11-2017

A Framework for the Evaluation of Cybersecurity Effectiveness of Abu Dhabi Government Entities

Abdulla Rashed Ali Mohamed Alnuaimi

UAEU

جامعة الإمارات العربية المتحدة
United Arab Emirates University

United Arab Emirates University

College of Business and Economics

A FRAMEWORK FOR THE EVALUATION OF CYBERSECURITY EFFECTIVENESS OF ABU DHABI GOVERNMENT ENTITIES

Abdulla Rashed Ali Mohamed Alnuaimi

This dissertation is submitted in partial fulfilment of the requirements for the degree of Doctorate of Business Administration

Under the Supervision of Dr. James Thomas

November 2017

Declaration of Original Work

I, Abdulla Rashed Ali Mohamed Alnuaimi, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this dissertation entitled *"A Framework for the Evaluation of Cybersecurity Effectiveness of Abu Dhabi Government Entities"*, hereby, solemnly declare that this dissertation is my own original research work that has been done and prepared by me under the supervision of Dr. James Thomas, in the College of Business and Economics at UAEU. This work has not been previously presented or published, or formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my dissertation have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this dissertation.

Student's Signature: _____ Date: 23/11/2017

Advisory Committee

1) Advisor (Committee Chair): James Thomas

   Title: Associate Professor Department of Business Administration

   College of Business and Economics, UAE University

2) Member: Abderrahmane Lakas

   Title: Associate Professor, Department of Computer and Network Engineering

   College of Information Technology, UAE University

Approval of the Doctorate Dissertation

This Doctorate Dissertation is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): James Kunnanatt
   Title: Associate Professor
   Department of Business Administration
   College of Business and Economics
   Signature _____ Date 23/11/2017

2) Member: Maqsood Sandhu
   Title: Associate Professor
   Department of Business Administration
   College of Business and Economics
   Signature _____ Date 23/11/2017

1) Member: Ezedin Barka
   Title: Associate Professor
   Associate Professor of Information Systems and Security
   College of Information Technology
   Signature _____ Date 23/11/2017

4) Member: Nelson Ndubisi
   Title: Professor
   College of Industrial Management
   Institution: King Fahd University (KSA)
   Signature _____ Date 23/11/2017

This Doctorate Dissertation is accepted by:

Acting Dean of the College of Business and Economics: Professor Mohamed Madi

Signature _____ Date 15/12/2017

for Dean of the College of Graduate Studies: Professor Nagi T. Wakim

Signature _____ Date 7/1/2018

Copy 5 of 9

Abstract

Cyberspace has become one of the new frontiers for countries to demonstrate their power to survive in the digitized world. The UAE has become a major target for cyber conflicts due to the rapid increase in economic activity and technology. Further, the widespread use of internet in the region to the tune of 88% by the end of 2014 has exposed the critical infrastructure to all forms of cyber threats.

In this dissertation, the researcher presents a detailed study of the existing cybersecurity defences globally and an investigation into the factors that influence effectiveness of cybersecurity defences in Abu Dhabi government entities. Further, the role of cybersecurity education, training and awareness in enhancing effectiveness of cybersecurity and the role of senior management in providing strategic direction to government entities on cybersecurity are evaluated in addition to determining the contribution of strategic planning and technology level in ensuring an effective cybersecurity system.

The study has evaluated the level of Cybersecurity Effectiveness (CSE) in Abu Dhabi Government Entities and the results show that Science and Technology entity performed better than all other Entities with CSE Mean = 4.37 while Public Order showed the least performance with CSE Mean = 3.83 and the combined model of six factors with R-square value 0.317 after multiple regression implying that 32% change in CSE in the government entities is occurring due to the six (6) independent variables used in the study. Further, results show that management has the responsibility of putting in place strategies, frameworks and policies that respond appropriately to the prevention, detection and mitigation of cyberattacks. Results

further indicate that culture sensitive training and awareness programmes add to the quality and effectiveness of cybersecurity systems in government entities.

Further, study findings reveal that qualified and experienced personnel in government entities show greater understanding of cyber and information security issues. Finally, the researcher proposes a cybersecurity framework and a checklist, with checkpoints, for evaluating the effectiveness of cybersecurity systems within government entities and future research interventions.

Keywords: Cyberspace, cybersecurity system, cybersecurity checklist, cybersecurity effectiveness (CSE).

Title and Abstract (in Arabic)

إطار لتقييم مدى فعالية الأمن الإلكتروني في الجهات الحكومية بإمارة أبوظبي

الملخص

أصبح الفضاء الإلكتروني واحداً من المجالات الجديدة التي تستغلها الدول لإظهار قوتها وقدرتها على البقاء في العالم الرقمي، وقد أصبحت دولة الإمارات العربية المتحدة هدفاً رئيسياً للصراعات الإلكترونية بسبب الارتفاع السريع في النشاط الاقتصادي والتكنولوجي فيها، إضافة إلى هذا، ساهم الاستخدام الواسع للإنترنت في المنطقة، والذي وصل إلى 88% بحسب إحصائيات عام 2014، في تعريض البنية التحتية الحيوية إلى كافة أشكال التهديدات الإلكترونية.

في هذه الأطروحة يقدم الباحث دراسة مفصلة حول دفاعات الأمن الإلكتروني الموجودة حالياً حول العالم ويحقق في العوامل التي تؤثر على فاعلية دفاعات الأمن الإلكتروني لدى الجهات الحكومية في أبو ظبي. إضافة إلى هذا، يعمل الباحث في هذه الدراسة على تقييم دور جهود التثقيف، والتدريب، والتوعية في مجال الأمن الإلكتروني في تعزيز فاعلية الأمن الإلكتروني وكذلك دور الإدارة العليا في توفير توجيه استراتيجي للجهات الحكومية حول موضوع الأمن الإلكتروني، إلى جانب تحديد مساهمة التخطيط الاستراتيجي ومستوى التكنولوجيا في ضمان كفاءة وفاعلية نظام الأمن الإلكتروني.

قامت الدراسة بتقييم مستوى فاعلية الأمن الإلكتروني لدى الجهات الحكومية في أبو ظبي وأظهرت النتائج أن الجهات العلمية والتكنولوجية قدمت أداءً أفضل من كافة الجهات الأخرى بمتوسط فاعلية أمن إلكتروني مقداره 4.37، في حين حقق قطاع النظام العام أقل بمتوسط فاعلية أمن إلكتروني مقداره 3.83 بالإضافة إلى النموذج المكون من ستة عوامل بمعامل تحديد 0.317 بعد انحدار متعدد أشار إلى أن ما نسبته 32% من التغيير في فاعلية الأمن الإلكتروني لدى الجهات الحكومية ناتج عن المتغيرات المستقلة الستة (6) المستخدمة في الدراسة. إلى جانب ذلك، تظهر النتائج أن الإدارة تتحمل مسؤولية تنفيذ استراتيجيات، وأطر عمل، وسياسات تستجيب بشكل مناسب لعمليات الوقاية من الهجمات الإلكترونية وكشفها

والتخفيف من آثارها. كما تُشير النتائج إلى أن برامج التدريب والتوعية القائمة على الثقافة تساهم في تعزيز جودة وفاعلية أنظمة الأمن الإلكتروني لدى الجهات الحكومية.

كما تُظهر نتائج الدراسة أن الموظفين المؤهلين ذوي الخبرة العاملين لدى الجهات الحكومية لديهم قدرة أكبر على فهم مشاكل وقضايا أمن الإنترنت والمعلومات مقارنة بغيرهم. وفي نهاية الدراسة يقدم الباحث إطار عمل وقائمة تحقق خاصة بموضوع الأمن الإلكتروني بهدف تقييم فاعلية أنظمة الأمن الإلكتروني لدى الجهات الحكومية والجهود البحثية المستقبلية.

مفاهيم البحث الرئيسية: الأمن الالكتروني، نظام الأمن الإلكتروني، قائمة التحقق الخاصة بالأمن الإلكتروني، فاعلية الأمن الإلكتروني، الإدارة الاستراتيجية.

Acknowledgements

First and foremost, I would like to express my profound appreciation to my DBA supervisors, Dr. James Thomas the advisor and Dr. Abderrahmane Lakas the co advisor as well as the entire DBA staff at the UAEU, for their continuous guidance, inspiration and patience, and for having given me the opportunity to conduct this research on cybersecurity. Without their advice and support I am sure I would not have been able to come to this point in my dissertation. In addition, I would like to thank my colleagues in the DBA programme for their friendship, help and useful discussions, to my professional colleagues in the cyber and information security practice for their endless encouragement and support over the entire research period. We pray that Almighty Allah rewards you abundantly.

Dedication

First and foremost, I dedicate this manuscript to my beloved wife, Hanan, and children, Khalid, Reem, Khalifa and Fatima, for their diligent contributions, second to my late father, my mother, my sisters and my brothers, for their positive encouragement, third to all my professional colleagues, the "Big Data Group", and the "Power Team", for the efforts they put into cyber, physical and information security in the UAE. Finally to HRH. Sheikh Khalifa, the President of the UAE and Ruler of Abu Dhabi and all other UAE Rulers for upholding the vision of this country

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ADSIC	Abu-Dhabi System and Information Centre
ATM	Asynchronous Transfer Mode
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSPP	Cybersecurity Policies and Procedures
CSSP	Cybersecurity Strategic Plans
ENEC	Emirates Nuclear Energy Corporation
ENISA	European Network and Information Security Agency
EU	European Union
FBI	Federal Bureau of Investigations
G2C	Government-To-Citizen
GCA	Global Cybersecurity Agenda
GCC	Gulf Cooperation Council
HR	Human Resources
ICT	Information and Communication Technology
IoT	internet of Things
ISMS	Information Security Management System
ISO	Information Security Officer
ITU	International Telecommunication Union
MENA	Middle East and North Africa
PII	Personal Identity Information

PIN	Personal Identification Number
PWC	Price Waterhouse Coopers
QECSP	Qualifications and Experience of Cybersecurity Professionals
RFID	Radio Frequency Identification
ROI	Return on Investment
SEM	Structural Equation Modelling
SME	Small and Medium Enterprises
SPSS	Statistical Package for Social Scientists
SWOT	Strength Weaknesses Opportunities and Threats
TAP	Training and Awareness Programmes
TNA	Training Needs Assessment
ToT	Training of Trainers
TRA	Telecommunications Regulatory Authority
UAE	United Arab Emirates
USA	United States of America
VEDP	Virginia Economic Development Agenda

Chapter 1: Introduction

1.1 Overview

This chapter provides an insight into the study concerning the identification of factors that influence or affect cybersecurity effectiveness in Abu Dhabi government entities. After an initial review of the literature, it is revealed that lack of cybersecurity effectiveness presents a management problem that needs critical attention (Kritzinger and Von Solms, 2010; Al Bawaba, 2012; and Rotvold, 2008). This critical literature review together with the researcher's professional experience in the practice of cyber and information security in the region made it possible to identify several management problems and the research gaps that justify the research topic, which would allow further analysis and the identification of key strategies to close these gaps. In this chapter, the research problem is illustrated followed by lists of the study objectives and underlying research questions. The remaining part of the chapter contains a brief discussion of the research variables, presentation of the research hypotheses, an estimate of the study's significance, overview of the research limitations and delimitations, presentation of terms of interest and finally a discussion of the outline of the dissertation. The outline of this chapter is indicated in the Figure 1 below.

