Future Research

5.1 Conclusion

In recent years the concept of cybersecurity awareness has claimed the interest of researchers and academia in general. One of the main challenges in the study of cybersecurity is to better define the context in which this concept could be adopted and studied, regardless of changes in technology. Literature in this field has revealed that cybersecurity awareness and information security awareness are two concepts used interchangeably in several studies, in an effort to embody all related terms as a unifying definition for security awareness over human and machine interactions in cyberspace.

Several authors prefer to adopt the term “information security awareness” in their operational definitions, since information is what is being managed and dealt with in cyberspace. However, it is a common practice to adopt the term “cybersecurity awareness” as inclusive of any terms related and/or associated with common terms, such as: information security; assets and network security; security protocols; and cyberspace interactions.

Nowadays, several organizations and institutions are taking charge of defining cybersecurity in terms of specific goals and/or benefits sought according to specific

missions. However, there are a few key words that permeate across definitions, such as: data security; damages; information protocols; security awareness; standards; etc. Furthermore, a review of current literature has also revealed different approaches towards the study of cybersecurity awareness. Current attempts range from behavioral sciences to information and risk management approaches.

Siponen (2000) rightfully stated that “to increase understanding of problems relating to awareness, two categories can be outlined, framework and content. Framework can be approached in a structural manner and by quantitative research, while content constitutes a more informal interdisciplinary field of study, and it should be approached using qualitative research methods” (p. 31).

Although there is no general consensus on how to assess self-reported awareness levels. It is noted that by continuously studying this subject through different approaches and contexts, one can learn more about it. In addition, only increased security awareness level can contribute to minimize user related mistakes, and to maximize the efficiency of future security techniques and protocols (Straub & Welke, 1998).

5.2 Impact of the Study

Awareness is frequently associated to operational situations, where specific reasons require individuals to have an identifiable awareness level for a specific context. Therefore, it is in the best interest of individuals and business organizations to seek out higher levels of cybersecurity awareness, since business continuity depends on how individuals respond to various situations, and ultimately, it depends on how well-informed

individuals (users) are about current and future security risks in their doings. Arora et al. (2006) noted that individuals consider the internet to be a safe environment. However, their behavior does not reflect a high level of security awareness when confronted with new cyber threats. Consequently, it is hard for organizations to plan for costs associated with cybersecurity incidents, since tangible behaviors that depict awareness are not seen frequently (Kirlappos & Sasse, 2012).

The findings of this study can be considered beneficial in terms of adding up to the general body of knowledge in the field of cybersecurity awareness. Further, several limitations prevent this study from generalizing results to make inferences about the population. However, there are numerous reasons why this research effort impacts the study of cybersecurity awareness, such as: a) It introduces effectively the data from a new survey to compare differences and relationships between groups; b) It studies the outcome of basic demographic factors on cybersecurity awareness level; c) Data sets include the outcomes from individuals located in three different geographic regions (Germany, UK, and USA). Although there is no conclusive evidence that all demographic factors have an impact on cybersecurity awareness level of individuals, it is noteworthy to mention that '*Education Level*' in one location seem to have an impact on the cybersecurity awareness level of the UK group. Therefore, it would be necessary to further study a more comprehensive groups of demographic factors to determine how relevant they are in the development of security awareness.

Finally, this research project provided me with a solid formative experience in the study of cybersecurity awareness, and it delivered several insights as to why it is necessary to create and to administer new surveys, and to continue observing awareness levels of

individuals (users), so we may debunk myths that could be adopted across society as general facts.

5.3 Future Research

This initial examination opens many lines of inquiry for future research in the field of cybersecurity awareness. For instance, future studies should consider a larger sample size, preferably from a population where proportionate-stratified sampling can be applied to, in an effort to become inclusive of multiple demographics. Further, psychologists and behavioral scientists consider gender as a basic variable that can affect behavioral outcomes. Although there is no conclusive evidence that gender plays a role in mediating factors that affect cybersecurity awareness and behaviors, Anward et al., (2017) noted that gender has some effect in security self-efficacy. Therefore, it is critical to consider in future studies the effect of gender in cybersecurity awareness. In addition, other demographic variables may include other groups of interest such as professionals in manufacturing and/or service sectors, acting in different capacities, such as entry level, middle level managerial, and top-level executives from different enterprise sizes (Small, Medium, and Large Organizations).

Since the definition of cybersecurity awareness continues to change over time due to new discoveries and innovations in ICT's, it is critical to employ new methodologies that reflect the current ecosystem of cybersecurity awareness. For instance, the development of Intrusion Detection Systems (IDSs) and Persistent Threat Detection Systems (PTDSs) have enormously contributed to defend computer systems from attacks. However, Feng,

Zhang, Hu, & Huang (2014) noted that these systems cannot adequately deal with new types of attack or changing computing environments, but such systems may help individuals “to learn the behaviors of networks automatically by analyzing the data trails of their activities” (p. 128).

Finally, current and future assessment tools applied to different areas of cybersecurity awareness may provide a good overview of the general awareness levels of individuals (users). However, since no single tool can guarantee comprehensive results that could be generalized to the population, it is important to consider the simultaneous application of several assessment tools in future studies, to conform with parallel forms of reliability for surveys. Moreover, the awareness level of individuals changes over time. Therefore, it is critical to consider these changes in longitudinal studies, in an effort to better understand how individuals improve their awareness level towards cybersecurity, and how the pace of technology discoveries and innovations affect basic awareness level and their development towards higher levels of mindfulness for cybersecurity risks and threats.

Bibliography

Abawajy, J. & Kim, T. (2010). 'Performance Analysis of Cyber Security Awareness Delivery Methods.' *Security Technology, Disaster Recovery and Business Continuity. Communications in Computer and Information Science*, Springer, Berlin, Heidelberg; 122.

Abraham, S. (2011). 'Information Security Behavior: Factors and Research Directions.' *Proceedings of the American Conference on Information Systems*; Detroit, USA Paper 462.

Abidi, B. R., Aragam, N. R., Yi, Y., & Abidi, M. A. (2008). 'Survey and Analysis of Multimodal Sensor Planning and Integration for Wide Area Surveillance.' *ACM Computer Survey 2008*; 41(1): 1e36.

Ahluwalia, R. (2000). 'An Examination of Psychological Processes Underlying Resistance to Persuasion.' *Journal of Consumer Research*; 27(2): 217-232.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). 'Gender Difference and Employees' Cybersecurity Behaviors.' *Computers in Human Behavior*; 69: 437-443.

Arce, I. (2003). 'The Weakest Link Revisited.' *Information. Security. IEEE Security Privacy 2003*; 1:72–76.

Arora, A., Nandkumar, A., & Telang, R. (2006). 'Does Information Security Attack Frequency Increase with Vulnerability Disclosure? An Empirical Analysis.' *Information Systems Frontiers*; 8 (5): 350-362.

Bada, M., & Sasse, A. (2014, July). '*Cyber Security Awareness Campaigns. Why Do They Fail to Change Behaviour?' Working paper. Global Cyber Security Capacity Centre*.

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010) 'Women in Cybersecurity: A Study of Career Advancement.' *IT Professional*; 12(1): 24-31.

Belaissaoui, H. & Elkhannoubi, M. (2015) 'A Framework for an Effective Cybersecurity Strategy Implementation: Fundamental Pillars Identification.' In 15th International Conference on Intelligent Systems Design and Applications (ISDA); Marrakech: 1–6.

Bicak, A., Liu, X. M., & Murphy, D. (2015). 'Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program.' *Information Systems Education Journal*; 13(3): 99.

Buczak, A. L., & Guven, E. (2016, 2nd Quarter) 'A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection.' *IEEE Communications Surveys & Tutorials*; 18(2): 1153-1157.

Campell, D. T., & Fiske, D. W. (1959). 'Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix.' *Psychological Bulletin*; 56: 81-105.

Canbek, G., & Sağıroğlu, Ş. (2008). 'Kişisel Gizlilik ve Yasal Düzenlemelere Kötücül Yazılımlar Açısından Bakış.' *Kara Harb Okulu Savunma Bilimleri Dergisi*; 7(2): 119-139.

Caputo, D., Lawrence P. Sh., Freeman, D. J., & Johnson, E. M. (2014). 'Going Spear Phishing: Exploring Embedded Training and Awareness.' *IEEE Security & Privacy*; 12(1): 28-38.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). 'Defining Cybersecurity.' *Technology Innovation Management Review*; 4(10).

Cavelty, M. D. (2008). 'Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate.' *Journal of Information Technology & Politics*; 4(1): 19-36.

Cavelty, M. D. (2010). *Cyber-Security. In J. P. Burgess (Ed.), The Routledge Handbook of New Security Studies*: 154-162. London: Routledge.

Ceraolo, J. P. (1996). 'Penetration Testing Through Social Engineering.' *Information Systems. Security*; 4(4): Winter.

Chang, F. R. (2012). 'Guest Editor's Column.' *The Next Wave*. 19(4): 1–2.

Cialdini, R. (2009). *Influence: Science and Practice*. (5th ed.). Boston: Pearson. USA.

Clavister, (2009). *Security in the Cloud,* Clavister White Paper. Available from: https://www.allaboutsecurity.de/fileadmin/micropages/Whitepaper_Security_Management/clavister-whp-security_in_the_cloud.pdf [Accessed on October 20, 2018].

CNSS: The Committee on National Security Systems (2004). CNSS Instruction No. 4009. Revised May 2003.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). 'Defining Cybersecurity.' *Technology Innovation Management Review*; 4(10).

D'Arcy, J., & Hovav, A. (2009). 'Does one size fit all? Examining the Differential Effects of IS Security Countermeasures.' *Journal of Business Ethics*; 89(1): 59-71.

De Bruijn, H., & Janssen, M. (2017). 'Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies.' *Government Information Quarterly* [Online]. 34(1): 1-7. doi.org/10.1016/j.giq.2017.02.007 [Accessed on October 15. 2018].

Dhillon, G. (1999). 'Managing and Controlling Computer Misuse.' *Information Management & Computer Security;* 7(4): 171-5.

DHS. (2014). *A Glossary of Common Cybersecurity Terminology*. National Initiative for Cybersecurity Careers and Studies. Department of Homeland Security. October 1, 2014.

Diakun-Thibault, N. (2014). 'Defining Cybersecurity.' *Technology Innovation Management Review*; 12-18.

Dinev, T., & Hu, Q. (2007). 'The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies.' *Journal of the Association for Information Systems*; 8(7): 386e408.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). 'Phishing for User Security Awareness.' Computers & Security; 26(1): 73-80.

Dolan P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). *MINDSPACE Influencing Behaviour through Public Policy.* Institute for Government, Cabinet Office. http://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf

Doty, P. (2015). 'U.S. Homeland Security and Risk Assessment.' *Government Information Quarterly*; 32(3): 342–352.

Dube, T. E., Raines, R. A., Grimaila, M. R., Bauer, K. W., & Rogers, S. K. (2013). 'Malware Target Recognition of Unknown Threats.' *IEEE Systems Journal*; 7(3): 467e77.

Dunkels, E. (2008). 'Children's Strategies on the Internet.' *Critical Studies in Education*; 49(2), 171-184.

Duval, S., & Wicklund, R. A. (1972). *A Theory of Objective Self Awareness*. Academic Press.

Elmaghraby, A. S., & Losavio, M. M. (2014). 'Cyber Security Challenges in Smart Cities: Safety, Security and Privacy.' *Journal of Advanced Research*; 5(4): 491–497.

Feng, W., Zhang, Q., Hu, G., & Huang, J. X. (2014). 'Mining network data for intrusion detection through combining SVMs with ant colony networks'. *Future Generation Computer Systems*; 37: 127-140.

Fenigstein, A., Scheier, M. F., & Buss, A. H. (1975). 'Public and Private Self-consciousness: Assessment and Theory.' *Journal of Consulting and Clinical Psychology*; 43(4): 522.

Finch, J., Furnell, S., & Dowland, P. (2003). 'Assessing IT Security Culture: System Administrator and End-User Perspectives.' *In Proceedings of ISOneWorld Conference and Convention*. Las Vegas, Nevada, USA.

Friedman, A. A., & West, D. M. (2010). 'Privacy and Security in Cloud Computing.' *Issues in Technology Innovation*; 3: 1-13.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). 'The Challenges of Understanding and Using Security: A Survey of End-Users.' *Computers & Security*; 25(1): 27-35.

Furnell, S., Bryant, P., & Phippen, D. (2007). 'Assessing the Security Perceptions of Personal Internet Users.' *Computers & Security*; 26: 410-417.

Furnell, S., Valleria, T., & Phippen, D. (2008). 'Security Beliefs and Barriers for Novice Internet Users.' *Computers & Security*; 27: 235-240.

Gandy, O. H. (2003). *The Real Digital Divide: Citizens Versus Consumers*. The Handbook of New Media 2003.

Geer, D. (2015). 'Six Key Areas of Investment for the Science of Cyber Security.' Futurist; 49(1): 10-15.

Goleman, D. (1995). Emotional Intelligence: Why It Can Matter More Than IQ, Bantam Books. UK ISBN 978-0-553-38371-3

Goodhue, D. L., & Straub, D. W. (1989). 'Security Concerns of System Users: a Proposed Study of User Perceptions of the Adequacy of Security Measures.' *In Proceedings of the 21st Hawaii International Conference on System Science (HICSS).* Hawaii, USA.

Gorham-Oscilowski, U., & Jaeger, P. T. (2008). 'National Security Letters, the USA PATRIOT Act, and the Constitution: The Tensions Between National Security and Civil Rights.' *Government Information Quarterly*; 25(4): 625–644.

Govern, J. M., & Marsch, L. A. (2001). 'Development and Validation of the Situational Self-awareness Scale.' *Consciousness and Cognition*; 10(3): 366-378.

Halima, I. K., Shareeful, I., & Mohammad, A. R. (2018). **'**An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System.' *Applied Sciences MDPI* [Online]; 8: 898. doi:10.3390/app8060898. [Accessed on 15 April 2018].

Hansche, S. (2001, January/February). 'Designing a Security Awareness Program: Part 1.' *Information Systems Security;* (1):14–22.

Hanus, B., & Wu, Y. A. (2016). 'Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective.' *Information Systems Management;* 33(1): 2-16.

Hassan, Q. (2011, Jan/Feb). 'Demystifying Cloud Computing.*' The Journal of Defense Software Engineering;* (1): 16–21.

Hernández-Ramos, J. L., Jara, A. J., Marın, L., & Skarmeta, A. F. (2013). 'Distributed Capability-Based Access Control for the Internet of Things.' *Journal of Internet Services and Information Security*; 3(3/4): 1–16.

Hogan, K. (2005). *The Science of Influence: How to Get Anyone to Say "Yes" in 8 Minutes or Less*. Hoboken, NJ. John Wiley & Sons. USA.

Hogan, J., Motivation, J., & Bolhuis, J. (2005). *The Behaviour of Animals: Mechanisms, Function and Evolution*. Blackwell Publishing. 41-70. Malden, MA. USA.

Hoffer, J. A., & Straub, D. W. (1989). 'The 9 to 5 Underground: Are you Policing Computer Crimes?' *Sloan Management Review*; 30(4).

Humaidi, N., & Balakrishnan, V. (2013). 'Exploratory Factor Analysis of User's Compliance Behaviour Towards Health Information System's Security.' *Journal of Health Medicine Information*; 4(2).

ISF (2003). *The Standard of Good Practice for Information Security*. Version 4.0. Information Security Forum.

ISF (2014). *From Promoting Awareness to Embedding Behaviours, Secure by Choice not by Chance,* Information Security Forum. February 2014: 71-170.

ISO 27000. ISO/IEC 27000 Family - Information Security Management Systems.

IT (2008). *IT Governance Institute. Information Security Governance*: Guidance for Information Security Managers. ITGI Publishing.

Kahneman, D. (2013). Thinking, Fast and Slow. Farrar, Straus and Giroux; 1st edition. ISBN-10: 0374533555.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). 'Effectiveness of information Security Awareness Methods Based on Psychological Theories.' *African Journal of Business Management*; *5*(26): 10862-10868.

Killingsworth, M. A., & Gilbert, D. T. (2010). 'A Wandering Mind is an Unhappy Mind.' *Science*: 330(6006): 932-932.

Kirlappos, I., & Sasse, M. A. (2012). 'Security Education Against Phishing: A Modest Proposal for a Major Rethink.*' IEEE Security and Privacy Magazine*; 10(2): 24-32.

Kirlappos, I., Parkin, S., Sasse, M. A. (2014). 'Learning from "Shadow Security": Why Understanding Noncompliance Provides the Basis for Effective Security.' *Workshop on Usable Security Kreuter.*

Kozlenkova, I. V., Samaha, S. A., & Palmatier, R. W. (2013). 'Resource-Based Theory in Marketing.' *Journal of Academic Marketing Science*; 42(1): 1-21.

Kritzinger, E., Bada, M., & Nurse, J.R. (2017). 'A Study into the Cybersecurity Awareness Initiatives for School Learners in South Africa and the UK.' World Conference on Information Security Education.

Kruger, H. & Kearney, W. (2006). 'A Prototype for Assessing Information Security Awareness.' *Computers & Security*; 25(4): 289–296.

Kumar, N., Mohan, K., & Holowczak, R. (2008). 'Locking the Door but Leaving the Computer Vulnerable: Factors Inhibiting Home Users' Adoption of Software Firewalls.' *Decision Support System*; 46: 254-264.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007) "*Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System.*' Institute for Software Research; Paper 21. Available from: http://repository.cmu.edu/isr/21 [Accessed on November 10, 2018].

Lamprecht, A. (2018). 'Internal Planning Presentation' [power point]. *2018 Planning Meeting* at The Steinbeis University Berlin. Germany. December 2018.

Lester, L. J. Y., & Dalat-Ward, Y. (2019). 'Teaching Professionalism and Ethics in Information Technology by Deliberative Dialogue.' *Information Systems Education Journal*; 17(1): 4.

Lewis, J. A. (2006). *Cybersecurity and Critical Infrastructure Protection*. Washington, DC: Center for Strategic and International Studies. http://cip.management.dal.ca/publications/Cybersecurity%20and%20Critical%20Infrastructure%20Protection.pdf. [Accessed on December 15, 2018].

Maseti, O., & Pottas, D. (2006). 'A Role-Based Security Awareness Model for South African Hospitals.' In Proceedings of the 6th Annual Information Security South Africa Conference. Sandton, South Africa, 5-7 July.

Mishra, S. & Dhillon, G. (2005). 'Information Systems Security Governance Research: A Behavioral Perspective.' *Proceedings of the Symposium on Information Assurance*, Academic Track of 9th Annual NYS Cyber Security Conference, pp. 18-26.

Mitnick, K. D., & Simon, W. L. (2003). *The Art of Deception*. John Wiley & Sons, Inc.

Mylonas, A., Kastania, A. & Gritzalis, D., (2012). 'Delegate the Smartphone User ? Security awareness in Smartphone Platforms.' *Computers & Security*; (34): 47–66.

National Cyber Security Alliance (2017). StaySafeOnline.org. (n.d.). https://staysafeonline.org/ [Accessed on April 15, 2017].

Nguyen, K. D., Rosoff, H., & John, R. S. (2017). 'Valuing Information Security from a Phishing Attack.' *Journal of Cybersecurity*; 1-13.

NIST (2003), *National Institute of Standards and Technology. Building an Information Technology Security Awareness and Training Program*. Computer Security Division Information Technology Laboratory. USA.

O'Donnell, A. (2018). 'How to Prevent IT "Security Fatigue".' http://netsecurity.about.com/od/advancedsecurity/a/How-To-Avoid-IT-Security Fatigue.htm

Oh, O., Agrawal, M., & Rao, H. R. (2011). 'Information Control and Terrorism: Tracking the Mumbai Terrorist Attack Through Twitter.' *Information Systems Front*; 13(1): 33e43.

Ostrom, E., & Hess, C. (2007) *Private and Common Property Rights*. In B. Bouckaert (Ed.), Encyclopedia of Law & Economics. Northampton, MA: Edward Elgar.

Parsons, K., McCormac, A., Pattinson, M., Butavicious, M., Zwaans, T., & Calic, D. (2014). 'A Study of Information Security Awareness in Australian Government Organisations.' *Information Management & Computer Security*; 334–345.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). 'The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies.' *Computers & Security*; 66: 40-51.

Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in Computing*. 4th ed. Upper Saddle River, NJ. Prentice-Hall. USA.

Podsakoff, P. M. & Organ, D. (1986). 'Self-reports in Organizational Research: Problems and Prospects.' *Journal of Management*; 12(4): 531-544.

Rahim, N. H. A., Hamid, S., Mat Kiah, M. L., Shamshirband, S., & Furnell, S. (2015). 'A Systematic Review of Approaches to Assessing Cybersecurity Awareness.' *Kybernetes*; 44(4): 606-622.

Rogers, R. W. (1985). 'Attitude Change and Information Integration in Fear Appeals.' *Psychological Reports*; 56: 183–188.

Roper, C., Fischer, L., & Grau, J. (2006). *Security Awareness, Education and Training*, United Kindom. Elsevier Inc.

SANS (2017). Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017a. White paper.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). 'Transforming the 'weakest link' a Human/Computer Interaction Approach to Usable and Effective Security.' *BT Technology Journal;* 19(3): 122e31.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). 'The impact of information richness on information security awareness training effectiveness.' *Computers & Education*; 52(1), 92-100.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). 'Analysis of End User Security Behaviors.' *Computers & Security*; 24(2): 124-133.

Straub, D. W., & Welke, R. J. (1998). 'Coping with Systems Risk: Security Planning Models for Management Decision Making.' *MIS Quarterly*; 2(4): 441-64.

Seccombe, A., Hutton, A., Meise, I. A., Windel, A., & Mohammed, A. (2009). 'Security Guidance for Critical Areas of Focus in Cloud Computing.' *Cloud Security Alliance*; 2(1): 25.

Schlienger, T., & Teufel, S. (2003). 'Information Security Culture – from Analysis to Change.' *South African Computer Journal*; 31: 46-52.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). 'The Impact of Information Richness on Information Security Awareness Training Effectiveness.' *Computers & Education*; 52(1), 92-100.

Sim, I., Liginlal, D., & Khansa, L. (2012). 'Information Privacy Situation Awareness: Construct and Validation.' *Journal of Computer Information Systems*; 53(1): 57e64.

Siponen, M. T. (2000). 'A Conceptual Foundation for Organizational Information Security Awareness.' *Information Management and Computer Security*; 8(1): 31–41.

Siponen, M. (2006). 'Information Security Standards Focus on the Existence of Process, Not Its Content.' *Communications of the ACM*; 49(8).

Sophos, (2009), *The Sophos Security Threat Report – 2009.* Available from: http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat report-jan-2009-na.pdf. [Accessed on 10 September 2018].

Straub, D. W. (1990). 'Effective IS Security: An Empirical Study.' *Information System Research*; 1(2): 255-77.

Subashini, S. N., & Kavitha, V. (2011). 'A Survey on Security Issues in Service Delivery Models of Cloud Computing.' *Journal of Network and Computer Applications*; 34: 1-11.

Syed, Z., Padia, A., Finin, T., Mathews, L., & Joshi, A. (2016). UCO: 'A Unified Cybersecurity Ontology.' In Workshops at the Thirtieth AAAI Conference on Artificial Intelligence.

Ten, C. W., Liu, C. C., & Manimaran, G. (2008). 'Vulnerability Assessment of Cybersecurity for SCADA Systems.' *IEEE Transactions on Power Systems* [Online]; 23(4): 1836–1846. Available from: http://dx.doi.org/10.1109/TPWRS.2008.2002298. (Accessed on June 25, 2018].

Tekerek, M., & Tekerek, A. (2013). 'A Research on Students' Information Security Awareness.' *Turkish Journal of Education*; 2(3).

Thomson, M. E., & von Solms, R. (1998). 'Information Security Awareness: Educating Your Users Effectively.' *Information management & Computer Security*; 6(4): 167-173.

Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook*. USA. Auerbach Publications.

Torten, R., Reaiche, C., & Boyle, S. (2018). 'The Impact of Security Awareness on Information Technology Professionals' Behavior.' *Computers & Security*; 79: 68-79.

Van Niekerk, J. F. (2005). *'Establishing an Information Security Culture in Organizations: an Outcomes Based Education Approach.'* Doctoral dissertation, Nelson Mandela Metropolitan University, Port Elizabeth. [Published].

Van Niekerk, J., & Von Solms, R. (2004). *Corporate Information Security Education. In Information Security Management, Education and Privacy* (pp. 3-18). Springer, Boston, MA.

Von Solms, R. (1998). 'Information Security Management (3): The Code of Practice for Information Security Management (BS7799).' *Information Management & Computer Security*; 6(5): 224-5.

Von Solms, S. H. (2010). 'Securing the Internet: Fact or Fiction?' *In Proceedings of the IFIP iNetSec Conference*, Sofia, Bulgaria.

Von Solms, R., & Von Solms, B. (2004). 'From Policies to Culture.' *Computers and Security*; 23(4): 275–9.

Wang, C., Wang, Q., & Ren, K. (2009). 'Ensuring Data Storage Security in Cloud Computing.' *Cryptology ePrint Archive*; Report 2009.

Winkler, I., & Manke, S. (2013). '6 Essential Components for Security Awareness programs' [Online]: http://www.csoonline.com/article/2133971/strategic-planning-erm/6essentialcomponents-for-security-awareness-programs.html
[Accessed on March 10, 2018].

Whitman, M. E., & Mattord, H. J. (2004). *Management of Information Security*. Boston, Mass.: Thomson Course Technology. USA.

Wilson, J. H. (2003). '*Building an Information Technology Security Awareness and Training Program*.' USA. National Institute of Standards and Technology.

Witte, K. (1993). 'Message and Conceptual Confounds in Fear Appeals: The Role of Threat, Fear and Efficacy.' *The Southern Communication Journal*; 58(2): 147-155.

Workman, M., Bommer, W.H. & Straub, D. (2008). 'Security lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test.' *Computers in Human Behavior*; 24(6): 2799-2816.