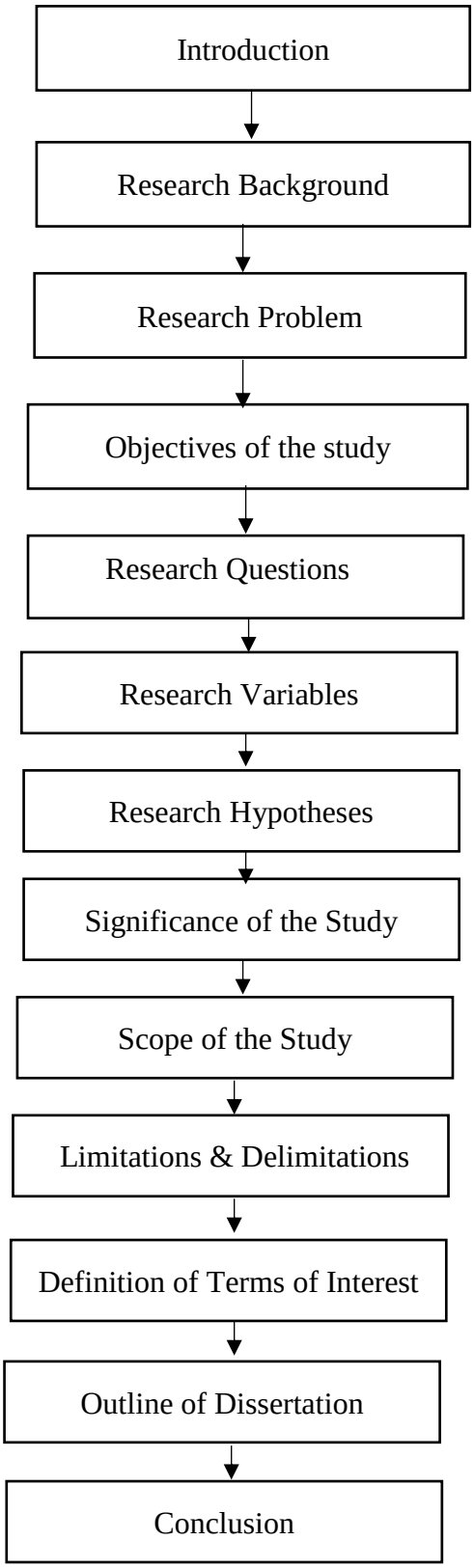


Figure 1: Design of Chapter One

1.2 Research Background

The Middle East and the whole world have witnessed an increase in cyberattacks on critical infrastructure, especially on such financial and energy sectors as banks and major oil firms (Saeed et al., 2014). These attacks have targeted major national security symbols, for instance, military and law enforcement departments. Preventing such attacks is a management issue that requires critical government attention and senior management support requiring high levels of understanding and knowledge. Furthermore, cybercrime has been cited as an escalating threat to the economies of the Gulf Cooperation Council (GCC) countries and their plans for digital transformation as well as the creation of smart cities. Therefore, failure to tackle the issue would impede the strategic development of the region if adequate policies are not formed and legal frameworks across member states are not more fully developed (Hakmer, 2017).

The latest emerging trends reveal that by the year 2020 over 25 billion devices will be connected globally and this Internet of Things (IoT) block chain will bring out the security challenges and cyber risks inherent in these technologies (KPMG Report, 2017). In spite of this, the report reveals that globally the numbers of skilled cybersecurity professionals are meagre to overcome these threats. Additionally, the Emirate of Dubai is working steadily towards achieving smart city status by the year 2020, which requires engagement in smart policies and frameworks for cyber defence such as tabling cybersecurity as a key stakeholder smart defence policy for the UAE through the creation of enough knowledge to assess cyberattacks (Efthymiopoulos and Christopher, 2014). This seems an additional justification for the present study.

Moreover, many global industrial cyberattacks have successfully defeated technological security solutions through preying on human weaknesses in knowledge and skills, and the manipulation of insiders within organizations into unsuspectingly delivering entry and access to critical organizational assets (Uchenna et al., 2016). This ever-expanding knowledge gap on cyber and information security issues among organizational managers and employees in different organizations justifies a study that will explore strategies for cybersecurity training, awareness and education in Abu Dhabi government entities.

Since cyber-criminal activities can be initiated anywhere in the world to target organizations within the UAE and neighbouring GCC states, it is difficult to control the number or sophistication of such attempts. However, senior management has the responsibility of putting in place strategies and structures in response to these attacks. In addition, the UAE is expected to double its cybersecurity budget to $10 billion within the next decade to bolster cybersecurity defences.

While this study is limited in scope to Abu Dhabi government entities, the results may easily be applicable to private sector organizations as well. As the cybersecurity effectiveness of government agencies is critical to the maintenance of services to the public, the researcher intends through this study to propose framework that can be used by management not only to evaluate how effective current measures are but also to prevent attacks that emanate from the internet. This framework was developed after a thorough review of the current literature that identified several variables. These include the competence of information security staff, effective user training programmes; effective user awareness programmes; presence of cybersecurity strategic plans and the type of technology deployed.

1.3 Research Problem

Over recent years, cyberattacks and threats have become a major problem facing a number of countries. The UAE in particular has become a major target for cyberattacks, due to the rapid increase in its economic activity, technological advances and the rise of the oil, gas and energy sectors (Andrew and Gotz, 2013). Furthermore, the extensive use of the internet in the region to the tune of 88% of the population by the end of 2014 has exposed the critical national assets vulnerable and left the prevailing cybersecurity defences and critical government infrastructure at the mercy of sophisticated cyberattacks. To mention a few of them, the destinations of such attacks include Saudi Arabia and Qatar in 2012 and 2013 respectively and the Iranian Green revolution in 2009 (Saeed et al., 2014; Cressey and Hayfer, 2012).

In order for residents and citizens to access e-government services, the UAE government has required each person to own an Emirates Identity card comprising an electronic chip embedded with key information about him/her (Al-Khouri et al., 2011; Al-Khouri, 2012). This card is necessary to access important services across the country. While it has been designed to ensure the confidentiality, integrity and availability of information for the user, it cannot guarantee that the existing cybersecurity defences will not be compromised by any attacker's tactics. A number of strategies have been devised to resolve cybersecurity issues globally. For instance, the National Institute of Standards and Technology (NIST) presented a cybersecurity framework for critical infrastructure in February, 2014, after the declaration of President Barack Obama's Executive Order 13636 of 2013, to formulate a framework that would harmonize consensus and standard industry best practices to provide a flexible and cost effective approach to enhancing cybersecurity

(Shackelford et al., 2014 and Shen, 2014).

The NIST framework proposes technological functions to resolve cyber threats through identification, protection, detection, response and recovery from cyberattacks. Despite these technological precautions, intruders may break into existing security systems by concentrating on their weakest link, the uninformed users who lack the basic cybersecurity training and awareness programmes that would equip them for newer forms of attack. Meanwhile, NESA issued new cyber-crime legislation for the UAE in 2012, with a major focus on defending against military attacks and critical infrastructure. However, it is uncertain how many government entities across the world have incorporated similar laws in their strategic planning processes, policies and operations. Therefore, a study to identify the factors that influence or affect the cybersecurity effectiveness of Abu Dhabi's government entities can be justified.

1.4 Objectives of the Study

The overall objective of the study is to identify the factors that influence or affect the cybersecurity effectiveness of Abu Dhabi's government entities and to propose a framework and a checklist that can be used to evaluate the effectiveness of their existing cybersecurity defences.

1.4.1 Specific Objectives

To achieve the overall goal of the study and to enable the researcher to address individual areas of concern, the research is specifically intended to investigate and determine:

i. The factors that contribute to the cybersecurity effectiveness of Abu

Dhabi government entities.

ii. The role of management in the prevention of cyberattacks in Abu Dhabi government entities.

iii. The role of training and awareness in the prevention of cyberattacks in Abu Dhabi government entities;

iv. The role of the technology level in the prevention of cyberattacks in Abu Dhabi government entities.

1.5 Research Questions

This section discusses the research questions and hypotheses that form the foundation for this study.

1.5.1 Research Questions

Since the Abu Dhabi government continues to invest and depend on e-government services, several questions can be raised. In this research, the researcher raises and investigates the following questions, as the basis for this study:

i. How effective are the existing cybersecurity defenses in stopping cyberattacks and response to breaches?

ii. To what extent does senior management support the establishment and implementation of cybersecurity defense strategies?

iii. Are the existing information security professionals in government entities well qualified and experienced to detect and stop cyberattacks?

iv. How effective are the implemented staff training programs in various departments?

v. Does cybersecurity strategic planning contribute to organizational cybersecurity effectiveness?

vi. How effective are the existing user awareness programmes in various departments?

1.5.2 Research Variables

In order to conduct this study, several variables have been identified as necessary for developing a robust framework for cybersecurity effectiveness. Cybersecurity effectiveness in an organization is made up of all the technologies, processes, procedures, policies, strategies and personnel that work together with the sole purpose of preventing cyberattacks from doing damage and responding to any threats against its information systems. Cybersecurity effectiveness is considered the dependent variable in this study. In order for the cybersecurity of any organization to become effective, the study theorizes that the conditions forming the independent variable are met as discussed below.

First, there has to be evidence of senior management support. Evidence of senior management support includes the presence of a senior officer at the rank of Chief Information Officer (CIO) or Chief Information Security Officer (CISO) with well-defined authority on information security matters in the organization and the presence of cybersecurity strategic plans for the entire organization or department. Further, this person must have demonstrated an understanding of cybersecurity matters in the organization through the deployment of well-qualified information security teams, supplemented by on-going continued-education programmes; implementation of effective policies and procedures; training and awareness programmes and deployment of appropriate technologies for all users; and adoption

by the organization of international best practices, (Kritzinger and Von Solms, 2010; Al Bawaba, 2012; Nigel and Rice, 2011).

Operationally, *senior management support* can be demonstrated in several ways. In a government department that takes cybersecurity seriously, the day-to-day operations of issues related to cybersecurity are governed by clear and well-articulated policies and procedures. These policies and procedures govern the behaviour of those who use the organization's information systems. The policies developed and implemented may range from those relating to email, internet use, password strength, mobile computing devices, to such issues as access, the distribution and destruction of documents, visitor management, etc. Employee awareness of these policies and procedures is a strong indication that the organization has an effective cybersecurity programme, (Knapp, 2009; Herath and Rao, 2009; Kritzinger and Smith, 2008; Rotvold, 2008; and Frank et al., 2008)

Second, further evidence that cybersecurity matters are taken seriously by the organization can be shown by the presence of cybersecurity strategic plans. Well thought out strategic plans are distributed and properly diffused throughout the organization and can be described by the senior staff who are responsible for matters of information security. These plans act as guides for the development of policies and procedures, training and awareness programmes, (Elbanna, 2010; Grant, 2003; Dutton and Duncan, 1987; and Andrew, 2014).

The third independent variable is the presence in the organization of competent information security staff. Evidence for this includes the possession of academic and industry certifications in the cybersecurity/information security domain. Moreover, there has to be strong evidence of continuing reminders that cyber-threat is an ever-changing phenomenon. Awareness of trends in the domain,

including a knowledge of the current threats, tools and techniques used by cyber-criminals, vulnerabilities in the organization's infrastructure, and the mitigation strategies used are clear evidence of the seriousness of the agency regarding cybersecurity. Additionally, these personnel should exhibit deep understanding and commitment to cybersecurity policies and procedures, (Rowe et al., 2011 and Cisco, 2017 and Siponen et al., 2014).

Fourth, the organization should conduct effective and culturally sensitive staff training programmes for all its employees; and fifth, it should carry out adequate number of user awareness programmes. Effective training and awareness programmes are comprehensive, measurable and regular. An organization that is serious about cybersecurity needs to put great emphasis on training and awareness programmes conducted by knowledgeable individuals for all users in the organization at set intervals during the year. For these training programmes to be effective, they should be culturally relevant to the audience. Further, measurements and evaluations should be used to determine the effectiveness of the training and the measures taken to improve them, (Greitzer et al., 2007; Pfleeger and Caputo, 2012; McCrohan, 2010; Hight, 2005; Kruger et al., 2011; Siponen, 2000; Da Veiga and Eloff, 2010; and Aloul et al., 2012)

The sixth and final independent variable is the level of technology**.** It is believed that government entities that have invested in modern cybersecurity technologies demonstrate their understanding of cybersecurity risks. There are many kinds of software and hardware technology already deployed by Abu Dhabi's government entities. The most common technologies used globally include different forms of firewall, data encryption, anti-malware, anti-spyware and anti-virus scanners, among others. For these tools to be effective, the human element that

supports and maintains these systems cannot be ignored, since most of these systems have limitations. From these variables, the following hypotheses are derived for testing, (Symantec 2016; Hunter, 2013; Choo, 2011; Aloul, 2010; Knapp, 2009; and Uchenna et al., 2016) among others.