Zhu, B., Sastry, S., & Joseph, A. (2011). 'A Taxonomy of Cyber Attacks on SCADA Systems.' *IEEE International Conference. IEEE International Conference on Cyber, Physical and Social Computing*. 380-388. doi:10.1109/iThings/CPSCom.2011.34. [Accessed on December 10, 2018].

Appendices

Appendix A: Sample Demographics by Location

Crosstabulation Germany

Gender		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	16	51.6	51.6	51.6
	Female	15	48.4	48.4	100.0
	Total	31	100.0	100.0	

Table 30: Gender Composition – Germany

A visual inspection of this table immediately reveals that 51.6% of participants (16 participants) are males, and that 48.4% of participants (15 participants) are females.

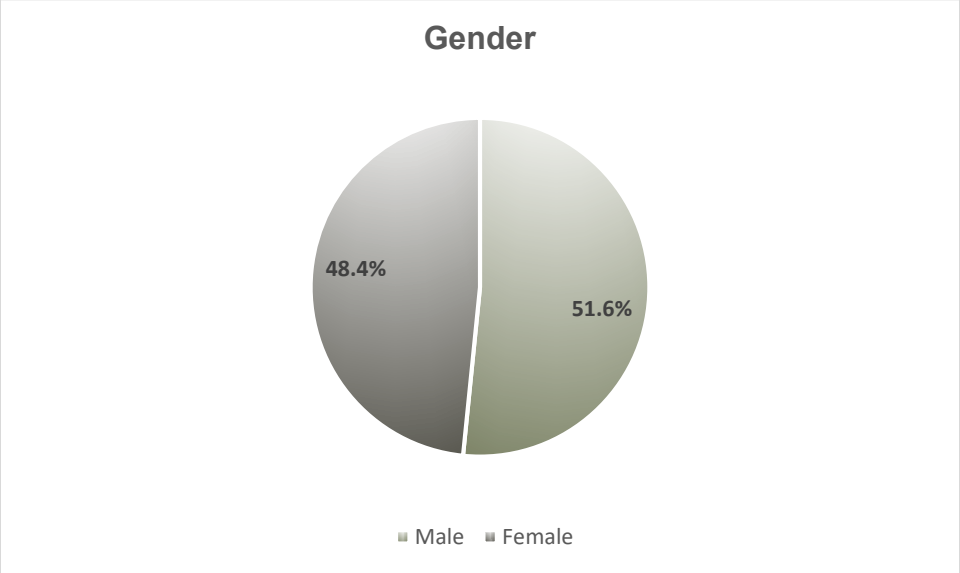


Figure 6: Gender Composition – Germany

Age range					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20 to 25	23	74.2	74.2	74.2
	26 to 30	5	16.1	16.1	90.3
	31 to 35	1	3.2	3.2	93.5
	36 to 40	2	6.5	6.5	100.0
	Total	31	100.0	100.0	

Table 31: Age range Composition – Germany

A visual inspection of this table immediately reveals that 74.2% of participants (23 participants) are between the ages of 20 to 25 years. This is the youngest group of participants in this study. Further, only 6.5% of participants (2 participants) self-reported being part of the oldest age group (36 to 40 years).

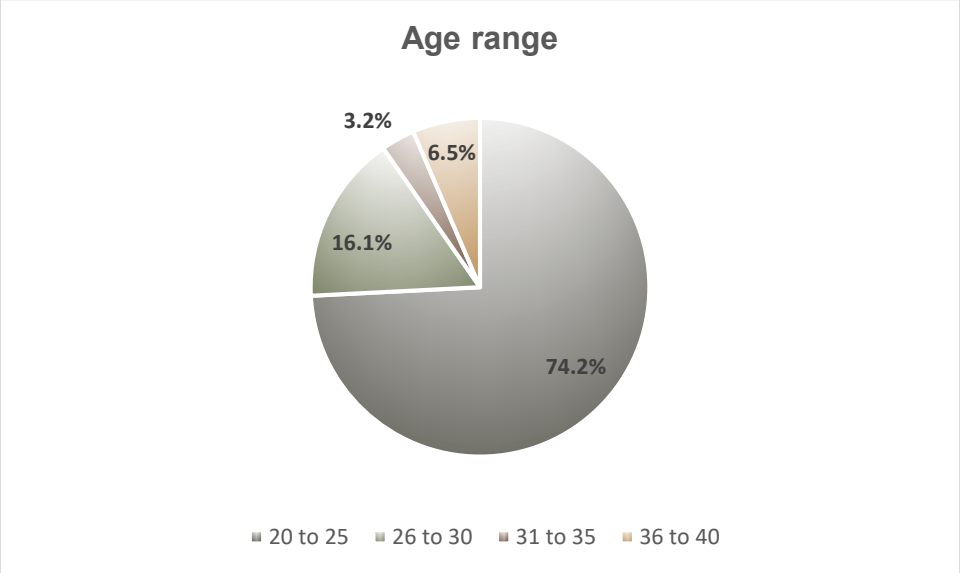


Figure 7: Age range Composition – Germany

Education Level					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High School	0	0	0	0
	Technical and Professional degree (any degree)	4	12.9	12.9	12.9
	Some University Studies (not completed in full)	22	71.0	71.0	83.9
	University degree (any degree)	5	16.1	16.1	100.0
	Total	31	100.0	100.0	

Table 32: Education Level Composition – Germany

A visual inspection of this table immediately reveals that 12.9% of participants (4 participants) self-reported to hold a technical/professional degree. Further, 16.1% of participants (5 participants) self-reported to have a university degree.

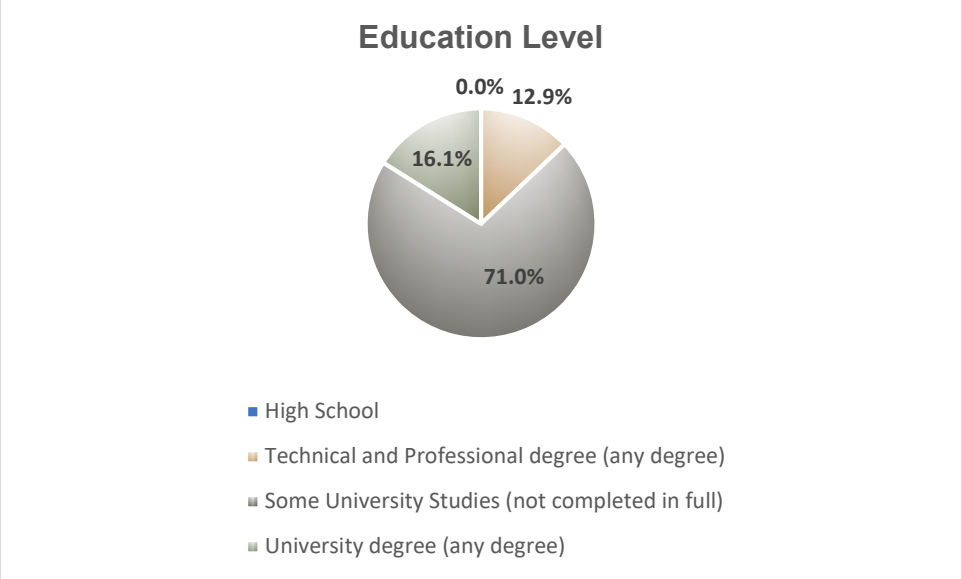


Figure 8: Education Level Composition – Germany

Employment Status					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unemployed	1	3.2	3.2	3.2
	Part-time	17	54.8	54.8	58.1
	Full time	13	41.9	41.9	100.0
	Total	31	100.0	100.0	

Table 33: Employment Status Composition – Germany

A visual inspection of this table immediately reveals that 3.2% of participants (1 participant) are unemployed. Further, 41.9% of participants (13 participants) self-reported to be employed full time. Only 54.8% of participants (17 participants) self-reported being employed as part-time basis.

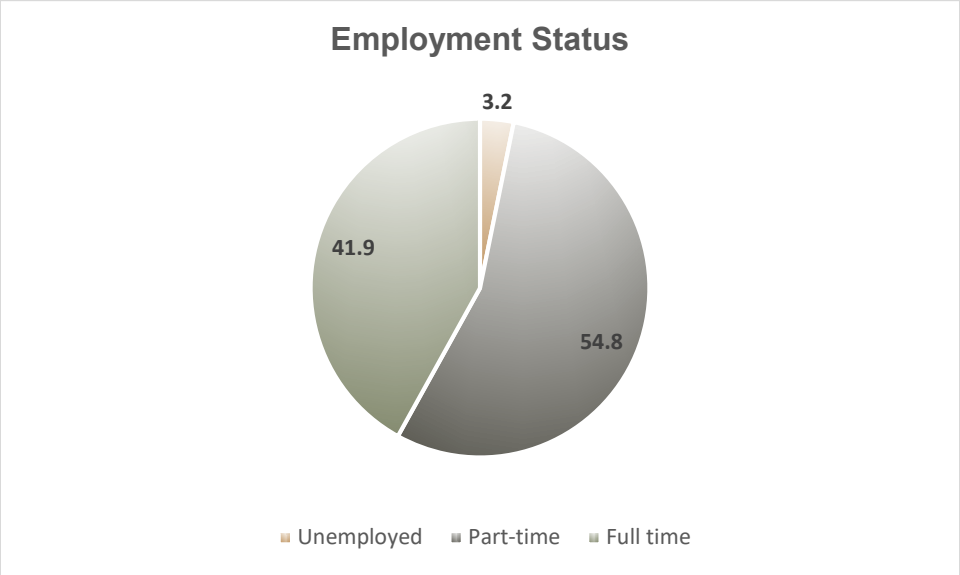


Figure 9: Employment Status Composition – Germany

Crosstabulation United Kingdom (UK)

Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	25	80.6	80.6	80.6
	Female	6	19.4	19.4	100.0
	Total	31	100.0	100.0	

Table 34: Gender Composition – UK

A visual inspection of this table immediately reveals that 80.6% of participants (25 participants) are males, and that 19.4% of participants (6 participants) are females.

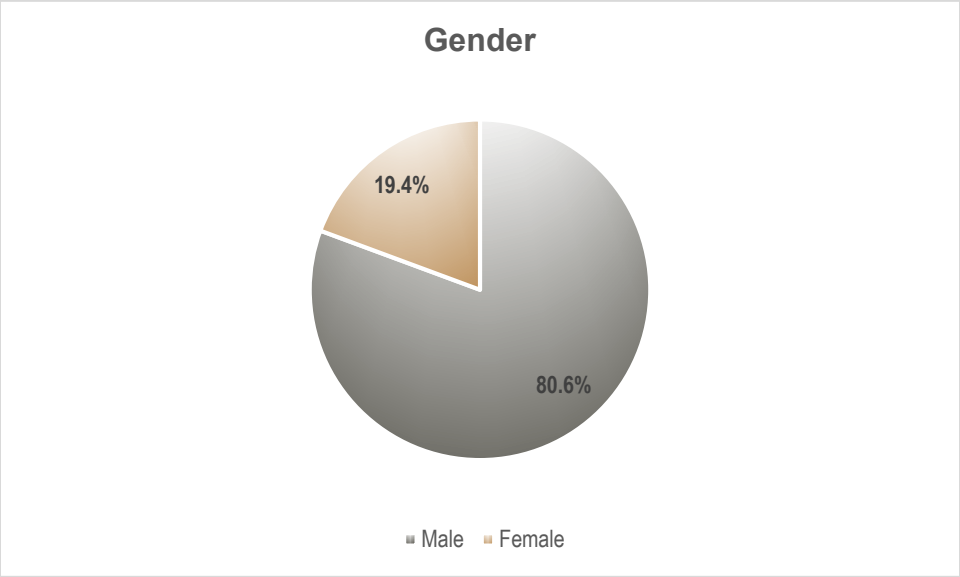


Figure 10: Gender Composition – UK

Age range					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20 to 25	21	67.7	67.7	67.7
	26 to 30	6	19.4	19.4	87.1
	31 to 35	1	3.2	3.2	90.3
	36 to 40	3	9.7	9.7	100.0
	Total	31	100.0	100.0	

Table 35: Age range Composition – UK

A visual inspection of this table immediately reveals that 67.7% of participants (21 participants) are between the ages of 20 to 25 years. This is the youngest group of participants in this study. Further, only 9.7% of participants (3 participants) self-reported being part of the oldest age group (36 to 40 years).

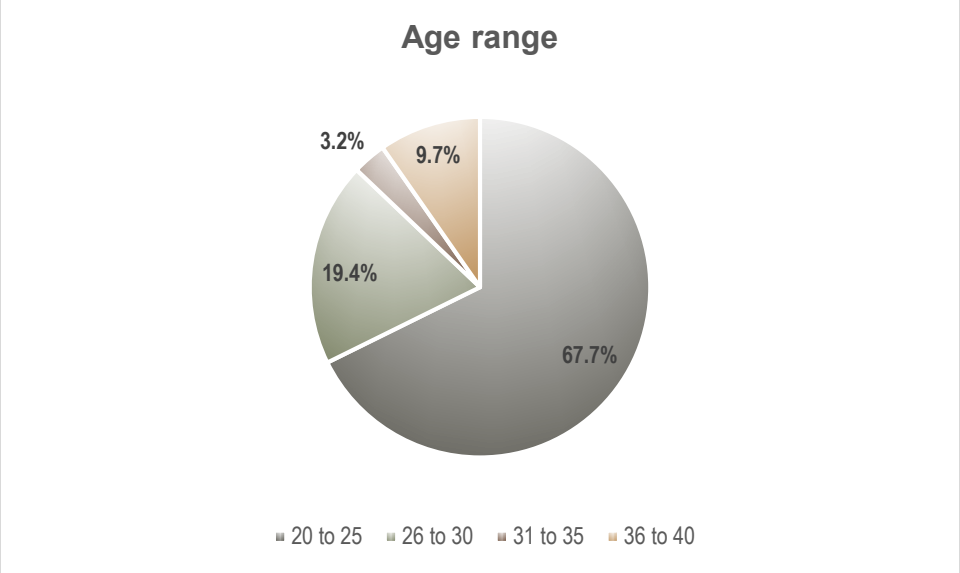


Figure 11: Age range Composition – UK

Education Level					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High School	5	16.1	16.1	16.1
	Technical and Professional degree (any degree)	8	25.8	25.8	41.9
	Some University Studies (not completed in full)	15	48.4	48.4	90.3
	University degree (any degree)	3	9.7	9.7	100.0
	Total	31	100.0	100.0	

Table 36: Education Level Composition – UK

A visual inspection of this table immediately reveals that 16.1% of participants (5 participants) have completed high school education level only. Further, 25.8% of participants (8 participants) self-reported to hold a technical/professional degree. Only 9.7% of participants (3 participants) self-reported to have a university degree.

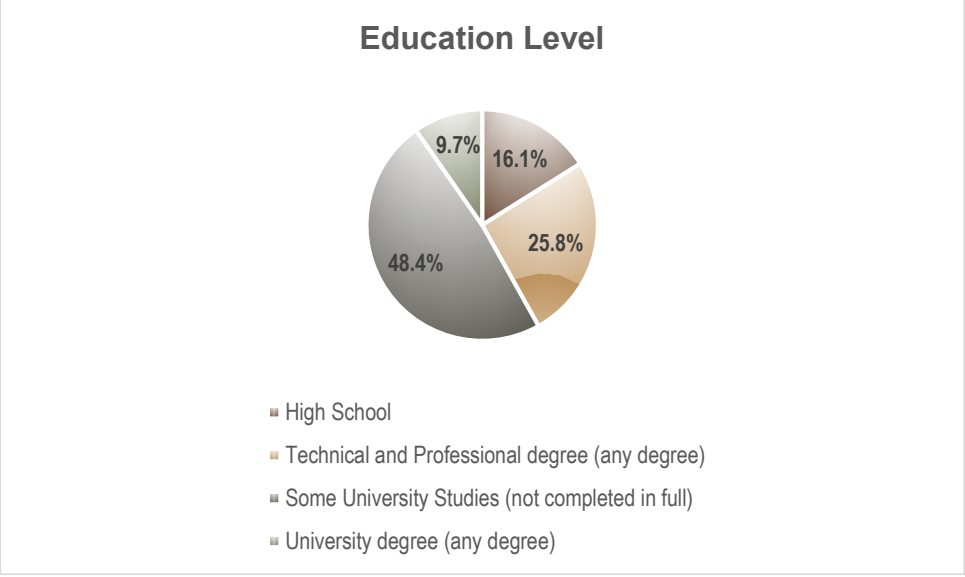


Figure 12: Education Level Composition – UK

Employment Status					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unemployed	1	3.2	3.2	3.2
	Part-time	2	6.5	6.5	9.7
	Full time	28	90.3	90.3	100.0
	Total	31	100.0	100.0	

Table 37: Employment Status Composition – UK

A visual inspection of this table immediately reveals that 3.2% of participants (1 participant) are unemployed. Further, 90.3% of participants (28 participants) self-reported to be employed full time. Only 6.5% of participants (2 participants) self-reported being employed as part-time basis.

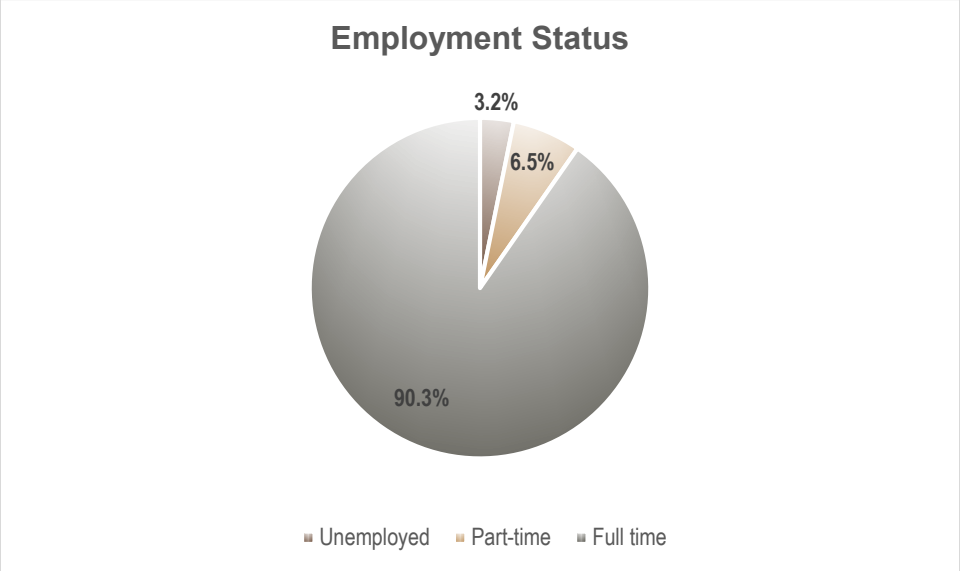


Figure 13: Employment Status Composition – UK

Crosstabulation United States (USA)

Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	20	64.5	64.5	64.5
	Female	11	35.5	35.5	100.0
	Total	31	100.0	100.0	

Table 38: Gender Composition – USA

A visual inspection of this table immediately reveals that 64.5% of participants (20 participants) are males, and that 35.5% of participants (11 participants) are females.

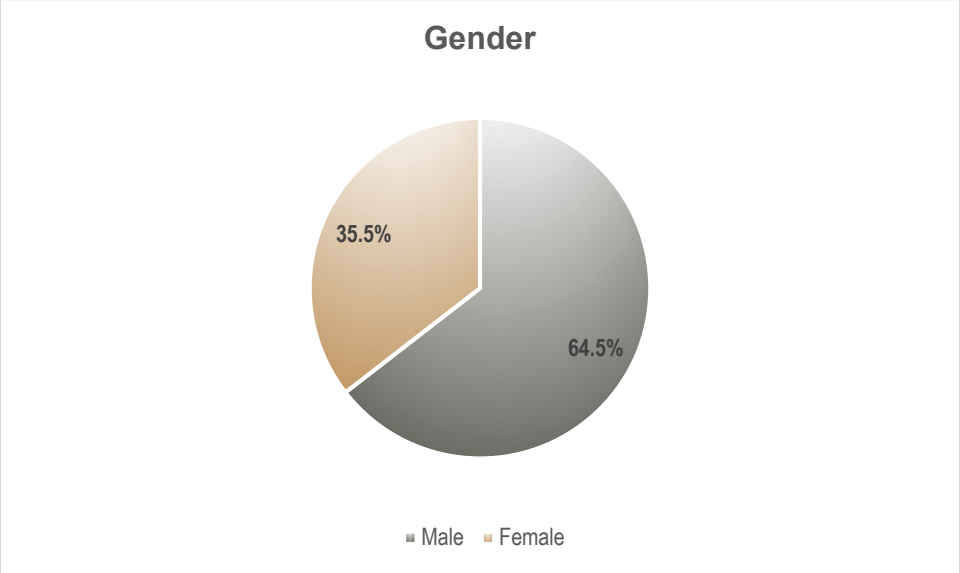


Figure 14: Gender Composition – USA

Age range					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20 to 25	31	100.0	100.0	100.0

Table 39: Age range Composition – USA

a visual inspection of this table immediately reveals that 100% of participants (31 participants) are between the ages of 20 to 25 years. This is the youngest group of participants in this study.

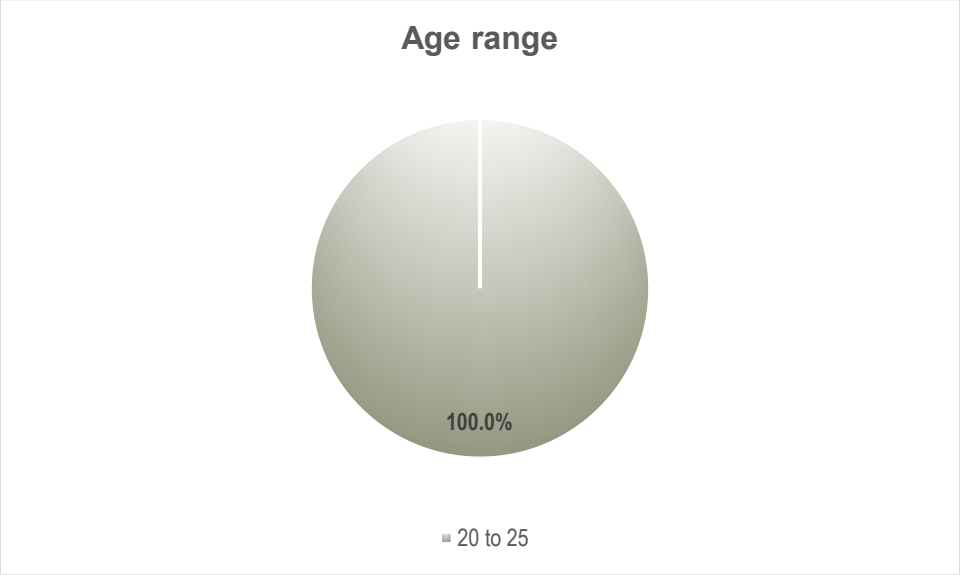


Figure 15: Age range Composition – USA

Education Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Technical and Professional degree (any degree)	0	0	0	0
	High School	9	29.0	29.0	29.0
	Some University Studies (not completed in full)	19	61.3	61.3	90.3
	University degree (any degree)	3	9.7	9.7	100.0
	Total	31	100.0	100.0	

Table 40: Education Level Composition – USA

A visual inspection of this table immediately reveals that 29% of participants (9 participants) have completed high school education level only. Further, no participants (0

participants) self-reported to hold a technical/professional degree. Only 9.7% of participants (3 participants) self-reported to have a university degree.

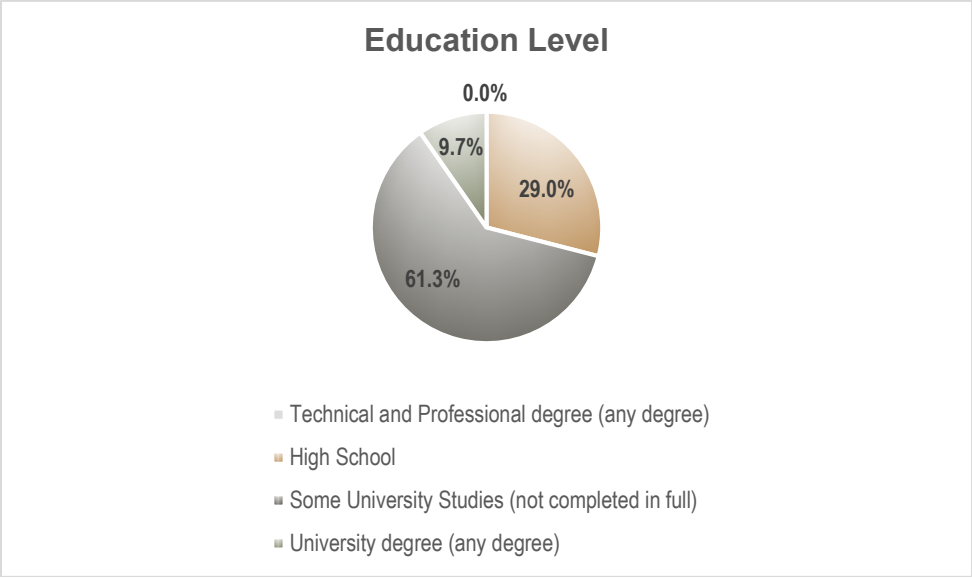


Figure 16: Education Level Composition – USA

Employment Status

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unemployed	10	32.3	32.3	32.3
	Part-time	15	48.4	48.4	80.6
	Full time	6	19.4	19.4	100.0
	Total	31	100.0	100.0	

Table 41: Employment Status Composition – USA

A visual inspection of this table immediately reveals that 32.3% of participants (10 participants) are unemployed. Further, 19.4% of participants (6 participants) self-reported to be employed full time. Only 48.4% of participants (15 participants) self-reported being employed as part-time basis.