1.6 Significance of the Study

The main purpose of this study is to identify the factors that influence or affect the cybersecurity effectiveness of Abu Dhabi's government entities and propose a framework as well as a checklist that can be used to evaluate the effectiveness of their existing cybersecurity defences. Such a framework and checklist could be standardized further to provide a benchmark or baseline measure of cybersecurity effectiveness in many public and private sector organizations. The researcher investigates the factors that contribute to cybersecurity effectiveness from both the literature and practice to provide a wider context for the subject. These factors are then collated into a framework that could easily be applied by the senior management of such departments to measure their readiness to defend them against attacks and also respond to attacks should they occur. This is important because society, specifically UAE society, continues to depend on government services that are accessible by information systems such as the internet. Any failure of such systems due to cyber-attack will negatively impact government services ranging from the immigration services at airports, visa processing for professionals and the routine issue or renewal of drivers' licenses to the disruption of critical national infrastructure, such as electricity, telecommunications and banking.

1.7 Scope of the Study

In this study, a critical review of the literature regarding cyber and information security mechanisms in the UAE, the GCC countries and globally is conducted. Emphasis has been put on identifying the factors needed to evaluate the effectiveness of cybersecurity defences in Abu Dhabi's government entities with a broad global perspective in mind. The role of senior management in the design and implementation of appropriate cyber and information security strategic plans, policies, training and awareness programmes is looked into. Further checks on the numbers (if any) of competent cyber and information security professionals in Abu Dhabi's government entities are needed, as a first step in mitigating the cybersecurity problem. Additionally, an investigation of the importance of cybersecurity training and awareness programmes in the prevention of cyberattacks has been critically pursued. Finally, a framework and checklist are proposed that could be used to assess the effectiveness of cybersecurity defences for Abu Dhabi's government entities.

1.8 Justifications for the Research

Cyberattacks on critical National Infrastructure have grown in complexity globally over the recent years with a focus on the United Arab Emirates, (Saeed et al., 2014 and Neuneck and Weizmann, 2013) with recent trends showing a 42% increase in global cyberattacks by the end of 2015 (Symantec, 2016). Additionally, global attacks have successfully defeated existing technological solutions by exploiting human weaknesses within organizations due to ever increasing knowledge gaps in Cyber and Information security (Uchenna et al., 2016). Further, the Abu Dhabi Government continues to depend on e-government platforms such the

Emirates ID to enhance service delivery, however, the drawback to such a system could be the attraction of more sophisticated attacks from multiple sources of the world especially from those who may want to exploit the same platform for personal gains and so seriously cripple government services that range from, immigration services at airports, visa processing for experts, routine issuing or renewal of driver's licenses to disruption of critical national infrastructures such as electricity, telecommunications and banking (Shackelford et al., 2014 and Shen, 2014).

Therefore, with the above input from available literature and consultations with subject matter experts in Abu Dhabi government, a study is required to develop a non-technology based framework as well as checklist for evaluating cybersecurity effectiveness of Abu Dhabi's government entities hence justifying the reason for conducting this study.

1.9 Research Limitations and Delimitations

1.9.1 Research Limitations

Limitations are potential weaknesses or constraints in a study out of the researcher's control that could affect the outcome of the study. This study was conducted with the following limitations:

i. Though cybersecurity is a global challenge that affects public and private organizations, this study is limited to Abu Dhabi's government entities with participations from the users, administrators, ICT management and senior management

ii. The study concentrates on the effectiveness of the existing cybersecurity strategies and frameworks employed within these government entities. A census study approach was taken to gather the research findings about these

entities but the study results cannot be generalized to other sectors of the emirate, such the private sector.

iii. Though many studies have been conducted on cybersecurity globally, little has been surveyed in the UAE, especially regarding government entities. This study draws on the few empirical studies that have centred on the Emirate and also on global contributions in the area of cyber and information security to generate the theoretical foundation and hypotheses for the study.

1.9.2 Research Delimitations

This study on cybersecurity effectiveness within the Abu Dhabi's government entities is based on a series of hypotheses grounded on literature, practice and related theory. The implementation of the proposed framework and cybersecurity checklist is not considered to be within the scope of the study. Furthermore, as highlighted by Birtwhistle and his team (2002), survey instruments are distributed with time constraints limiting the possibility of maximum response rates. Moreover, the study was limited to a population of 535 respondents from Abu Dhabi's government entities.

1.10 Definition of terms of interest

In this study, some interesting terms were encountered frequently and are applied in several of its discussions. Some of these terms may be defined as follows:

i. Cybersecurity

Cybersecurity involves the organization and collection of resources, processes and structures used to protect the cyberspace and cyberspace enabled systems from occurrences that are mis-aligned from de facto

property rights (Craigen et al., 2014).

ii. Cyberspace

Cyberspace comprises networks, computer hardware, software and other devices capable of storing and exchanging information across borders (Kritzinger and Smith, 2008; Obama, 2009).

iii. Cyber threat

The possibility of a malicious attempt to damage or disrupt a computer network or system.

iv. Cybersecurity Framework

A platform for measuring or evaluating how well a security system operates. Such frameworks can be used for measuring and or mitigating the risks involved in cyberattacks on a country's critical infrastructure (National Institute of Standards and Technology (NIST) Cybersecurity Report, 2014).

v. Training and Awareness Programmes

This represents formal programmes designed for educating employees of an organization about existing global, national or organizational issues, such as cyber and information security, corporate policies and procedures.

vi. Role of Management

The overall responsibilities of management operate through functions such as planning, organizing, staffing, directing, monitoring and control to address the critical issues pertaining to an organization, for example, cybersecurity issues.

vii. Technology

The application of science and use of practical as well as intellectual

resources to develop systems and products that address organization-wide problems.

viii. Cybersecurity effectiveness

Effective response to global and national cybersecurity challenges.

ix. Experience

Experience in this context refers to the knowledge or maturity of a subject gained through involvement or exposure leading to the acquisition of relevant skills over a period of time.

x. Strategic Planning

Refers to an organization's process of defining its strategy or direction to allow the efficient allocation of resources.

xi. Qualification of users

Denotes the fitness for purpose of users shown by their fulfilment of all the necessary conditions, for example, completion of the required skills-based training or academic level.

xii. Assets

In the context of this study, assets represent any organization's information resources that could be subjected to cyberattacks for example all forms of data, software, hardware, networks and utility programs that require monitoring in terms of Confidentiality, Integrity and Availability.

xiii. Critical Infrastructure

Represents all sectors whose assets are very vital to the UAE's national security. Destruction or attacks on such sectors would pause a devastating effect on national security and economic drawback. Examples of UAE Critical Infrastructure includes the communications sector, the Energy

sector (Oil and Gas sector), International Airports, Transportation systems among others.

1.11 Outline of the Dissertation

This dissertation has been organized into five major chapters arranged as follows. Chapter One introduces the study on cybersecurity globally and in the United Arab Emirates (UAE) in particular. A research problem is defined which is grounded on the fact that the UAE has become a target for many cyberattacks in the region, as a result of the ever increasing numbers of technologies, economic activities and people connected to the internet. The broader goal of the study is to propose a framework and checklist for the evaluation of cybersecurity effectiveness in Abu Dhabi's government entities. Keeping in mind the goal of the study, the following specific and measureable objectives emerge in this chapter: 1) examining the factors contributing to an effective cybersecurity system; and 2) setting research questions and hypotheses. Hypotheses are developed to build a comprehensive theoretical framework and underlie the quantitative analysis of this study. In parallel, the importance of this study is defined and a summary of the entire thesis is offered.

In Chapter Two, the literature from several existing studies, journals, and published conference papers among others concerning the subject matter is reviewed. The researcher examines the cyber threat landscape, defining stages of a typical cyberattack and a cyber-forensic cycle. Moreover, the chapter considers the most recent cyberattacks in the region and globally, such as the Saudi Aramco and Stuxnet worm of 2009 (Cressey and Hayfer, 2012; Pepitone, 2011; and Symantec, 2013) among others, as notable references. Furthermore, the literature on existing global cybersecurity frameworks and strategies are reviewed to provide a strong foundation

for this study, the research design and formulation of the security framework (Burgers et al., 2013; Nambiro et al., 2014; NIST, 2014; and Abraham and Nair, 2015), among others. Additionally, the chapter elaborates the role of strategic planning, technology and cybersecurity legislation in the UAE and the GCC countries (Choo, 2011; Cisco, 2017; Hunter, 2013; Aloul et al., 2012; Elbana, 2010; Grant, 2003, Liedtka, 2000; and Gercke, 2014) are some of the notable references. In addition, the researcher reviews challenges to the effectiveness of cybersecurity defences globally and seek to provide an insight into some of the solutions to address these challenges. Examination of the role of cybersecurity training, awareness and education in the prevention of cyberattacks is assessed in detail and the role of the culture in the understanding of cyber and information security issues pertaining to an organisation is looked into (Siponen, 2000; Kritzinger and Smith, 2008; Rezgui and Marks, 2008; Kalberg and Bhavani, 2012; Vroom and Solms, 2004; and Leach, 2003), among others. Finally, after a critical review of other study contributions, the researcher identifies six study hypotheses to guide further analysis and a research gap that formulates the basis for further investigation and analysis.

Chapter Three presents the methodological approach undertaken to address the research questions and study hypotheses. A detailed discussion of the research strategy, tools and the research design is presented. The chapter further presents various tests conducted to validate and ensure the reliability of the research instrument, which include the presentation of the instrument to subject-matter experts, reliability statistics involving the examination of values of Cronbach's alpha for all the predefined constructs, and principal component factor analysis against the research hypotheses to examine the factor loading scores. In the same chapter, previously existing frameworks such as NIST for assessing cybersecurity

effectiveness are scrutinized (Tin, 2010). This scrutiny as well as the theoretical foundation grounded from literature review contributed to the formation of the proposed framework for the evaluation of cybersecurity effectiveness of the Abu Dhabi's government entities. Finally, the study analysis tool and justification for choosing it is briefly discussed, together with a description of the pilot survey conducted on a midsized organization in Abu Dhabi. In the conclusion of the chapter, study limitations and ethical issues are discussed.

In Chapter Four can be found the data analysis and study results including the method of analysis, reliability and validity checks, demographic statistical results, and correlation results are presented. Finally, Chapter Five discusses the research contributions, presents a checklist for cybersecurity assessment with the aid of key check points to evaluate the effectiveness and readiness of a department's cybersecurity programme and suggests recommendations as well as directions for future research.

1.12 Conclusion

Grounded on the primary review of literature and the researcher's professional experience in the practice for a period of over 17 years, problems were identified concerning cybersecurity effectiveness from a management perspective. Further, the research problem and research gaps were identified for further analysis, the research questions and variables for the study were also presented. In this way, the researcher argued to fill these gaps fulfilled by the present study. The main research contributions were consequently established. A general outline of the research dissertation was added, to provide insight into the research study, analysis

and findings. The next chapter presents a detailed review of literature related to the study.

Chapter 2: Literature Review

2.1 Introduction

In the previous chapter, problems affecting the cybersecurity effectiveness of organizations and factors that seemed to contribute to organizational cybersecurity effectiveness were proposed for this study. In this chapter, the researcher presents the research hypotheses showing the different study relationships examined, further a critical review of literature on the factors for evaluating the cybersecurity effectiveness of Abu Dhabi's government entities is conducted as a basis for the theory behind the research study and to identify gaps for further investigation. Specifically this chapter is divided into seven sections with each successive section narrowing down the ideas to reveal the gaps that exist and the possible ways of filling them. In section one, an overview of the cyber-threat landscape is presented and various terminologies relating to cybersecurity are defined. It considers the view that cybersecurity is a management issue that requires well-defined senior management approaches. The impact of cybercrime on organizational performance is highlighted in this section. Further, the most recent trends and research relating to cybersecurity threats, defences, and training and awareness programmes developed around the world are examined. These provide a wide view of the research problem and hence an insight into the factors that can be proposed for the evaluation of cybersecurity in Abu Dhabi's government entities.

Section two looks at the role of Qualifications and Experience (the competence of staff) in building an effective cybersecurity programme for an organization. Meanwhile, section three examines the role of management in the prevention of cyberattacks while section four discusses the common types of

technology and their role in cyber-crime prevention. In section five the role of staff training of n the prevention of cyberattacks against an organization is presented.

Section six looks at strategic planning and cybersecurity effectiveness. In this section, the use of strategic planning tools in addressing uncertain conditions is emphasized. Section seven discusses the role of cybersecurity user awareness programmes, followed by a discussion of the regulatory issues and various cybersecurity frameworks. The literature review chapter ends with an overview of the existing research gaps for further investigation in this study. The design of this chapter is illustrated in Figure 2 below.