Figure 17: Employment Status Composition – USA

Appendix B: Awareness Level by Location Crosstabulation

Crosstabulation Germany

Awareness Level		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Unaware	0	0	0	
	Unaware	2	6.5	6.5	6.5
	Neutral	7	22.6	22.6	29.0
	Aware	17	54.8	54.8	83.9
	Very Aware / Always	5	16.1	16.1	100.0
	Total	31	100.0	100.0	

Table 42: Awareness Level Composition – Germany

A visual inspection of this table immediately reveals that 16.1% of participants (5 participants) self-reported being very aware of cybersecurity issues. In addition, 22.6% of participants (7 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 6.5% of participants (2 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

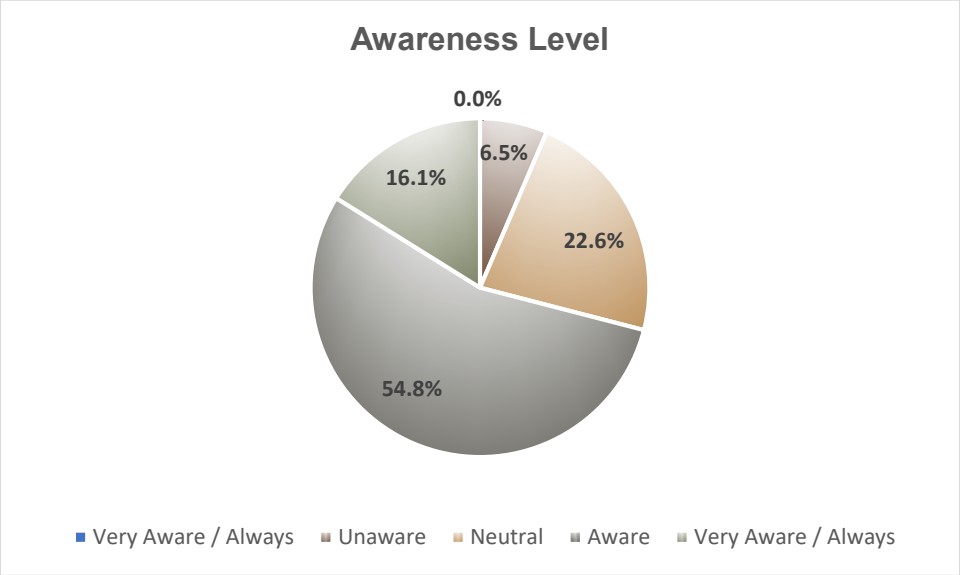


Figure 18: Awareness Level Composition – Germany

Crosstabulation United Kingdom (UK)

Awareness Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Unaware	0	0	0	0
	Unaware	0	0	0	0
	Neutral	6	19.4	19.4	19.4
	Aware	18	58.1	58.1	77.4
	Very Aware / Always	7	22.6	22.6	100.0
	Total	31	100.0	100.0	

Table 43: Awareness Level Composition – UK

A visual inspection of this table immediately reveals that 22.6% of participants (7 participants) self-reported being very aware of cybersecurity issues. In addition, 19.4% of participants (6 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, no participants (0 participants) self-reported being unaware of cybersecurity issues, as defined in the survey.

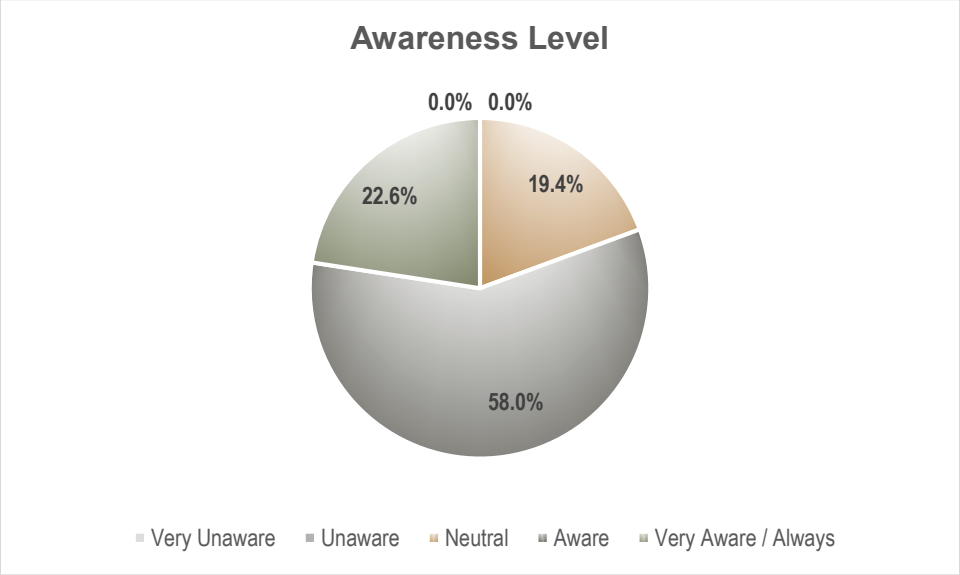


Figure 19: Awareness Level Composition – UK

Crosstabulation United States (USA)

Awareness Level		Frequency	Percent	Valid Percent	Cumulative Percent
	Very Unaware	0	0	0	0
Valid	Unaware	1	3.2	3.2	3.2
	Neutral	12	38.7	38.7	41.9
	Aware	15	48.4	48.4	90.3
	Very Aware / Always	3	9.7	9.7	100.0
	Total	31	100.0	100.0	

Table 44: Awareness Level Composition – USA

A visual inspection of this table immediately reveals that 9.7% of participants (3 participants) self-reported being very aware of cybersecurity issues. In addition, 38.7% of participants (12 participants) remained neutral and did not acknowledge any cybersecurity awareness level or the lack of it. Further, only 3.2% of participants (1 participant) self-reported being unaware of cybersecurity issues, as defined in the survey.

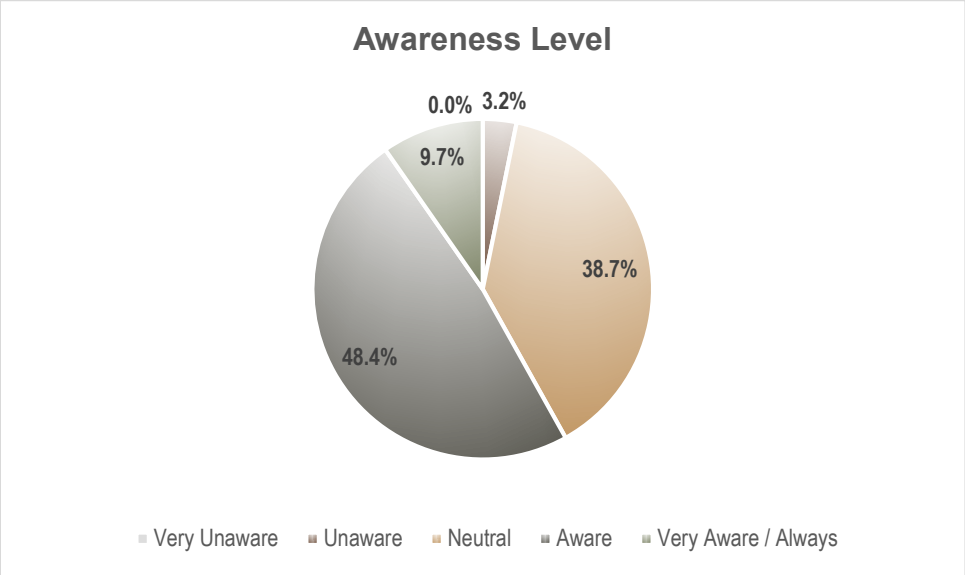


Figure 20: Awareness Level Composition – USA

Appendix C: Awareness Level by Location

Germany

Gender and Awareness Level (Location Germany; *n*=31)					
H_0(a)	There is no difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.				
H_1(a)	There is a difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.				
Test:	Mann-Whitney U	**Value (U):**	101.0	**p- value:**	0.407
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(a). Therefore, there is no evidence against the null hypothesis.				

Table 45: Gender and Awareness Level Difference – Germany

Age range and Awareness Level (Location Germany; *n*=31)					
H_0(b)	There is no relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.				
H_1(b)	There is a relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	-0.053	**p-value:**	0.563
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(b). Therefore, there is no evidence against the null hypothesis.				

Table 46: Age range and Awareness Level Relationship – Germany

Education Level and Awareness Level (Location Germany; *n*=31)					
H_0(c)	There is no relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
H_1(c)	There is a relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	0.034	**p-value:**	0.796
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(c). Therefore, there is no evidence against the null hypothesis.				

Table 47: Education Level and Awareness Level Relationship – Germany

Employment Status and Awareness Level (Location Germany; *n*=31)					
H_0(d)	There is no relationship between the cybersecurity awareness level of individuals and their employment status, in an academic setting in higher education.				
H_1(d)	There is a relationship between the cybersecurity awareness level of individuals and their employment status, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	0.016	**p-value:**	0.915
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(d). Therefore, there is no evidence against the null hypothesis.				

Table 48: Employment Status and Awareness Level Relationship – Germany

United Kingdom (UK)

Gender and Awareness Level (Location UK; *n*=31)					
H_0(a)	There is no difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.				
H_1(a)	There is a difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.				
Test:	Mann-Whitney U	**Value (U):**	60.500	**p- value:**	0.414
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(a). Therefore, there is no evidence against the null hypothesis.				

Table 49: Gender and Awareness Level Difference – UK

Age range and Awareness Level (Location UK; *n*=31)					
H_0(b)	There is no relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.				
H_1(b)	There is a relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	-0.103	**p-value:**	0.516
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(b). Therefore, there is no evidence against the null hypothesis.				

Table 50: Age range and Awareness Level Relationship – UK

Education Level and Awareness Level (Location UK; *n*=31)					
H_0(c)	There is no relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
H_1(c)	There is a relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	-0.272	**p-value:**	**0.017**
Interpretation:	When p-value ≤ 0.05 the null hypothesis H_0(c) is rejected. Therefore, there is evidence against the null hypothesis.				

Table 51: Education Level and Awareness Level Relationship – UK

Employment Status and Awareness Level (Location UK; *n*=31)					
H_0(d)	There is no relationship between the cybersecurity awareness level of individuals and their employment status, in an academic setting in higher education.				
H_1(d)	There is a relationship between the cybersecurity awareness level of individuals and their employment status, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	0.012	**p-value:**	0.905
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(d). Therefore, there is no evidence against the null hypothesis.				

Table 52: Employment Status and Awareness Level Relationship – UK

United States (USA)

Gender and Awareness Level (Location USA; *n*=31)					
H_0(a)	There is no difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.				
H_1(a)	There is a difference between the cybersecurity awareness level of individuals and their gender, in an academic setting in higher education.				
Test:	Mann-Whitney U	**Value (U):**	91.000	**p-value:**	0.389
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(a). Therefore, there is no evidence against the null hypothesis.				

Table 53: Gender and Awareness Level Difference – USA

Age range and Awareness Level (Location USA; *n*=31)					
H_0(b)	There is no relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.				
H_1(b)	There is a relationship between the cybersecurity awareness level of individuals and their age, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**		**p-value:**	
Interpretation:	Unable to compare to other age range groups, since there is only one age range group.				

Table 54: Age range and Awareness Level Relationship – USA

Education Level and Awareness Level (Location USA; *n*=31)					
H_0(c)	There is no relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
H_1(c)	There is a relationship between the cybersecurity awareness level of individuals and their education level completed, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	-0.109	**p-value:**	0.459
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(a). Therefore, there is no evidence against the null hypothesis.				

Table 55: Education Level and Awareness Level Relationship – USA

Employment Status and Awareness Level (Location USA; *n*=31)					
H_0(d)	There is no relationship between the cybersecurity awareness level of individuals and their employment status, in an academic setting in higher education.				
H_1(d)	There is a relationship between the cybersecurity awareness level of individuals and their employment status, in an academic setting in higher education.				
Test:	Kendall-Stuart tau-c	**Value (Tau-c):**	-0.100	**p-value:**	0.503
Interpretation:	When p-value ≥ 0.05 we fail to reject the null hypothesis H_0(d). Therefore, there is no evidence against the null hypothesis.				

Table 56: Employment Status and Awareness Level Relationship – USA

Appendix D: Cybersecurity Awareness Survey

Cybersecurity: User Awareness
Date:
Room:

#	ITEMS (30)
	Survey Items (26)
	Demographic Items (4)
1	**I am familiar with the University's Information Security Policies and my responsibilities for protecting University resources?**
2	**When away, I always lock my PC and employ my system's password protected screen saver?**
3	**I understand the requirements for and use of strong passwords?**
4	**I never share my password or post it where others may obtain access to it?**
5	**I know how to protect against 'social engineering' 'phishing' and 'cybercrime'?**
6	**I am careful not to discuss sensitive information in public places?**
7	**I know the location of my department's shredder or secure recycle bin for disposal of 'sensitive' information?**
8	**When browsing or downloading from the Internet, I only access trusted, reputable sites?**
9	**When downloading software, I abide by all license/copyright laws?**
10	**I am careful when opening email attachments and links?**
11	**I know when and who to contact if I suspect an information security incident?**
12	**I know the types of information handled in my area and the applicable regulations?**
13	**I understand what information is considered 'sensitive' (Confidential and Proprietary)?**
14	**I am familiar with the appropriate methods for transmitting, storing, labeling and handling sensitive information?**
15	**I always encrypt sensitive data when sending via external email and I know how/when hardware and mobile devices should be encrypted?**
16	**I ensure that sensitive data is protected on mobile devices?**
17	**I do not leave sensitive data unattended in open areas (copiers, faxes, desktops)?**
18	**My sensitive/critical data is backed up on a routine basis and recovery is tested periodically?**
19	**I am aware of my department's Business Continuity Plans and of my responsibilities?**
20	**I am aware that texting or posting sensitive data on social sites or using 3rd party storage may violate policy or regulations?**
21	**I am aware of and adhere to physical security practices?**
22	**I physically secure my mobile computing devices (laptops, portable drives, smart devices)?**
23	**I am aware of building evacuation and safety plans?**
24	**My University owned computing devices are current with virus protection and software patches?**
25	**If approved to use my personal computing devices, I am aware of and use security measures?**
26	**My sensitive/critical data is stored on systems which are located in a secure area?**
27	*My Gender is:*
28	*My age range is:*
29	*My Highest education is:*
30	*I am employed:*

Appendix E: Frequencies Comparison Among the Three Groups

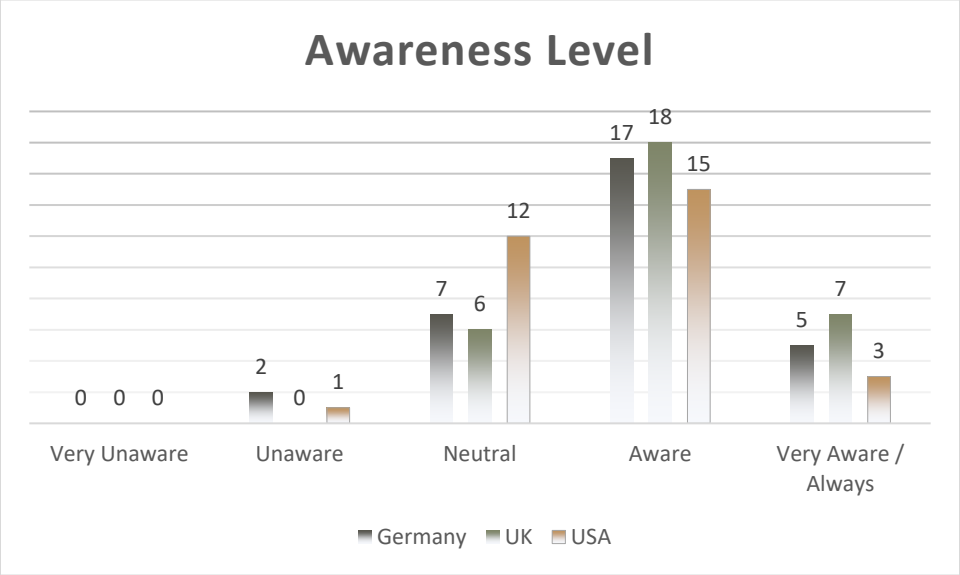


Table 57: Awareness Level Frequencies

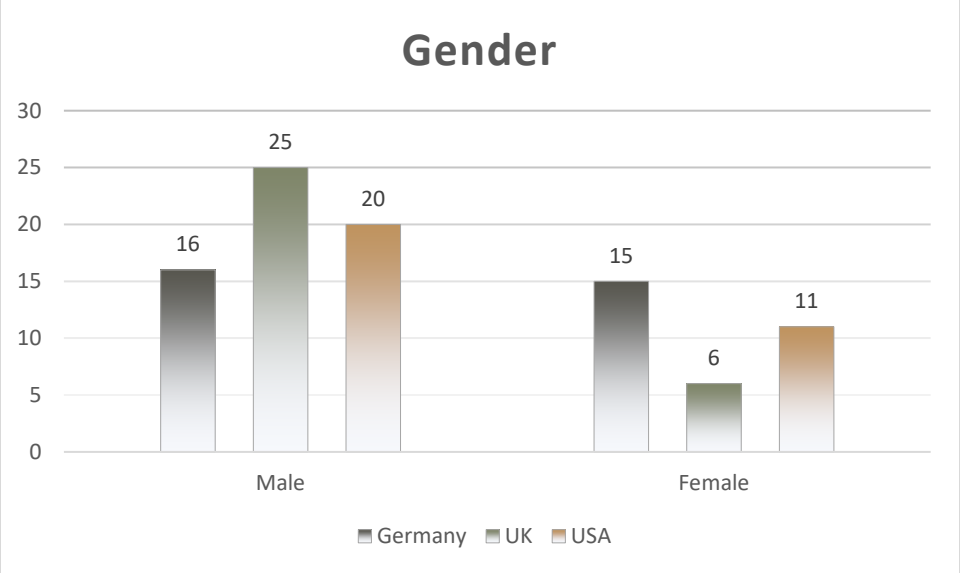


Table 58: Gender Frequencies

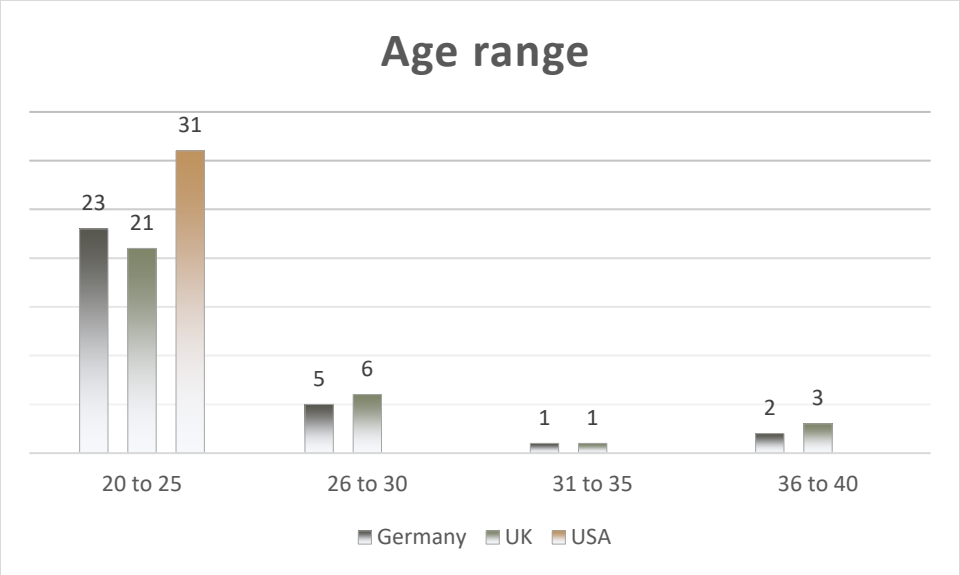


Table 59: Age range Frequencies

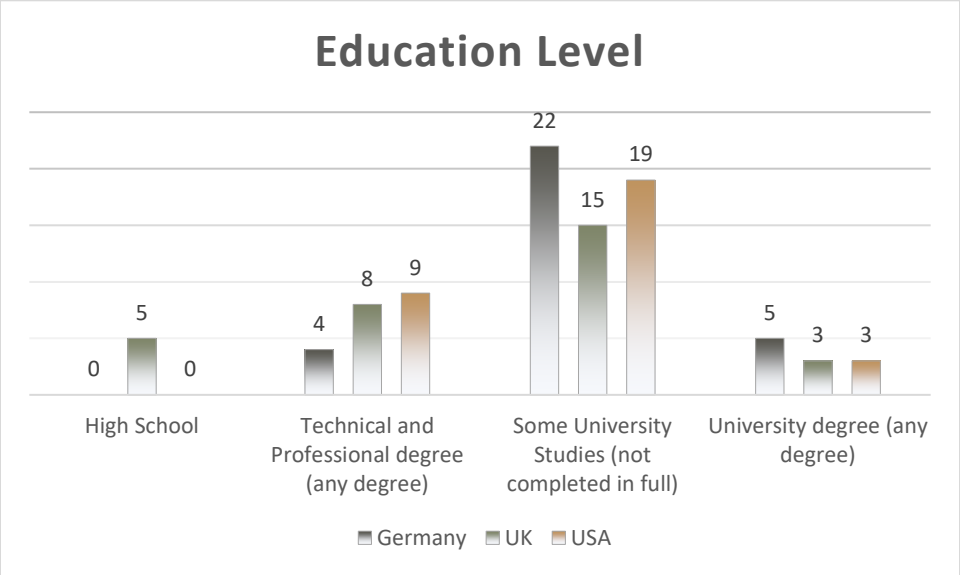


Table 60: Education Level Frequencies

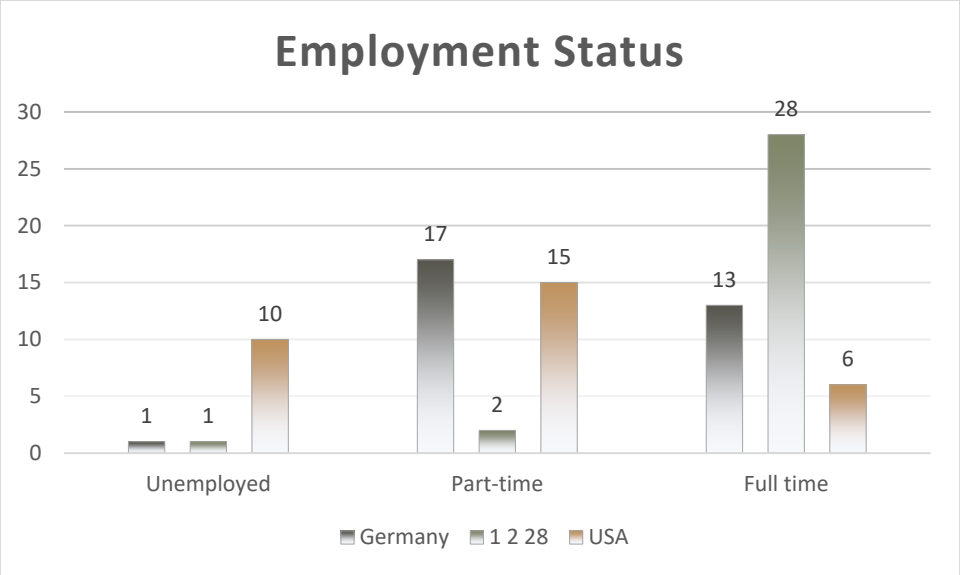
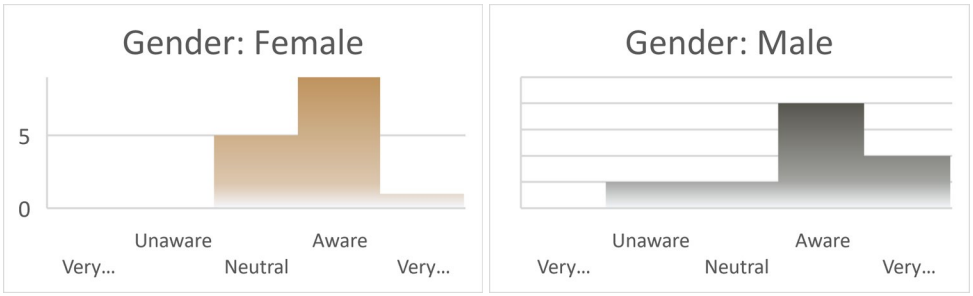


Table 61: Employment Status Frequencies

Appendix F: Evaluation of Distributions for the Mann-Whitney U test



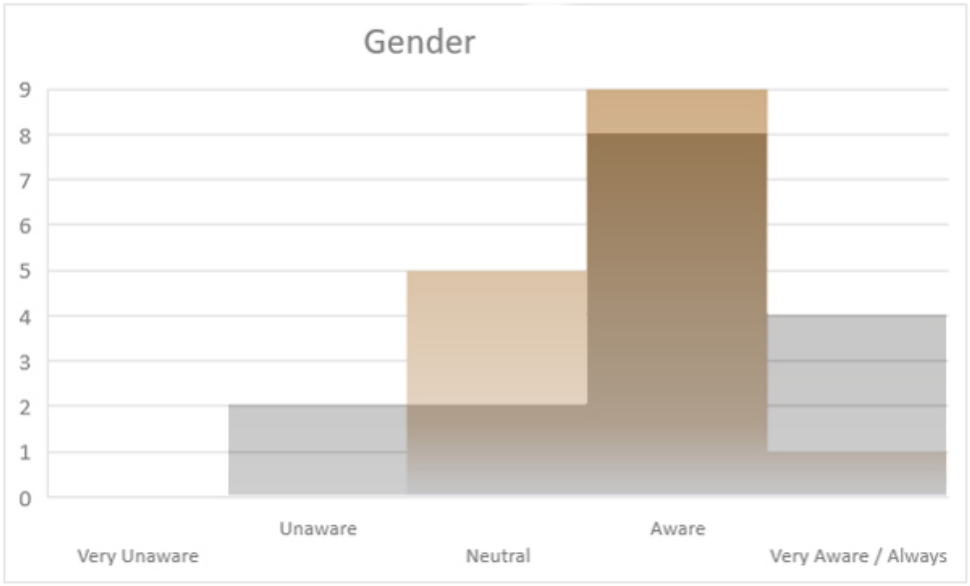
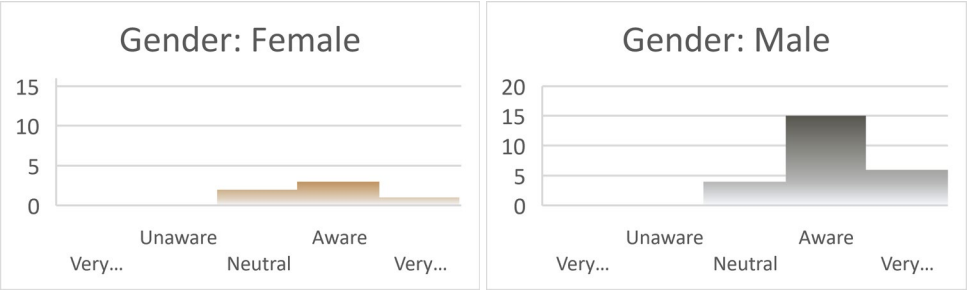