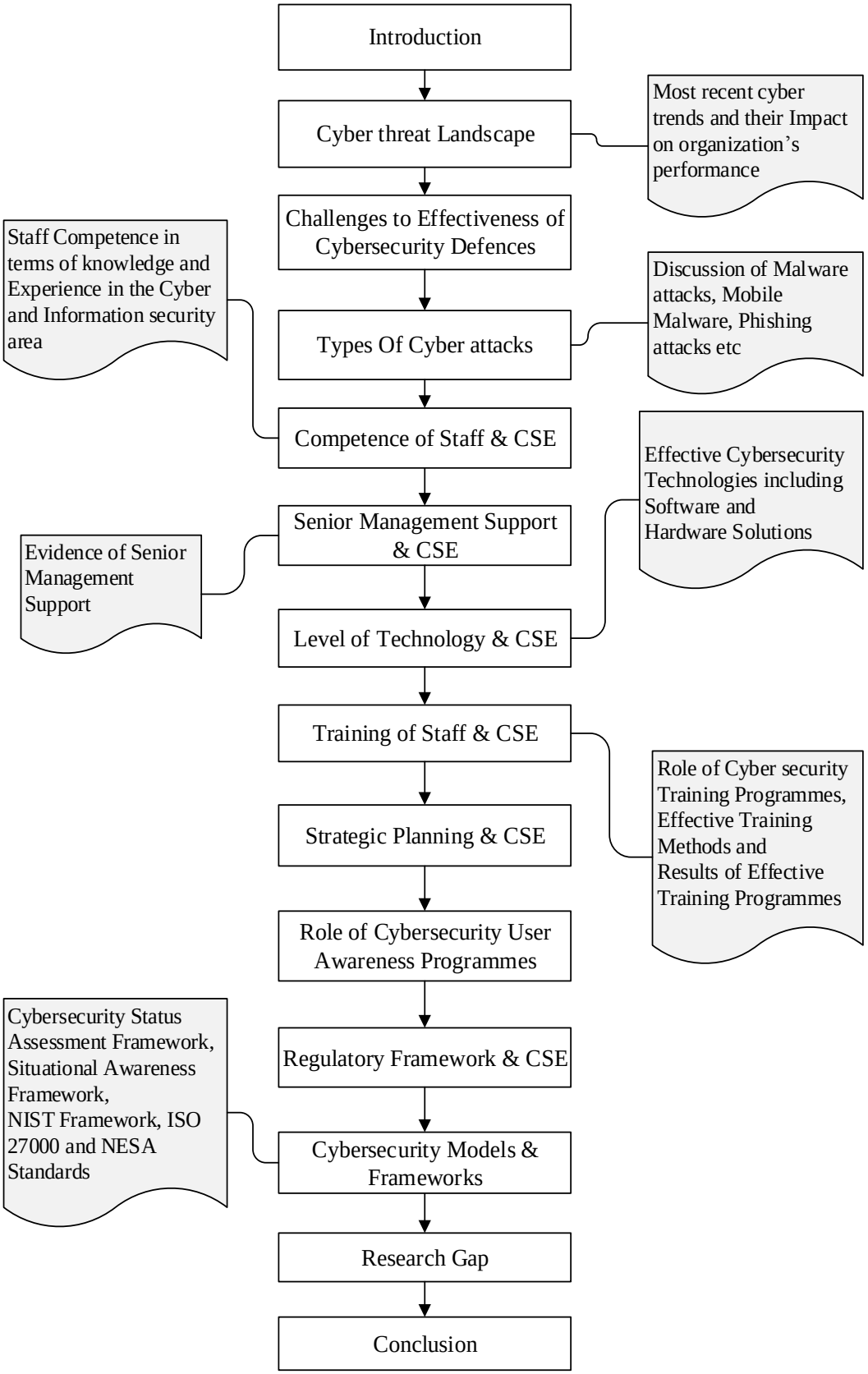


Figure 2: Design of Chapter Two

2.2 The Cyber Threat Landscape

The present information age has brought many advantages to society, from ease of access to services through Internet enabled devices to communication and collaboration over long distances. The UAE Government in particular increasingly depends on the power of the Internet to provide services to the people and to other governments across the globe (Al-Khouri, 2012). Most financial institutions charge extra fees for services provided over the counter, as the expectation is that customers should access the same services easily online. This dependency on the information infrastructure has brought new and dangerous risks (Kritzinger and Von Solms, 2010).

Although the Internet has brought new opportunities to society, it has also brought new opportunities to others whose goals are to exploit inbuilt weaknesses through cyberattacks (Choo, 2011). A cyber-attack can be defined simply as "any crime that employs a computer network in any phase of the crime" (Kshetri, 2005). Senior management's understanding of the cyber threat landscape is critical to government operations as a necessary step in developing corrective and preventive measures. The importance of national cybersecurity strategies was captured in a speech by President Obama in 2009. He remarked:

> "This world cyberspace is a world that we depend on every single day. It is our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives. It is the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It is the classified military and intelligence networks

> that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. So cyberspace is real and so are the risks that come with it. It is the great irony of our information age, the very technologies that empower us to create and to build those who would disrupt and destroy. And this paradox seen and unseen is something that we experience every day", (Obama, 2009).

Numerous attacks, for example, malware, phishing, corrupted programs, password manipulation, computer session hijacking, denial of service among others, have increased greatly in the UAE and the GCC in recent years. Examples of such attacks include the August, 2012 attack that affected ARAMCO, the major oil and gas company in Saudi Arabia, the Stuxnet worm of 2009 which targeted the Programmable Logical Controllers (PLC) of the Iranian nuclear industry, the Lulzec Sony pictures attack that seized the bio data of many people (Cressey and Hayfer, 2012; Pepitone, 2011), the Shamoon Virus that infected over thirty thousand (30,000) stations and destroyed business processes for almost a week, among others. These ever increasing information security vulnerabilities in vital or critical government infrastructure and industrial data can partially be attributed to the large amounts of data moving into data centres, increased numbers of mobile subscribers and massive Internet connectivity in the GCC region amounting to 88% by the end of June 2014.

Furthermore, Cressey and Hayfer (2012) argue that real time threats are more sophisticated and so require continuous monitoring by government and all other stakeholders due to the massive threat to data and proprietary information. Much as governments try to keep pace with these threats, they have not integrated their

security strategies to provide a more complex solution to cyberattacks. These ever-increasing information security threats call for the development of complex cybersecurity defences for Abu Dhabi's government entities, the UAE and the entire GCC region.

Aloul et al. (2012) have looked at the security concerns of the UAE traditional electrical power grid which will soon evolve into a smart Grid system. They analyze the vulnerabilities and debate the current and needed security solutions. Power Grids normally face attacks on intelligent devices and physical connections attacks such as IP spoofing and denial of service attacks. Therefore, if the UAE grid fell under a cyber-attack it would pose great danger and loss to the government and the entire economy. Furthermore, Kwangjo and Kaist (2012) stress that nuclear power plants are very important infrastructure for providing efficient and uninterrupted electricity and so require continuous government vigilance and protection. The use of such digitized systems brings new vulnerabilities and threats over cyber space due to the unbroken dependence on software and networks. Therefore, there is need to develop security frameworks that would provide guidelines or checklists to users of such critical infrastructure in the UAE's government entities.

At the same time Assante and Tobey (2011) provide an insight into educating the cybersecurity workforce by proposing the need to devise ways of producing competent information security professionals who can build, manage and secure reliable digital infrastructures as well as effectively identifying plans for such threats. They present a model for developing the next generation of cyber workers which combines assessments, simulations, customization and support systems. However, their model suitability to Abu Dhabi's government departmental setup may not be

assured, since it was found to be less effective for interconnected networks. There is need to build a framework which can aid the robust UAE interconnected network systems to enable joint detection and control cyber threats; this is the major contribution of this dissertation.

The United Nations Institute for Disarmament Research report (2013), asserts that government efforts to protect critical infrastructure and undertake law enforcement in the cyber sphere are complicated, due to the fact that most of the infrastructure and assets involved are owned and operated by private sector organizations with diverse motivations and competing impartialities to protect. This complicates the entire legislation and law enforcement process. For instance, civil liberties may be mostly concerned about protecting people's rights instead of protecting people's privacy online.

Additionally, attackers have raised their levels of organization and research, especially in the area of cloud security and desktop virtualization which are envisioned to be the hub for the next generation of data storage areas for critical organizational data. The cyber criminals have been much inspired by recent political instabilities, especially in the Arab region, and monetary support from some hacktivist groups. In addition, most recent statistics show a dramatic increase in UAE cybersecurity threats; for instance official statistics from the Dubai police show a dramatic 88% increase in the number of electronic crime cases reported in 2013 as compared to the year before (https://securelist.com/the-rise-of-cybercrime-in-dubai-and-uae/63682/, accessed, 22nd September, 2017). The cyber investigation department of Dubai Police received a total of 1,820 reports in 2015, representing an increase of 15% over the previous year (Symantec, 2016). This trend validates a continued increase in cybercrime within the United Arab Emirates which signifies a

major requirement for cybersecurity research in the region to reduce the existing knowledge gap. The trend in Dubai's cybercriminal cases can be seen in Figure 3 below:

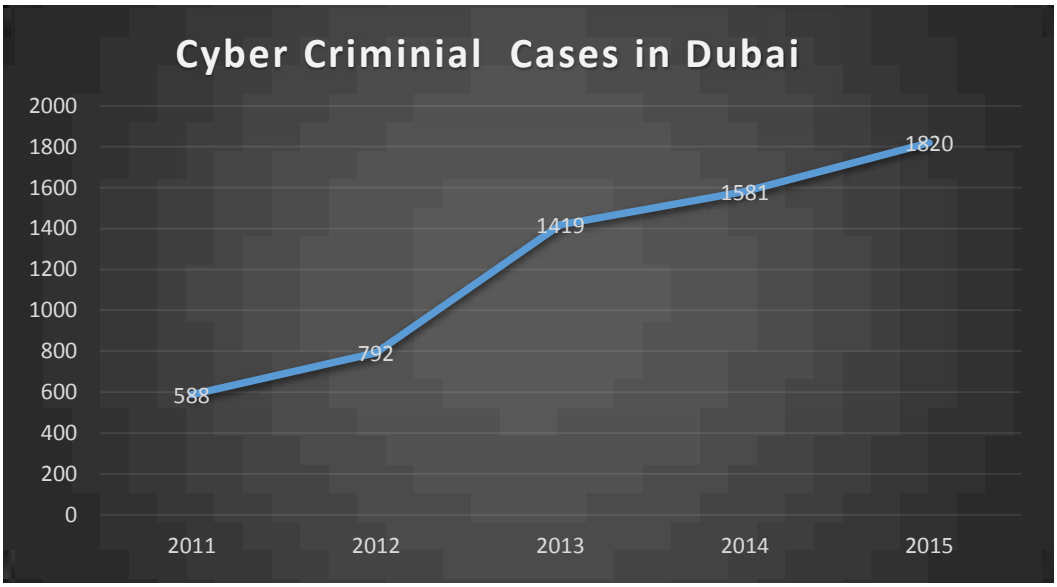


Figure 3: Cyber-criminal Cases in Dubai Source: Symantec, 2016

From Figure 3 above, the number of cybersecurity threats reported by the Dubai police was analysed for a period of five years, from 2011 to 2015. While the data show that cyber-crimes have been on the increase in the UAE, they are not conclusive as the increase could be attributed to other causes such as increase in awareness of the crime, hence more victims reporting it. Still, such data provide the justification for the UAE government and Abu Dhabi's government entities in particular to advance their cybersecurity defences.

The Middle East has been recognized as the most attacked region in the world, especially due to the recent shift in economic growth from southwards to eastwards. For instance, according to Symantec, 1.5 million people or about 17% of the entire population of the UAE were victims of cyber-crime in 2011 and it is

claimed that each of the victims suffered an average loss of $283.00 making an estimated loss of over $400 million (Symantec, 2016).