Figure 21: Distribution Evaluation – Germany



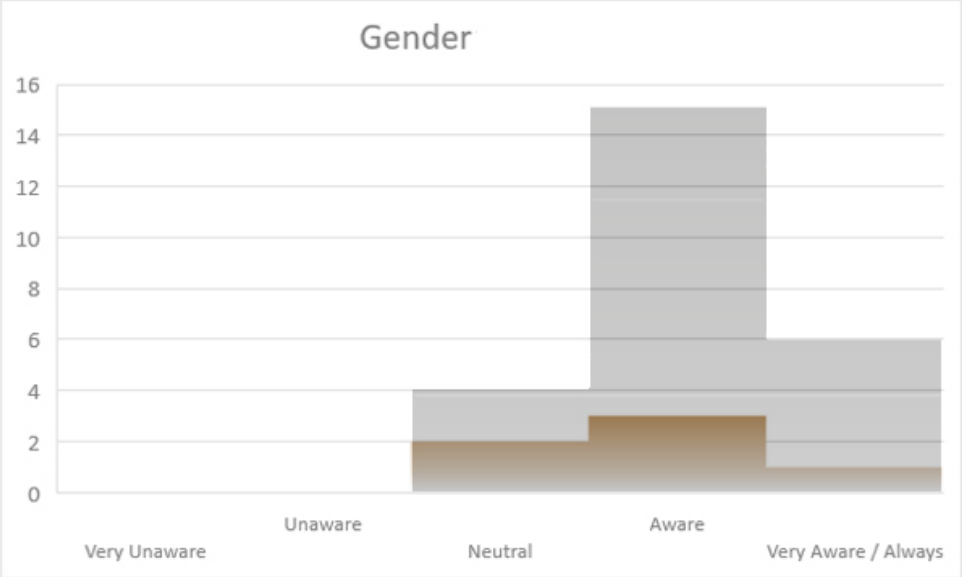


Figure 22: Distribution Evaluation – UK

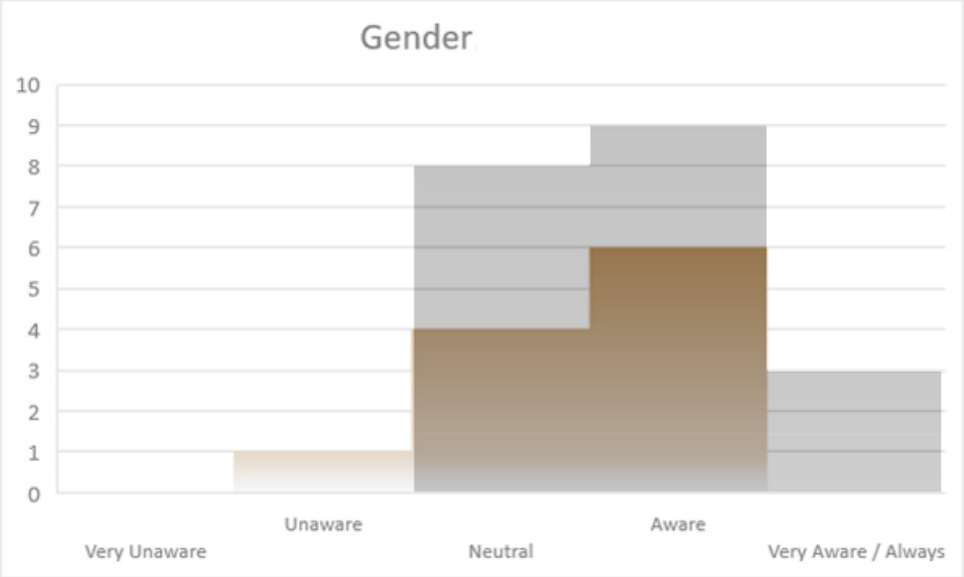


Figure 23: Distribution Evaluation – USA

Appendix G: Emergent Cybersecurity Definitions, Critiques, Conceptual Categories

	Participant Working Definitions	Critique(s)
1	"Cybersecurity is the protection of information/data, assets, services, and systems of value to reduce the probability of loss, damage/corruption, compromise, or misuse to a level commensurate with the value assigned."	In the main, the feedback suggested that the inclusion of value introduced the human concepts related to security, but that the definition was too prescriptive and suffered the problem of a restrictive "listing" of what is being protected.
2	"Cybersecurity is a collection of interacting processes intended to protect cyberspace and cyberspace-enabled systems (collectively resources) from intentional actions designed to misalign actual resource property rights from the resource owner perceived property rights."	This definition introduced the emerging cyber-physical environment and included the important concept of control over property rights. However, the definition's focus on "human intentional actions" was viewed as being overly restrictive.
3	"Cybersecurity is a collection of interacting processes intended to make cyberspace safe and secure."	Specifically intended to be broader than the seed definition, this definition introduced more problems than it solved because it was unnecessarily broad and introduced the contested notion of safety with security.
4	"Cybersecurity is a domain dedicated to the study and practice of the protection of systems or digital assets from any action taken to impose authorization on those systems or digital assets that do not align with the property rights of the resource facility as understood by its owner."	In this definition, the concepts of property rights and control were introduced. However, there were concerns about the potential implications of "action taken" to mean limiting cybersecurity to human actors. Also there were concerns regarding the terms, which imposed limits on the scope of the definition such as "study" and "practice", thereby situating the issues largely within the academic domain.
5	"Cybersecurity is the state in which power over the execution of computers (sensu lato) and over information in the control of computers is where it should be."	This definition reinforced the notions of control over information and systems. The main criticism was defining cybersecurity as a state.

Table 62: Emergent Cybersecurity Definitions, Critiques and Conceptual Categories

Source: Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). 'Defining Cybersecurity'. *Technology Innovation Management Review*; 4(10).

Category	Definition
Asset	In general, defined as "a useful or valuable thing or person". Here, we refine the definition to refer to "cyberspace and cyberspace-enabled systems".
Capability	An abbreviation for the organization and combination of resources, processes, and structures.
Misalign	Align is defined as "put (things) into correct appropriate relative positions"; hence, misalign results in incorrect or inappropriate positions.
Occurrence	An incident or event.
Organization	"A firm's policies and procedures 'organized to exploit the full competitive potential of its resources and capabilities'" (Kozlenkova et al., 2013). We generalize "firms" to "institutions".
Process	The fact of going on or being carried on, as a action or series of actions; progress, course. *in (the) process of (doing something):* in the course of; in the act of carrying out (a particular task, etc.). *in process:* going on, being done; in progress
Property right	An enforceable authority to undertake particular actions in specific domains. Includes the rights of access, withdrawal, management, exclusion, and alienation (Ostrom & Hess, 2007).
Protect	Keep safe from harm or injury.
Resource	"Tangible and intangible assets ['firms'] use to conceive of and implement [their] strategies" (Kozlenkova et al., 2013). We generalize "firms" to "institutions".

Table 63: Conceptual Categories and Their Definitions

Source: Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). 'Defining Cybersecurity'. *Technology Innovation Management Review*; 4(10).

Appendix H: Essential Skills for a Career in Cybersecurity

	General IT job skills	Cybersecurity-specific skills
early career skills	Technical skills (system administration, database, networking, programming languages)	Technical skills (security packages, networks and network security components, firewall management skills, understanding security processes and controls)
	Problem-solving skills	Problem-solving skills (investigation and forensic analysis to detect intruders)
	System development methodology	Support skills (24x7 availability to protect information security)
	Analytical aptitude	communication skills (explain security in simple language and to non-IT personnel)
	Ability to work hard (staying up-to-date on new technology)	
	common sense	
	People skills (establish client confidence, be a team player, encourage loyalty)	
Additional skills for career advancement	Breadth of knowledge	Understanding cybersecurity project strategies and relating them to business and technical requirements
	Ability to learn new technology	
	continuous skill improvement	establish and implement security polices
	communication skills	Audit and review security skills
	Project design	
	Understanding enterprise-level infrastructure	
	Ability to relate business and technical requirements to project strategies	
	Multitasking skills	
	expertise in outsourcing	
	Ability to satisfy clients and customers	
	Loyalty, honesty, and ethical behavior	
	Leadership skills	
	Management aptitude	
	Industry networking skills	

Table 64: Essential Skills for a Career in Cybersecurity

Source: Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). 'Women in cybersecurity: A study of career advancement'. *IT professional*; 12(1): 24-31.

Appendix I: Attitude System towards Security

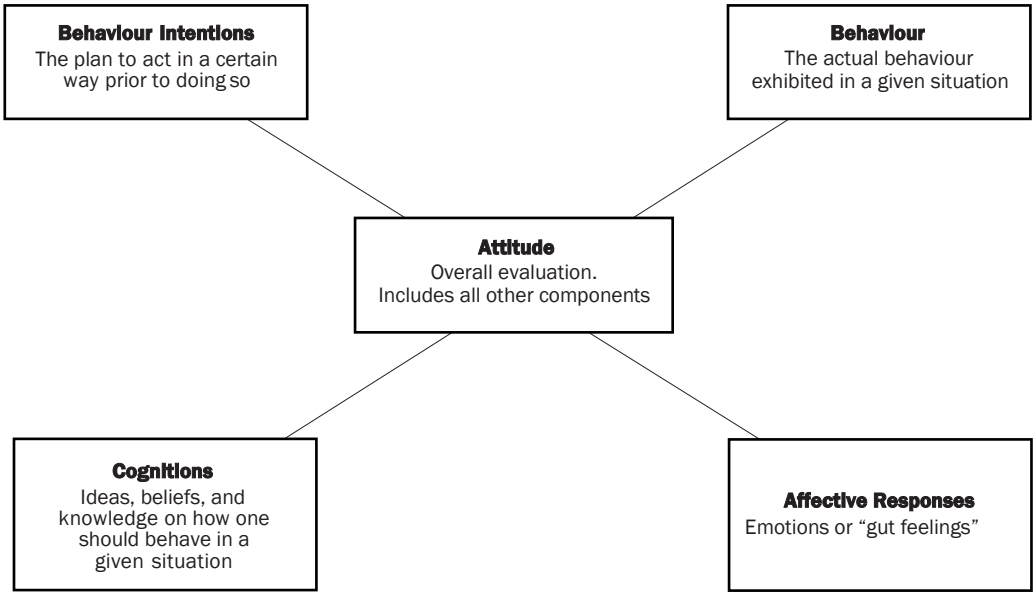


Figure 24: Attitude System towards Security

Source: Thomson, M. E., & von Solms, R. (1998). 'Information security awareness: educating your users effectively'. *Information management & Computer Security*; 6(4): 167-173.