A still more worrying trend has been identified by information security researchers in the region/ It is suspected that cyber-criminals were able to record magnetic information and PINS from bank ATM machines to create replica cards which were used after to scam customers, leading to exposure of their critical financial information and losses Hunter (2013). It is further revealed that since bank ATM networks are not always connected to the Public Internet, most of the fraudsters uploaded the malware codes through insiders Choo (2010). Therefore, more work needs to be done by the government to install state of the art technologies to cub insider attacks. Further, more work needs to be done especially in training innocent users in the importance of protecting critical organizational assets and personal data from any form of unauthorised access. A number of challenges exist for both space and cyber domains against the existing defensive strategies implemented by organizations; daily threats posed by attackers require senior management in organizations to set the right priorities especially in resource allocation, governance, decision making and the right security culture for all employees. Some of the major challenges to cybersecurity defences are presented in the next section.

2.3 Challenges to the Effectiveness of Cybersecurity Defences

The cybersecurity issue has been critically analysed as a global challenge. While there are multiple ongoing efforts that seek to enhance cybersecurity, an integrated governmental strategy to meet the challenges has only begun and has not been fully implemented. It is envisaged that all strategies demand recognition of risk

and the prioritization of resources. Therefore, governments need to focus on key national security problems and provide solutions for the enhancement of cybersecurity defences.

The International Telecommunications Union report (2012) revealed a number of challenges in the prevention of cybercrime globally. First was organizations' over-reliance on ICTs for the control and management of security functions in buildings, cars, aviation services, water and energy supply, which has made the systems more vulnerable to different forms of cyber-attack. This over-reliance means that a cyber-attack could lead to catastrophic results that might be life threatening. A good example is the recent "Wannacry" attack affecting several London hospitals in May, 2017. The second challenge is the fact that there has been an overwhelming increase in the number of Internet users to the tune of 3 billion users world-wide, representing 50% of the global population (Source: *Internet Live Stats* (www.InternetLiveStats.com)). The large number of the public connected to the Internet poses a huge challenge to the authorities in designing and implementing adequate preventative measures from attacks that emanate literally from anywhere in the world (Aloul et al., 2012; Kwangjo and Kaist, 2012). While there are delays in establishing regulations and effective measures in response to such threats as they emerge, attackers are able to adjust their techniques quickly to combat any technological advancements.

Elbanna (2010) argues that whereas it is cheap to mobilize cyberattacks, technologies for guarding against such crimes have become more and more expensive. Therefore, the war against cybercrime should be jointly handled by all stakeholders in the UAE region with major support from government. Furthermore, the problem can be eliminated by a combination of defensive technologies,

continuous in-depth analysis, traditional diplomacy and culturally sensitive cybersecurity training and awareness programmes. More still, top management in the various government entities, especially the chief executive level (C-Level), need to be very vigilant in the planning stages for their organizations by incorporating cybersecurity in their strategic plans.

It has been revealed that new approaches to cybersecurity have emerged, based on the analysis of data on successful attacks to replace the counter reactive network security methods used in the past. These new approaches encourage continuous monitoring of the health of networks with relatively straightforward mitigation strategies to provide a basis for better cybersecurity. It is further conveyed that most governments have not agreed on the "rules" which can be applied to cyberspace nor how to apply the existing "rules" for espionage, crime and warfare. Most attackers take advantage of the Internet's ability to seamlessly cross borders and so reside in countries that tolerate their activities and therefore sit outside the grasp of national law enforcement (Andrew, 2014).

It should also be noted that improving primary level security may not solve or isolate the cybersecurity problems completely, but merely make them more manageable and ultimately easier to solve. Therefore, the prevention of cyberattacks against critical national infrastructure should be a continuous effort by all stakeholders in government entities. Most organizations that fall prey to attacks are found to possess exploitable weaknesses in their operations and security systems. Lydon (2013) further reveals that 96% of the breaches occurring in the year 2012 could have been avoided if the victims had put in place simple or intermediate controls. 85% of the penetrations took months to be discovered and if discovered were often reported by third parties rather than the victims.

The nature of cyberattacks is comparable to the nature of conventional attacks by the military. Just like conventional wars, such as the recent Iraq and Afghanistan wars, cyberattacks are launched with specific goals in mind. Understanding these goals would help management to know who the enemy in cyberspace is.

Another challenge is the need to understand the motivations and the propagators behind cyberattacks. Kshetri (2005) draws from the psychology and economic literature to identify the motivations for cyberattacks. He splits the attackers into two broad groups: those with intrinsic and extrinsic motivation. The theory of intrinsic motivation assumes that an individual does something because of the enjoyment derived from the activity, and not for the result to be achieved in the end. In cyberspace this could be compared to an individual or group of individuals who enjoy developing malware or viruses for the sake of it. Extrinsic motivation maintains that human behaviour is driven by a goal external to people. Extrinsically motivated individuals are then likely to attack organizations to steal information of financial value, or target banks and even individuals to divert funds to accounts within their jurisdiction.

Most human behaviour is probably some variant of the two motivators. A report by the US-China Economic and Security Review Commission of 2013 identified perpetrators of cyberattacks from China as falling into four categories, namely: Military groups, the Intelligence service, Independent actors such as; 1. “activists”, 2. “for profit hackers”, 3. “purely criminal hackers”; and 4. “Corporate” actors. It is also noteworthy that widely available reports indicate that Russian government backed actors were responsible for hacking attempts to influence the 2016 U.S. Presidential elections (United States Congress, 2017)

Whereas two of the groups, military and intelligence, are state sponsored, the Independent actors may not be directly sponsored by the state but its members are often hired by the state to conduct cyberattacks on its behalf. With the increase of state owned companies in the military-industrial complex and telecommunications industries, cyber-attackers in industry aim at gaining intellectual property from their Western counterparts illegally.

2.4 Types of Cyberattacks

Discussions of the cyber threat landscape in the UAE cannot be accomplished without considering the types of attack launched by cyber-criminals as in Table 1. Understanding various attacks is particularly critical to those trusted as the guardians of data and the infrastructure they use. Furthermore, senior management who head government organizations in Abu Dhabi's government entities should have a high level of understanding of how the various forms of cyberattacks happen and their effect on critical national infrastructure. This would aid the development of appropriate strategic plans, policies and procedures in the departments to protect against cyberattacks and malicious activity. While there are many types of cyber-attack, most of the disastrous activities are species of Malware and Phishing.

Cyberattacks increased by 43% worldwide between 2014 and 2015 according to Symantec (2016). However, while some forms of attack increased, there were noticeable reductions in others. Such changing and extreme changes in the attacks imply that senior management needs to be familiar with the ever changing cyber-landscape to allow effective resource allocation and timely responses. The table below summarises the attack landscape for the period 2014 to 2015 as shown in the Symantec Report of 2016. Meanwhile, a report by McAfee in 2014 indicated that

more than 307 new security threats were generated every minute and that mobile malware samples had grown steadily to about 16 percent during the first quarter of 2013, while overall malware surging grew by 76 percent over the same year (McAfee, 2014). The researchers acknowledged new attempts to attack which take advantage of Internet trust models, e.g. secure socket layer (SSL) susceptibilities such as Heart bleed and the continued abuse of digital signatures to cover malware as legitimate code McAfee Report (2014). Furthermore, the report predicted that in 2015 and beyond malicious parties would seek to extend their ability to avoid detection over long periods, by adopting cyber espionage capabilities for monitoring and collecting valuable data over extended targeted attacks. It added that more aggressive efforts to identify application, operating system and network vulnerabilities were needed, and so was an increasing focus on the limitations of sandboxing technologies as hackers attempt to evade applications and hypervisor-based detection.

Table 1: Symantec Internet Security Threat Report 2016

Attack Type	2014	2015	Trend
Overall Email Virus Rate	1-in-244	1-in 220	Increasing
Overall Email Phishing Rate	1-in-965	1-in-1846	Decreasing
Mobile Malware Families Increase (% Increase over previous year)	32%	214%	Increasing
Crypto-ransomware	269,000	362,000	Increasing
Web Attacks Blocked / Day	493,000	1.1 Million	Increasing
New Mobile Vulnerabilities	168	528	Increasing

From Table 1 above, the results show a considerable decrease in Email Phishing Rates from 1 in 965 in 2014 to 1 in 1846 in 2015. However, attacks increased via mobile malware to the tune of 214% over the year 2014. Results also showed an increase of crypto-ransomware from 269,000 in 2014 to 362,000 in 2015 Symantec (2016). Detailed discussion of the types of malware follows next.

2.4.1 Malware

In recent years, it has become evident that the most significant pieces of suspect code are used in many computer systems sitting on critical information infrastructure. Abu Dhabi's government needs to strengthen its security defences by establishing and maintaining strong malware incident response strategies, especially for critical national infrastructure. Malware is defined as malicious software such as a virus, specifically designed to disrupt or damage a computer system or any critical communication networks. Malware is ranked as the greatest threat to business, government critical infrastructure and individuals Choo (2010). It can be divided into

two broad forms; (a) generic malware that targets the general population; (b) customized information stealing malware which targets specific institutions. These two forms can further be divided into three major categories. This is mainly based on the way in which they enter a computer system and their behaviour once they have attacked. These broad categories are as follows

a. Viruses

A virus is a software program that enters a computer system through self-replication by inserting copies of itself into host programs or system data files. Viruses are often triggered through user interaction processes such as the opening of files, running of programs, or exchange of USB storage devices. They can be divided into compiled Viruses that are executed by an operating system like file infectors, boot sector viruses that affect the Master Boot Record (MBR), multipartite viruses, which combine the characteristics of file infectors and boot sector viruses and interpreted viruses which are normally executed by running applications.

b. Worms

Worms are self-replicating programs that execute themselves without user intermediation. They are divided mainly into Network Service Worms, which exploit vulnerabilities in a network service and Mass Mailing Worms, which are self-contained such as Trojan horses. Several types of attacker tool may be delivered to a system as part of a malware infection or other system compromise. These tools allow attackers to gain unauthorized access to or use of infected systems and their data, or to launch additional attacks. A popular type of attacker tool is a backdoor. A backdoor allows attackers to perform a certain set of actions on a system, for instance authenticating themselves by acquiring passwords or executing arbitrary system

commands. Typical backdoor malware includes zombies that are installed on a system for the purpose of attacking other systems; remote administration tools, which are installed on a system to enable a remote attacker to gain access to the system's functions and data as needed; and E-Mail generators which generate programs that can be used to create and send large quantities of e-mail, such as malware, spyware, and spam.

c. Trojan Horses

A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on a hard disk or any other form of external storage device. Progressively, Trojan horses constitute the first stage of an attack and their primary purpose is to stay under cover while replicating themselves within systems by downloading and installing stronger threats, such as a bot. Unlike viruses and worms, Trojan horses cannot spread by themselves. They are often distributed to a victim in an email message through deceptions such as images or jokes; or through a malicious website, which installs the Trojan horse on a computer through vulnerabilities via web browser software such as Microsoft Internet Explorer or Mozilla. After it is installed, the Trojan horse lurks silently in the infected system, invisibly continuing its misdeeds, such as downloading spyware, while the victim continues innocently with normal activities.

2.4.2 Mobile Malware

The ever rising popularity of mobile devices in payment systems and across the counter has increased their value to attackers; hence the increasing attacks

outside unregulated third party app stores. While mobile malware continues to remain an emerging threat, software that uses aggressive advertising frameworks, known as adware, is more persistent. The threats will continue to grow as attackers find ways to avoid the protection of the mobile eco-system. Attacks such as the Android defender in 2013 are very common for mobiles. Other attacks continued in 2014, including OlegPliss, an attack on Apple's iCloud that locked victim's phones by using the "Find-My-iPhone" functionality. Attacks on smart phones have increased recently because they present more capabilities in data storage and application features (Symantec, 2016). The UAE's government entities, therefore, need to implement strategies for controlling the mobile devices used in all government entities.

2.4.3 Phishing Attacks

Aloul (2010) looks at "Phishing" as a form of "Social Engineering" Internet fraud, aimed at stealing valuable user information such as credit card information, social security numbers and user credentials. Such fraudulent activities start by creating a fake website that looks exactly like that of a known legitimate organization but with a slightly different URL address. In many cases, the attackers target financial institutions such as banks, and other big firms dealing in e-commerce transactions. An email is sent to thousands of Internet users asking them to access the counterfeit websites, which are replicas of the trusted sites, to update their records by entering their personal details, including security access codes. These pages generally look genuine and the email seems to have come from addresses that are identical to the original organization address. However, such email can be falsified by a hacker and actually comes from the hacker's computer.

According to Choo et al. (2007) cyberattacks can be “syntactic”, “semantic” or “blended”. Syntactic attacks are those that develop computer code in the form of a virus, Trojan horse or worm which is then used to infect other computers by exploiting weaknesses in their software or hardware. Attacks of this kind using malware are “syntactic”. Semantic attacks take advantage of human social behaviour and weaknesses to gain personal information which are then used in the cyberattacks. Blended attacks, for their part, use “technical tools to facilitate social engineering in order to gain privileged information”. Phishing attacks are a type of social engineering. They represent online scams that frequently use unsolicited messages purporting to originate from legitimate organizations, particularly banking and other finance services, to deceive victims into revealing financial or Personal Identity Information (PII) to commit or facilitate other crimes (Choo, 2010).

The United Arab Emirates was in the frontline of phishing attacks in the Middle East and North African countries (MENA) in 2014, with one-third of attempts aimed at stealing money according to the latest data collected by the Kaspersky Lab study on “Financial Cyber Threats in 2013”. The study reveals that over 38.38 percent of phishing attacks in the region were targeted at UAE followed by Saudi Arabia (29.31 percent), Egypt (10.16 percent), Qatar (9.64 percent), Kuwait (6.29 percent) and Oman (6.21 percent). To combat such complicated cyber and information security challenges, organizations need to recruit competent cybersecurity staff with the right knowledge and experience to resolve cyberattacks. Next we investigate if any relationship exists between the competence of cybersecurity staff and the effectiveness of their organization’s cybersecurity programmes (Wunderle, 2006).

2.4.4 Competence/ Knowledge of Staff and Cybersecurity Effectiveness (H1)

In order to bridge the existing cybersecurity skills gap and the ever changing cyber threat landscape in most organizations, the experience and qualifications of professionals should be emphasized. Evidence of quality cybersecurity support staff includes the possession of hands on skills in cybersecurity and relevant academic qualifications and industry certifications in the cyber and information security domain. Further, there has to be strong evidence of continuing education, given that the cyber-threat is an ever changing one with unique attacker profiles created and published to the global networks from time to time. Awareness of trends in the domain includes knowledge of the current threats, tools and techniques used by cyber-criminals; vulnerabilities in the organization's infrastructure and mitigation strategies used; these are clear evidence of the seriousness of the agency in cybersecurity.

The personnel will exhibit deep understanding and commitment to cybersecurity policies and procedures in place to ensure the optimum protection of the innocent users. However, certification alone should not be the yardstick in determining how well a potential candidate will fit into an organization's cybersecurity programme, since many professionals pass the tests and earn the certificates but lack experience and job skills. At the end of the day, experience as well as certification (qualifications) should be the criterion for hiring most cybersecurity professionals. Rowe et al. (2011) reveal a shortage of about 20,000-30,000 qualified cybersecurity specialists in the US public sector alone, yet it is one of the most financially facilitated countries in its cybersecurity. Authors reveal that

only graduates with the right skills and experience will be able to resolve the ever rising level of international cyber conflict.

According to the new cybersecurity workforce study by ISACA's Cybersecurity Nexus (ISACA and RSA Conference, 2016), as enterprises invest more resources in data protection, their main challenge still remains that of finding top-flight security practitioners with the right skills for the job. "When positions go unfilled, organizations have a higher exposure to potential cyber-attack, in "a race against the clock", according to Christos Dimitriadis, ISACA board chair and group director of Information Security. The report further reveals that most job applicants do not have the hands-on experience and or certifications required to combat today's corporate hackers, leaving the organizations vulnerable to all forms of cyber-attack. It is therefore recommended that organizations invest in performance-based mechanisms for recruitment, create a culture of talent maximization and staff retention and groom employees with tangential skills to fill the available cybersecurity positions. (www.isaca.org/Cybersecurity Skills Gap Leaves 1 in 4 Organizations exposed).

Evidence of quality cybersecurity support staff includes the possession of academic and industry certifications in the cybersecurity/information security domain. Further, there has to be strong evidence of continuing education, given that the cyber-threat is an ever changing one. Awareness of trends in the domain, including knowledge of the current threats, tools and techniques used by cyber-criminals; vulnerabilities in the organization's infrastructure and the mitigation strategies used are clear evidence of the seriousness of the agency in cybersecurity. Additionally, these personnel will exhibit deep understanding and commitment to cybersecurity policies and procedures. This research strongly contends that a strong

relationship exists between the experience and qualifications of cybersecurity staff (hereafter 'the competence of staff') and the cybersecurity effectiveness of their organizations. On this basis, we formulate the following hypothesis: H1: *There is a positive relationship between the competence/knowledge of staff and cybersecurity effectiveness*.

Even if organizations recruit competent staff, senior management needs to play a great role in the cybersecurity programmes of the organization. Sadly, many organizations' cybersecurity teams continue to struggle to convince senior management of cybersecurity issues. Likewise, senior management also struggles to effectively articulate cybersecurity strategy and policies to technical cybersecurity personnel. It is as though two parts of the same organization were speaking a foreign language to one another, and each party had a very little or no knowledge of the other party's language (Cisco, 2017). Therefore, the role of senior management in ensuring the effectiveness of the existing cybersecurity programme and information security strategy needs to be well understood. In the next section, the role of senior management in the cybersecurity effectiveness of organizations is described.

2.5 Senior Management Support and Cybersecurity Effectiveness (H2)

Senior management are required to exercise "due care" and "due process" in ensuring the cybersecurity effectiveness of their organizations. To this end, they have multiple tools at their disposal that range from the application of management tools such as strategic planning to ensure a sufficient budgetary allocation for cyber and information security. Strategic planning can be defined as a written plan used by an organization to guide its activities so that certain predefined objectives can be achieved to ensure improved performance in future (Elbanna, 2010). These plans

usually take into account the prevailing economic and technological environment under which the firm operates, its strengths and weaknesses which influence how or whether to take advantage of the opportunities available under normal conditions as well as mitigating any threats that it may encounter (Glaister and Falshaw,1999). Organizations need to include mechanisms for detection, prevention, mitigation, response, reconstitution and remediation against the different forms of cyber and information security threat into their long term organizational strategic planning, strategic policies and frameworks. In this study, we investigate whether senior management in various Abu Dhabi government entities have incorporated cybersecurity planning into their organizations' strategic plans, policies and frameworks.

Studies reveal that cyber-crime has an overwhelming effect on a company and could damage its positioning in the market place Rees (2011). In the case of government entities, it could lead to criticism and loss of public trust Zhao (2010). As such, the prevention of cyber activities is considered a strategic management issue for both the private and public sectors. Dutton and Duncan (1987) proposes that strategic planning comprises "markets for strategic issues". The authors contend that these "strategic issues" can either represent problems to the organization if not acted upon, or opportunities when acted upon. Any department or organization that expects cybersecurity as a strategic issue and takes appropriate action in response will stand to benefit. Given the incidence of cyber-criminal activities in recent years, stakeholders would rather deal with organizations that do not have the negative publicity of losing massive amounts of sensitive data. The stakeholder's opinion of corporate readiness in addressing cybersecurity is therefore critical in the fight against the varied forms of cyber and information security challenges globally and

the UAE in particular. While an increasing number of organizations in the UAE already use strategic planning as a management tool, they have not realised the positive impression of its benefits Elbanna (2010) Their use is limited to what Brews and Purohit (2007) name "symbolic" or "rational" planning. The former points out the overall mission, vision and purpose of the organization. Rational planning starts with high level statements set out in the symbolic planning and breaks it down further into action plans, time lines and accountabilities. While this kind of planning is common among organizations that conduct strategic planning, it fails to deal with unpredictable situations that arise following a cyber-attack (Ginsberg, 1997).

The kind of strategic planning that is better positioned to deal with cyberattacks would be either transactive or procreative. Transactive planning requires constant feedback from management that further modifies and fine-tunes the plan to suit the current situation. Procreative planning instead "encourages product/service innovation and the degree to which plans encourage internal process innovation" (Brews and Purohit, 2007). Liedtka (2000) extends the procreative planning model further. In her paper entitled, "Strategic Planning as a Contribution to Strategic Change: A Generative Model," an alternative model of the strategic planning process is proposed. Her theory advocates separating strategic planning into two features, cognitive and behavioural. The author argues that strategic change begins with a cognitive framework in the minds of managers, with the creation of a gap in their view of the current situation and the image of a future to which they aspire. From the above argument, C-level management in various government entities needs to create frameworks that incorporate cybersecurity changes and their effects on organizations' information assets.

The second process of strategic management advocated by the same study is the "behavioural" process, where organizational members must begin to act in new ways according to the present situation. It is these new actions and the lessons learned from the new routines that create capabilities which allow the organizations to close the ever-increasing gap between "today's reality and tomorrow's vision" (Liedtka, 2000, pp. 200). It is further argued that the application of the cognitive process leads to an increased level of awareness and attitude changes necessary for addressing the information security issues raised. Strategic planning has to be thoughtful and conscious; it results in understanding the present situation, projecting a desired future outcome and then applying a process to come up with concrete steps in bridging the current gaps.

While the author confirms that many empirical studies show an association between strategic planning and performance, as measured by economic indicators. The findings of her study, paradoxically do not reveal any relationship between strategic planning and cybersecurity. We intend to establish these relationships as part of the findings of this study. Since strategic planning is a management tool that guides organizations in the management of change in turbulent times and since cyber-criminal events can have disastrous results to critical organization infrastructure and information assets, we propose a framework that incorporates strategic management into the cybersecurity planning for all Abu Dhabi's government entities.

Meanwhile Rohmeyer (2006) reveals that information security managers are expected to work as information mediators between the general management departments and the technical departments to ensure smooth information dissemination. The authors further claim that high effectiveness in information

security management is positively related to the skills and experience of the information security officer. According to the (ISACA and RSA conference, 2016) a global survey was conducted on 461 cybersecurity managers and practitioners, suggesting that 75% of the respondents expected to fall prey to cyberattacks by the end of 2016. This implies that Senior Management needs to demonstrate cyber resiliency support through proactive measures in policy enforcement, budgetary support for cybersecurity technologies and training programmes, among other methods to ensure the effectiveness of the programmes. They highlight a struggle to acquire enough skilled cybersecurity staff, with over 60% of the recruited individuals failing to resolve complex incidents.

2.5.1 Evidence of Senior Management Support

Evidence of senior management support includes the presence of a senior officer at the rank of Chief Information Officer (CIO) or Chief Information Security Officer (CISO) with well-defined authority in information security matters in the organization and the presence of cybersecurity strategic plans for the entire organization. This person further should have demonstrated an understanding of cybersecurity matters in the organization through the deployment of well qualified information security teams supplemented by on-going education programmes; the implementation of effective policies and procedures; training and awareness programmes for all users; appropriate technologies; and the adoption of international best practices.

Further evidence that cybersecurity matters are taken seriously by the organization can be shown by the presence of cybersecurity strategic plans. Well thought out strategic plans are distributed throughout the organization and can be

described by the senior staff which is responsible for matters of information security. These plans act as guides for the development of policies and procedures, training and awareness programmes.

In a government department that takes cybersecurity seriously, the day-to-day operations of issues related to cybersecurity are governed by clear and well-articulated policies and procedures. These policies and procedures govern user behaviour in the organization's information systems. The policies developed and implemented may range from those relating to email, Internet use, password strength, mobile computing devices, to issues such as access, distribution and destruction of documents, visitor management, etc. User awareness of these policies and procedures is a strong indication that the organization has an effective cybersecurity programme. From this section we arrive at the following two hypothesis: *H2: There is a positive relationship between senior management support and cybersecurity effectiveness;* Next we evaluate the role of the technology level in ensuring an effective cybersecurity platform.

2.6 Level of Technology and Cybersecurity Effectiveness (H3)

2.6.1 Effective Technologies for the Prevention of Cyberattacks

Government entities that have invested in the latest cybersecurity technologies demonstrate better understanding of cybersecurity risks than those without cybersecurity investment budgets. There are numerous kinds of software and hardware technology already deployed by Abu Dhabi's government entities. The most common technologies used globally include different forms of firewall, data encryption, anti-malware, anti-spyware and anti-virus scanners, among others.