Appendix J: Data Set

Q 0	Q 1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7	Q 8	Q 9	Q 10	Q 11	Q 12	Q 13	Q 14	Q 15	Q 16	Q 17	Q 18	Q 19	Q 20	Q 21	Q 22	Q 23	Q 24	Q 25	Q 26	Q 27	Q 28	Q 29	Q 30	Q F
1	3	5	4	4	4	4	4	3	2	4	5	4	3	4	3	3	4	2	4	2	3	5	4	2	4	4	2	1	3	3	4
2	4	4	4	3	2	4	3	3	3	4	4	4	4	3	3	4	4	2	4	4	4	4	3	4	4	4	1	1	1	3	4
3	1	5	5	5	3	5	5	5	5	5	5	5	5	5	3	3	5	3	5	5	5	3	5	5	5	3	2	2	3	3	5
4	4	4	4	5	3	2	4	4	5	4	4	5	5	4	4	4	5	4	3	3	4	4	4	4	4	3	1	1	3	2	4
5	4	5	4	5	2	5	4	4	2	5	3	2	5	4	2	2	5	5	4	3	4	4	1	2	3	5	2	2	4	3	4
6	1	3	2	4	5	4	1	3	2	4	2	3	4	4	2	3	4	2	3	4	3	2	3	4	3	2	1	4	3	3	3
7	4	3	5	5	5	4	5	4	3	5	1	4	4	3	3	4	4	4	3	4	3	3	3	4	4	2	1	1	3	3	4
8	1	5	5	5	3	4	5	5	3	5	4	4	5	4	3	4	5	2	5	4	3	4	3	3	4	4	1	2	2	3	4
9	4	5	4	5	4	5	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	1	1	3	3	3
10	3	5	5	5	4	5	5	4	5	5	5	4	5	4	3	2	5	1	3	5	5	4	2	3	5	5	1	1	3	3	4
11	3	5	5	4	3	4	5	4	3	5	4	4	4	3	2	2	4	2	3	2	3	4	4	4	4	4	2	1	3	3	4
12	1	5	5	2	5	3	4	3	1	3	5	4	3	4	3	3	4	5	3	4	4	5	3	5	4	2	1	1	4	3	4
13	1	4	5	4	3	4	5	3	4	4	4	4	4	4	3	2	4	2	1	5	3	2	2	5	4	4	1	4	2	3	4
14	2	3	4	2	2	2	2	3	2	2	2	4	4	4	5	4	4	5	4	3	3	2	2	2	2	4	2	2	4	3	3
15	2	5	5	5	4	4	5	5	5	4	3	4	4	4	3	2	4	3	4	2	3	3	4	4	4	3	1	1	1	3	4
16	1	5	5	5	5	5	3	5	1	5	5	4	4	4	5	5	5	5	2	5	4	5	1	4	2	5	1	1	1	3	4
17	4	5	5	5	5	5	5	4	4	5	5	4	5	5	4	4	4	5	5	5	4	5	2	4	5	4	1	1	2	2	5
18	3	5	5	5	4	4	3	4	2	5	4	4	4	4	3	4	5	4	3	3	4	3	4	5	4	4	1	1	1	3	4
19	2	5	5	5	4	3	2	4	3	4	4	3	3	2	5	4	5	3	2	4	3	4	5	4	4	4	1	1	3	3	4
20	2	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	1	1	2	3	5
21	2	4	4	5	4	4	3	4	1	4	4	3	5	4	3	3	3	5	5	5	4	5	4	4	3	3	1	1	3	3	4
22	5	5	5	5	5	4	5	4	3	5	5	5	5	5	4	5	5	4	5	5	5	3	5	5	5	4	1	1	1	3	5
23	4	5	4	5	4	4	5	4	4	4	3	4	4	5	3	4	4	4	3	4	4	5	5	4	4	5	1	1	2	3	4
24	1	5	4	5	1	4	4	2	2	2	3	4	3	3	2	2	4	2	4	4	2	1	2	3	3	3	1	1	3	3	3
25	4	5	5	5	4	5	5	3	3	4	4	3	5	4	5	3	5	2	4	5	4	3	5	5	5	3	1	1	3	3	4
26	3	5	5	2	3	4	3	1	4	2	4	2	1	1	4	1	4	4	2	3	3	4	3	4	2	2	2	3	2	1	3
27	2	5	5	5	4	5	4	3	2	5	4	2	5	4	1	1	5	1	1	1	4	4	2	2	1	5	1	2	3	3	3
28	5	5	5	5	5	4	5	5	2	5	5	4	3	4	4	5	4	3	4	4	5	3	5	4	5	4	1	1	3	3	5
29	5	5	5	5	5	5	4	4	3	4	4	4	3	4	3	4	3	4	4	3	3	4	3	3	4	4	1	1	3	3	4
30	2	5	5	5	4	5	3	4	4	4	4	4	5	4	5	4	5	5	4	4	4	3	4	5	4	5	1	2	2	3	5
31	3	5	5	5	4	4	5	4	5	5	3	3	4	3	3	5	5	5	4	5	4	3	4	5	4	5	1	4	2	3	5

Table 65: Data Set UK

Q 0	Q 1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7	Q 8	Q 9	Q 10	Q 11	Q 12	Q 13	Q 14	Q 15	Q 16	Q 17	Q 18	Q 19	Q 20	Q 21	Q 22	Q 23	Q 24	Q 25	Q 26	Q 27	Q 28	Q 29	Q 30	Q F
1	3	5	5	5	2	5	2	4	5	5	4	2	4	5	2	4	5	3	3	4	2	5	5	4	5	4	1	1	1	1	4
2	2	5	5	5	5	5	5	5	5	5	3	3	4	3	3	3	4	4	2	3	3	3	3	3	3	3	1	1	3	2	4
3	5	5	5	5	5	5	1	5	4	5	5	5	5	5	4	5	5	3	4	5	4	5	1	5	5	5	1	1	4	3	5
4	3	5	5	5	2	5	2	5	4	5	5	3	5	4	2	4	5	3	2	4	5	5	5	2	2	4	2	1	4	2	4
5	2	1	4	5	2	4	2	2	3	5	2	2	4	2	2	2	4	2	2	2	2	4	2	2	2	2	2	1	3	2	2
6	4	4	3	2	1	3	2	4	3	3	4	2	5	5	1	3	4	2	4	4	3	3	4	4	5	3	2	1	3	2	3
7	3	5	5	5	5	5	1	5	5	5	5	4	5	5	5	3	5	3	3	3	5	5	5	5	5	5	1	1	3	2	5
8	3	4	5	5	3	5	4	5	5	4	4	4	5	5	4	4	5	4	4	4	3	5	3	3	4	3	1	1	3	2	4
9	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	3	4	4	4	1	1	1	1	4
10	3	5	5	5	5	5	4	3	1	5	1	3	5	4	1	4	5	4	4	5	4	4	1	3	3	3	1	1	3	3	4
11	2	5	4	5	2	4	3	4	3	4	4	4	5	4	3	4	4	4	4	5	4	5	5	5	4	5	2	1	3	1	4
12	2	5	4	4	2	4	2	4	4	4	2	2	4	4	3	4	4	4	2	4	4	4	2	4	4	4	1	1	1	2	4
13	2	5	5	5	1	4	2	4	4	4	2	2	4	3	1	3	5	1	1	4	3	3	3	3	4	4	1	1	3	3	3
14	2	1	1	1	2	5	2	5	5	4	3	2	5	4	1	2	5	3	2	1	4	5	3	4	2	3	2	1	4	3	3
15	2	4	4	4	2	4	2	4	3	4	2	2	4	2	2	2	4	2	2	2	4	4	2	3	4	4	1	1	1	2	3
16	2	5	3	1	3	5	1	4	4	4	3	3	5	2	1	3	5	5	1	4	3	5	3	3	4	4	1	1	1	2	3
17	4	4	5	5	4	4	4	4	5	4	5	4	5	3	3	4	5	3	4	5	3	5	3	5	5	4	1	1	1	1	4
18	2	5	4	5	3	4	3	4	3	4	4	4	5	4	3	4	4	4	4	5	4	5	5	5	4	5	1	1	3	1	4
19	2	4	4	5	3	4	2	4	4	4	2	2	4	2	2	4	4	2	2	2	4	4	2	2	4	2	1	1	3	1	3
20	3	5	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	5	2	1	3	2	3
21	2	5	4	4	2	4	2	4	4	4	2	2	4	4	3	4	4	4	2	4	4	4	2	4	4	4	2	1	1	2	4
22	2	4	4	3	2	5	4	5	5	4	4	4	5	5	4	4	5	4	4	4	3	5	3	3	4	3	2	1	3	2	4
23	3	5	5	5	3	4	1	4	5	5	2	2	4	3	1	4	5	1	1	4	4	4	3	1	4	4	1	1	3	1	3
24	3	3	4	5	2	4	2	3	2	4	3	2	4	2	2	3	4	2	2	3	2	2	2	2	2	2	1	1	3	3	3
25	2	3	5	4	3	3	4	3	2	3	3	3	4	3	2	2	3	2	2	4	2	4	3	3	4	2	1	1	3	2	3
26	4	5	5	5	4	5	4	5	5	5	4	3	4	4	3	5	4	4	3	4	4	5	5	5	5	4	1	1	1	1	5
27	3	5	4	4	3	5	4	4	3	5	2	3	5	4	5	5	5	4	3	4	4	5	5	4	4	3	2	1	3	3	4
28	2	5	4	5	2	4	3	4	3	4	4	4	5	4	3	4	4	4	4	5	4	5	5	5	4	5	2	1	3	1	4
29	3	4	4	5	2	4	2	4	4	4	3	3	3	3	3	3	4	2	2	2	4	4	2	2	4	2	2	1	3	1	3
30	3	4	4	3	2	4	2	4	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	5	1	1	3	2	3
31	2	5	4	4	2	4	2	4	4	4	2	2	4	4	3	4	4	4	2	4	4	4	2	4	4	4	1	1	1	2	4

Table 66: Data Set USA

Q 0	Q 1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7	Q 8	Q 9	Q 10	Q 11	Q 12	Q 13	Q 14	Q 15	Q 16	Q 17	Q 18	Q 19	Q 20	Q 21	Q 22	Q 23	Q 24	Q 25	Q 26	Q 27	Q 28	Q 29	Q 30	Q F
1	3	5	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3	3	2	1	1	3	2	4
2	5	5	5	5	3	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	1	1	3	2	5
3	1	4	5	4	5	5	5	5	4	5	5	3	5	2	1	1	4	4	5	5	3	1	5	3	5	4	2	4	3	2	4
4	2	5	4	4	1	5	2	4	1	1	1	1	4	2	1	1	4	1	1	1	1	1	5	1	4	1	1	2	4	3	2
5	4	5	4	5	5	5	5	4	4	5	5	5	5	5	4	5	5	4	4	5	4	5	5	4	4	5	1	1	4	2	5
6	2	4	5	3	3	2	1	2	1	3	3	3	3	3	2	3	4	3	2	2	3	4	1	2	3	2	1	2	3	3	3
7	4	5	5	5	3	5	3	4	5	5	5	3	5	4	3	5	5	3	2	5	3	5	4	4	4	3	2	1	3	2	4
8	2	3	3	5	3	3	3	4	3	2	4	3	3	1	1	3	3	3	2	3	3	3	3	3	2	2	2	1	3	2	3
9	2	5	5	5	5	5	2	3	2	5	5	5	5	5	5	5	5	5	3	5	5	5	5	5	5	5	1	1	3	2	5
10	1	4	4	5	3	4	2	3	3	3	2	3	3	3	1	3	4	2	3	3	3	3	2	2	2	3	1	1	3	2	3
11	1	5	5	5	2	5	5	4	4	5	1	1	4	4	3	3	3	5	1	5	4	5	3	1	4	3	1	1	3	2	4
12	4	5	4	4	1	5	1	4	3	4	2	2	4	2	1	2	4	1	2	4	4	4	4	3	3	2	2	1	3	1	3
13	3	2	4	5	2	4	4	4	4	4	2	2	3	4	2	3	5	3	2	4	3	2	2	2	2	3	2	1	3	2	3
14	1	4	4	4	2	4	2	3	3	5	1	1	3	2	1	3	4	2	1	2	4	5	5	3	2	3	2	1	3	2	3
15	4	1	1	1	1	4	2	3	3	2	2	2	2	2	2	2	4	2	2	2	4	2	2	3	2	3	1	1	3	2	2
16	4	5	5	5	5	5	2	5	5	5	4	3	5	4	5	5	5	3	3	5	5	5	5	5	5	5	2	1	3	2	5
17	2	5	4	4	2	4	5	4	5	5	2	1	4	3	2	3	5	4	2	4	2	4	2	4	4	4	2	3	4	3	4
18	4	5	5	5	2	5	1	5	5	5	3	3	5	1	1	3	5	5	3	5	4	5	5	4	4	5	2	1	3	2	4
19	3	2	4	5	2	4	4	4	4	4	2	2	3	4	2	3	5	3	2	4	3	2	2	2	2	3	2	1	3	2	3
20	4	5	4	5	5	5	5	4	4	5	5	5	5	5	4	5	5	4	4	5	4	5	5	4	4	5	1	1	4	2	5
21	1	5	5	5	2	5	5	4	4	5	1	1	4	4	3	3	3	5	1	5	4	5	3	1	4	3	1	1	3	2	4
22	4	3	5	5	5	4	5	4	3	5	1	4	4	3	3	4	4	4	3	4	3	3	3	4	4	2	2	1	3	3	4
23	1	5	5	5	3	4	5	5	3	5	4	4	5	4	3	4	5	2	5	4	3	4	3	3	4	4	1	2	2	3	4
24	4	5	4	5	4	5	2	5	3	5	4	5	5	5	4	4	4	2	2	2	2	2	2	3	4	4	1	2	2	3	4
25	3	5	5	5	4	5	5	4	5	5	5	4	5	4	3	2	5	1	3	5	5	4	2	3	5	5	1	1	3	3	4
26	3	5	5	4	3	4	5	4	3	5	4	4	4	3	2	2	4	2	3	2	3	4	4	4	4	4	2	1	3	3	4
27	1	5	5	2	5	3	4	3	1	3	5	4	3	4	3	3	4	5	3	4	4	5	3	5	4	2	1	1	4	3	4
28	1	4	5	4	3	4	5	3	4	4	4	4	4	4	3	2	4	2	1	5	3	2	2	5	4	4	1	4	2	3	4
29	1	5	5	5	3	4	5	5	3	5	4	4	5	4	3	4	5	2	5	4	3	4	3	3	4	4	2	2	2	3	4
30	4	3	5	5	5	4	5	4	3	5	1	4	4	3	3	4	4	4	3	4	3	3	3	4	4	2	2	1	3	3	4
31	3	5	4	4	4	4	4	3	2	4	5	4	3	4	3	3	4	2	4	2	3	5	4	2	4	4	2	1	3	3	4

Table 67: Data Set Germany