For these tools to be effective, the human element that supports and maintains these systems cannot be ignored, for most of these systems have limitations.

In the electronic world, even though the access problem has been greatly resolved through advanced technologies, for example, the application of database and electronic records of management systems when handling most of the business transactions, a new encounter is generated when it comes to managing information access. Furthermore, as software vendors increase the functionality of mobile computing platforms and web services, the availability of data increases drastically. However, this rapid increase leads to other challenging issues such as the confidentiality and integrity of information. The early design of the Internet focused mainly on shared access and trust, with security measures as an afterthought. Many of the designed Internet protocols depend on trust between individuals to give their services, which may not be very effective especially for today's complex traffic, involving highly sensitive transactions between people and institutions. Such challenges pose significant demands for highly secure software and hardware platforms to maintain the appropriate level of confidentiality, integrity and access to critical data (Conklin, 2006).

Technological advancement is a key issue of concern, especially when it comes to the prevention and mitigation of cyber and malware attacks. However, as more vigilant corporations continue to implement more effective security defences in the UAE, threat actors have progressively stepped up their attacks on government entities, middle-tier and small organizations, many of which may not have security devices to match those of larger businesses. Small firms often consider themselves too insignificant to attract threat actors which is clearly a misperception. It is important to note that sophisticated opponents often target small and medium-sized

organizations as a means to gain a base on the interconnected business ecosystems of the larger organizations that partner with the smaller ones. This dangerous situation is compounded by the fact that big companies often make little effort to monitor the security of their partners, suppliers, and supply chains, (Price, 2015). Organizations need to invest heavily and periodically upgrade their cybersecurity technology if they are to match the onslaughts of cybercrime.

It is critical for cybersecurity experts and C-Level officers within government entities and the private sector to understand the risks associated with new technologies deployed within their organizations. The ever increasing threats to cyber and information security, at the level of the individual, the firm, and government and critical infrastructure, make security everyone's obligation. Abu Dhabi's government needs to ensure that the highest level of security is embedded in all national identification documents such as the Emirates identity card, driver's licence and labour card. More still, management needs to determine appropriate levels of risk tolerance, security requirements and the necessary technical safeguards to ensure the protection of such highly sensitive documents.

Based on some great technological advances, the Cyberspace Policy review by PwC identified vulnerabilities in cybersecurity as systemic risks introduced into infrastructure, defence, and personal property resulting from the widespread adoption of and dependence on various technologies. The more a nation relies on cyberspace as a critical part of its national infrastructure, the more responsibility it has to protect it. In addition, the Internet is constantly changing the way we live and conduct our business. These changes occur both in ways that we currently experience (e-commerce, real-time information access, e-learning, expanded communication

options, among others) and in ways that we have yet to experience or understand (Price, 2014).

A growing percentage of Internet and information access is through broadband connections, now that most users and organizations are increasingly interconnected across physical and logical networks. Network and system connectivity has broadened; the volume of electronic information exchanged through cyberspace has thus increased to include multimedia, process control signals and other forms of data. Several software and hardware solutions to protect organizations from cyber and information security vulnerabilities such as malware attacks have been widely deployed in industry and government entities across the globe and the UAE. However, the question whether these technologies are effective in doing their job remains unanswered. It is critical to focus on the rapid detection of security intrusions and an effective, timely response to malware incidents. Therefore to address this concern, Abu Dhabi's government needs to reposition its security strategy by establishing a close link between technology, processes, people skills and appropriate risk management activities. Several people including some in government still see information security as mainly a technical problem and believe that by simply buying the right software and hardware platforms, they will resolve the issues and security concerns involved. However, this may not be the case, since information security involves people, processes, and technology; hence, a balance between these integral parties needs to be struck.

Most organizations are no longer certain if their present technologies, methods and strategies are still adequate to prevent future cyberattacks. The sophisticated technologies which have been developed globally by many organizations may not be a solution to the prevention of low level attacks by new

viruses that continually damage protected systems worldwide, affecting millions of systems.

There are numerous kinds of technologies deployed to protect firms from different forms of cyber and malware attacks. Some of these technologies like biometric systems are meant to provide edge protection to entry points while others provide assurances against data modification. The most common technologies used globally include the different forms of firewalls, data encryption, anti-malware, anti-spyware and anti-virus scanners, among others. Other technologies provide means of recovery in case of successful attacks being launched (Rees, 2011). Regardless of these technologies deployed, their sole purposes include the following:

a. Confidentiality of information by ensuring that information or data is only accessible by an authorized persons.
b. Integrity that is acquired by ensuring that information or data can only be modified by only the authorized persons and no-one else and that no theft of information occurs.
c. Availability by ensuring that information systems will not be disrupted or users denied access as a result of malicious behaviour such as a cyber-attack.

Most of the cyberattacks across the Internet are opportunistic rather than attacks targeting specific business entities or government entities. An opportunistic attack occurs when an attacker targets several parties by using one or many of the common ways to attack such parties, in the hope that some of them will prove vulnerable. In an opportunistic attack, an attacker has many targets and will not care much who the victims are, but how of them fall into the trap. Organizations have also started realizing that new technologies assumed to prevent cyberattacks have their

own drawbacks and vulnerabilities. It must therefore be acknowledged that more than simply investing in new technologies, organizations must develop complete strategies, solutions and methods to combat security problems. Furthermore, the question of the adequacy of the available software and hardware solute, such as password protection, secret key encryption, public key Encryption, Secure Sockets Layer (SSL) Access Control Lists (ACLs) and other security protocols still remains an issue of great concern (Bronk and Eneken, 2013).

2.6.2 Software Solutions

Several software solutions exist globally which make a considerable effort to detect, prevent, mitigate and protect organizations from different forms of cyber-attack. We review some of the common ones below:

2.6.2.1 The Use of Encryption Codes

Encryption is the process of encoding messages (or information) in such a way that spies or hackers cannot read it. In an encryption scheme, the message or information is encrypted by an encryption algorithm, turning it into an unreadable code. This is usually done by means of an encryption key, which specifies how the message is to be encoded. Encryption at a very primitive level protects data privacy and their integrity. But more use of encryption brings more challenges to cybersecurity. Encryption is also used to protect data in transit, for example, data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms, etc. Hence, by encrypting the code one can know if any information has been leaked.

According to the Emerging Cyber Threats Report (2015), encryption could be a solution in online transactions, although it is still difficult to apply effectively, since most governments have continued to resist its deployment due to their great fear of failing to gather the necessary evidence. Furthermore, it is clear that while the privacy concerns of most sensitive users and technology companies lie in data collection, government officials and security conscious citizens are most worried over the loss of visibility into the activities of malicious actors. The major concern is the relationship between technology and privacy since every new technology poses a new privacy threat to an organizations. Encrypting data before it moves into the cloud may be a key solution for compromising data since the user could access them only after a complete decryption process. However, we are not sure if the existing encryption algorithms may not be easily compromised by attackers with superior counter algorithms.

2.6.2.2 Anti-Virus Software

Antivirus software is a computer program that detects, prevents, and takes action to deactivate or remove malicious software programs from host computers or any other electronic devices. Such malicious programs include spyware, viruses, worms and Trojan horses. The most common antivirus programs include an auto-update feature that enables the program to download profiles of new virus definitions so that it can check for them as soon as they are discovered. The antivirus software products discover malware mainly by looking at certain characteristics of known instances. Such sets of characteristics are known as signatures. Signatures are highly effective for identifying known malware and are also often a good means of identifying new modifications of known malware, such as a macro virus that has

been altered slightly from the original. The major antivirus vendors usually release signatures for a significant new threat within several hours, a remarkable feat considering that each vendor must analyse the threat, write a signature, test it, and distribute it, along with documentation. Because signatures are based on known threats, they are not capable of identifying completely new malware. To address this, antivirus software vendors have incorporated heuristic techniques into their products; these techniques are designed to identify unknown instances of malware by examining many characteristics of files.

2.6.3 Hardware Solutions

Several hardware solutions for the prevention, detection, response, counter attack and surveillance to combat the various forms of cyber-attack have been developed. The question is whether these existing technologies can be enough to combat the cybersecurity problems in society. Some of these existing technologies are discussed in detail in the next section of this study.

2.6.3.1 Firewalls

A firewall is a software program or piece of hardware that helps screen out the hackers, viruses and worms that try to reach a computer over the Internet. All messages entering or leaving the Internet pass through the firewall presented, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting malware. Today Firewalls have become the staple of network security architectures, primarily providing access control to network resources, and they have been successfully deployed in the large majority of networks such as those of government

organizations and individual users. Firewall and Intrusion Detection (IDS) together are adopted more frequently. Network attacks are a crucial element in providing networks with the reliability required in today's competitive environment. However, while most firewalls provide effective access control, many are not designed to detect an attack at the application level (Uchenna et al., 2016).

When most people think of network security, they think of firewalls. Firewalls are widely deployed as a first level of protection in a multi-layer security architecture, primarily acting as an access control device by permitting specific protocols (such as HTTP, DNS, SMTP) to pass between a set of source and destination addresses. Integral to accessing policy enforcement, firewalls usually inspect data packet headers to make traffic flow decisions. In general, they do not inspect the entire content of the packet and cannot detect or prevent malicious code embedded within normal traffic. Firewalls offer excellent protection against network threats, but they are less than complete protection against these threats by incorporating physical security, host security, and user education into am overall security plan.

2.6.3.2 Intrusion Detection Systems (IDS)

Intrusion detection is a set of techniques and methods that are used to detect suspicious activity at both the network and host levels. Intrusion detection systems fall into two main categories: signature-based intrusion detection systems and anomaly detection systems. Intruders such as computer viruses, have signatures that can be detected using software. The IDS tries to find data packets that contain any known intrusion-related signatures or anomalies related to Internet protocols. Based upon a set of signatures and rules, the detection system is able to find and log

suspicious activity and generate alerts. Anomaly-based intrusion detection usually depends on packet inconsistencies present in the protocol header parts. In some cases these methods produce better results than signature-based IDS do.

Network IDS products inspect the entire contents of every packet traversing the network in order to detect malicious activity. This content inspection technique provides deeper packet analysis than a firewall or a router. Intrusion Detection Systems are effective when sophisticated attacks are embedded in familiar protocols, such as an HTTP session, which would normally pass a firewall undetected. It is not surprising that the processing power required for an Intrusion Detection System is an order of degree higher the for a firewall product.

Just as a firewall has many shortcomings, Intrusion Detection System (IDS) also has many, such as low detection ability, lack of an effective response mechanism, poor manageability, etc. However, used together, the cooperation between IDS and firewalls can improve the network security to a great extent. On the one hand, IDS monitors the network, provides a real-time detection of attacks from the interior and exterior, and automatically informs the firewall as well as dynamically altering the rules of a firewall once an attack is found; on the other, the firewall loads dynamic rules to hold up the intrusion, controls the data traffic of IDS and provides security protection for it (Uchenna et al., 2016).

An extension of the IDS is the Intrusion Prevention System (IPS) which is used for both detecting intrusion activities or threats and managing responsive actions in these systems throughout the network. IPSs monitor real time packet traffic with malicious activities or which match specific profiles and will trigger the generation of alerts; they can drop or block this traffic in real time as it passes through the network. The IPS's main counter measure is to stop an attack in

progress. IPS can be termed the extension of IDS which exercises access control to protect computers from exploitation. IPS is an intelligent device that is capable of not only detecting malicious activities, but also taking preventive actions to secure the host or the network. Many organizations fail to address employee insider vulnerabilities as well as the assessment of third party partners and supply chains. This is specially demonstrated by their failure to strategically invest in cybersecurity to ensure that it is in line with their business objectives (UNDP, 2012).

From this section we see that those departments that have invested in current cybersecurity technologies demonstrate an understanding of cybersecurity risks. Given that effective technology is necessary for the successful prevention of cyberattacks, the following hypothesis can be formulated: *H3. There is a positive relationship between the technology deployed and cybersecurity effectiveness.*

Apart from deploying state of the art technologies for protection against all forms of cyber-attack, organizations need to put in place periodic training programmes for staff to develop essential competences, reveal new attacker techniques and security vulnerabilities and thus ensure continuous knowledge sharing and development. Therefore, in the next section we discuss the role of training for cybersecurity staff and the awareness of users in ensuring the effectiveness of their organizations' cybersecurity system.

2.7 The Role of Cybersecurity Training Programmes (H4)

Effective training and awareness programmes are comprehensive, measurable and regular. An organization that is serious about cybersecurity needs to put great emphasis on training and awareness programmes conducted by knowledgeable individuals across all user departments in the organization at set frequencies during

the year. For these training programmes to be effective, they should be culturally relevant to the audience.

Meanwhile, the Oxford English Dictionary provides a definition of the key words in the phrase "training and awareness" that helps in formulating the conceptual foundation of this section. The dictionary looks at training as "the action of teaching a person or an animal a particular skill or type of behaviour" and "Awareness" as "knowledge or perception of a situation or fact" (http://www.oxforddictionaries.com/). From the dictionary definitions of the two concepts, it can be inferred that Information Security Training consists of thoughtful activities conducted by an organization to teach skills or behaviours to its employees so that they gain an understanding of threats against their electronic information and the systems around them. This understanding helps them to take appropriate action to prevent the threats from materialising. Since the "understanding" that leads to appropriate action requires an attitude change, any initiative by a company to create this awareness among its employees requires careful planning, implementing and measuring for it to make the needed attitude change.

Employees are the weakest link when it comes to incidents involving information security and the insiders of the organization (Vroom and Von Solms, 2004; Da Veiga and Eloff, 2010; and Wilson and Hash, 2003). An "insider" is an individual who currently or at one time had authorization access to an organization's system, data or network. While 48% of cybersecurity breaches were accidental, 17% were intentionally committed and 35% malicious (Vroom and Von Solms, 2004). According to these authors, companies ignore insiders and instead focus on external threats. They spend money on the technical side but pay little attention to the human factor. Focusing on technical solutions to prevent cyberattacks is, however, not

enough since effective cybersecurity defences require users to be fully aware of and to use the available security measures within the organization.

An increasing number of security breaches in organizations can be attributed to insider attacks by employees by either neglect or choice. Most employees consider information security issues to be the sole responsibility of the IT department (Dutton and Duncan, 1987). However, there is no way that IT departments alone can ensure data security. The failures to prevent or minimize security breaches due to end-users' non-compliance are evidence of failed or non-existent programmes to promote information security awareness. Still, since training and awareness programmes issues are non-technical, it is easy for information security managers and senior management to ignore their importance; they may instead focus on technologies such as firewalls and intrusion detection systems (Rezgui and Marks, 2008).

The last two decades have seen advances in security technologies. Twenty years ago, only one kind of firewall existed; today there are hundreds (Schultz, 2005). Given the abundance of useful technology that exists, one would then think that achieving suitable levels of security would be minor. Surprisingly, however, many organizations that have an abundance of technical controls nevertheless experience a big number of security related breaches (Schultz, 2005, p.425). The primary reason why there has been an increase in breaches of information security is that information security is a people problem, not a technical one. While millions of dollars to protect them from external cyberattacks are being spent by organizations, the greatest threats to information systems are from within organizations whose users lack basic knowledge and training. However, the focus should not change from the external to the internal threat landscape, but rather that equal emphasis should be placed on both. According to Leach (2003), 80% of major security breaches could

result from poor security solutions. An effective information security training programme should take into account the fact that user behaviour and attitudes will need to change if the incidence of insider attacks is to reduce.

Several surveys complemented by various media reports in the recent past reveal that current or former employees and contractors are second only to hackers as the main offenders behind the increased cyberattacks against USA organizations (Greitzer et al., 2008). The kinds of crime associated with these insider threats include spying, disruption, terrorism, fraud, blackmail and dishonesty. The authors contend that in order to help staff, management and personnel understand the risks posed by insider attacks, training and awareness programmes targeting different roles and responsibilities should be conducted. The methodologies to be used to design effective training and awareness programmes should be drawn from "philosophical and theoretical roots to theorists such as Jean Piaget, John Dewey and Lev Vygotsky." They argue that this is necessary because the effort requires complex knowledge and skills to be communicated, such that the users "constructed" or discovered meaning that was new to them. According to this view, a traditional teacher-centred approach will not be successful, as it does not take into account the behavioural or attitudinal changes necessary to have a long term impact.

The success of information security training and awareness programmes depends on how effective they are in changing user behaviours towards information security. According to Leach (2003) there are five behaviours that present internal threats to organizations; (a) Lack of security common sense, where a user does something "dumb" such as opening an executable file or email attachment; (b) a user forgetting to apply simple security procedures such as failing to back up files; (c) a user taking inappropriate risks because he did not accept the level of risk involved,

e.g. leaving a laptop unattended in an open office; (d) Wilful acts of negligence where users failed to follow necessary security processes, e.g. mailing a highly sensitive document outside the organization without any protection; (e) Deliberate attacks against the company's interests. All these behavioural issues need to be addressed through training and awareness programmes that may be organized from time to time, especially for the less experienced users of the Internet and information systems.

Several authors (Greitzer et al., 2007; Pfleeger and Caputo, 2012) agree that the key to developing an effective information security training and awareness programme requires an understanding of human behaviour. In their paper "Leveraging behavioural science to mitigate cybersecurity risk" they pose the following questions:

(a) Which aspects of human behaviour offer the most promise in making cybersecurity processes and products more effective?
(b) What role should education and training play?
(c) How can we encourage good security practices without unnecessarily interrupting or annoying users? How can we create a cyber-environment that provides users with all the functionalities they need without compromising enterprises of national security?

Hight (2005) argues that training and awareness programmes explain the employee's role in the area of information security by showing the users what they can do to protect their organization's critical data and instilling in those who manage critical information a sense of responsibility. A further analysis reveals that people's mistakes cannot be solved by the simple addition of technology but through a joint

effort and participation between the IT communities of interest, the business community and the nationals through training and awareness, along with critical government and top management support. Meanwhile (Pfleeger and Caputo, 2012) maintain that in order to prevent cyber threats, the whole development cycle of technologies from concept design, development, implementation and usage need built-in information security components. They use insights from the behavioural sciences to develop their theory in response to the questions raised above.

The areas of behavioural science which were found relevant to cybersecurity included:

(a) Recognition easier than recollection

People are more likely to remember passwords consisting of images rather than alpha-numerical characters. While this theory is currently being applied for user-computer authentication, its use is still not widespread.

(b) Interference

This theory states that frequent changes to a memorized item always interfere with recalling the newer version of the same item. This has been applied to studies where it was shown that login failures increased with the frequency of required password changes. However, login failures fall where a system allows for multiple trials to enter a password. A system that is less strict in the number of attempts therefore experiences fewer login failures.

To further their theory, (Pfleeger and Caputo, 2012) investigated other areas from psychology, behavioural medicine and other disciplines that affect the behaviour related to reasoning and bias and have a potential for improving cybersecurity. For example they found that a theory in cognition called the

"identifiable victim effect" would have relevance to cybersecurity. This theory looks at a tendency of individuals to "offer greater aid when a specific, identifiable person (the victim) is observed under hardship, when compared to a large, vaguely-defined group with the same need". According to this theory, users are bound to choose a stronger password for their online banking, for example, when they personally know of someone whose bank account has been recently hacked.

The implications of this theory for training and awareness programmes was captured in a study conducted by McCrohan (2010) provided insights into how the security awareness of the organization can be improved by educating users about the threats. They hypothesized that:

i. If users have greater degree of awareness about threats to information systems, they will engage in behaviours that enhance security.
ii. An appeal based on threats to the online banking activities of the participants will result in enhanced behaviour.

They further indicated that if individuals are; (a) informed of threats facing their online activities; (b) informed of their ability to mitigate security threats; and (c) provided with detailed information on how to create strong passwords, they will be more inclined to do so. In this thesis we determine the role of information security training and awareness programmes and their contribution to cybersecurity effectiveness, especially in Abu Dhabi's government entities.

To test the effect of threat awareness on weak passwords, an experiment was created by employing two levels of threat information: High and Low. The primary hypothesis of the study was that the strength of passwords at Time 1 would not differ, but that high information treatment would have a greater effect on the strength of

passwords at Time 2. Participants were randomly assigned to either the High or Low information group. They were then asked to log into a website created for the study, where they were directed to create passwords to access the information for the study. The password created before any experimental manipulation was the key pre-treatment dependent variable of the study. The low information security group was then given basic information about security, while the high information security group was treated with stories and evidence of the cybersecurity exploits of online personal banking of millions of people worldwide. After two weeks the groups resumed again and were directed to change their passwords as the old password had expired. The study found that the group treated with high information on security breaches improved the strength of their passwords by over 46% between Time 1 and Time 2. They attributed this positive shift to the awareness training given to them. In this study we conducted a pilot study on cybersecurity training and awareness by training a selected target group on issues of cyber and information security. The objective was to investigate the role of culture in the design of appropriate cyber and information security training and awareness programmes, as well as checking the impact of training on cybersecurity effectiveness.

2.7.1 Training and Cybersecurity Effectiveness (H4)

The worldwide increase in ICT security threats has mostly been due to the increased amount of electronic data, increased number of mobile terminals, well organized groups, difficulties in tracing attackers and limited knowledge of IT security amongst ordinary people (Aloul et al., 2012). This has led to the introduction of cyber laws in many countries, including in the United States, the Middle East and the UAE. Unfortunately, cyber threats are likely to succeed due to differences in

cultural attitudes between different groups of people globally. The author argues further that while organizations continue to train their professionals in technology very little effort has been put into general cybersecurity training and awareness, which creates a major risk to the employees when a cyber-attack occurs.

The Gartner Group reports that security training and awareness produces more Return on Investment (ROI) than any other activity in information security, yet most organizations have approached this area as one of low priority. Usually when a budget crisis occurs in an organization the area of information security that is most likely to be cut is that of information security training and awareness. Schultz (2005) explains this to the difficulty of determining the direct benefit of training and awareness. He claims that employees who receive security awareness sessions will afterwards be less vulnerable to social engineering than others. This however does not happen often, as most training programmes are inferior and not aligned to the organizations' business goals.

Information security effectiveness requires a change in organizational culture and behaviour (Vroom and Von Solms, 2003). An information security culture can be defined "as a way things are done in the organization to protect its information security assets" (Da Veiga and Eloff, 2010). Organizational culture includes the ideas shared by work colleagues and communicated between each other. Culture is the single most important factor which accounts for success or failure of an information security programme. The ideal culture would be where it comes as second nature for staff to follow the guidelines of the organization. Leach (2003) believes that the behaviour of users can be improved through a variety of interconnecting methods which together work to create a strong security culture and strengthen the way

security influences the behaviour of others. We need to instil a security culture amongst departmental employees as a way of improving cybersecurity effectiveness.

The contribution of culture to organizational change has been thoroughly studied. For instance Schein (2004) defines culture as:

> The pattern of basic assumptions that a given group has invented, discovered or developed in learning to cope with its problems of external adaptation and internal integration and that have worked well enough to be considered valid, and therefore to be taught to new members as the correct way to perceive, think, and feel in relation to these problems (p 1).

Furthermore the author divides culture into three layers. The first level is the "artefacts" of the culture. These are the visible elements that relate to that culture. In the information security domain these would be the firewalls, monitoring tools, published policies and procedures. Next are the "espoused" or shared values. These are semi-visible. In information security these would the strategies dictated by senior management (Vroom and Von Solms, 2003).

The final and deepest levels of culture are the basic tacit assumptions which are hidden and occur at the individual level. These assumptions are the underlying beliefs and values of the staff of the company. Between the various layers, there is constant interaction. The organizational culture could therefore have a huge impact on the information security of the firm. The benefits of changing culture to engage in security automatically in daily life would positively affect the success of the organization. Information security culture consists of a subset of information security behaviours and information security components. This culture develops when users interact with information security components. To cultivate an acceptable level of

information security, organizations should ensure that a comprehensive and adequate set of information security components is implemented. Examples of components include the human element, the processes used and the technical controls implemented. Organizations should furthermore ensure that employees' interactions are in line with the requirements of the information security policies implemented.

Katz (2005) carried out a comprehensive survey on wireless networks at thousands of access points in Dubai and Sharjah between 2008 and 2010; the results show that 32% of the access points were unprotected, while the others used weak security techniques. The biggest threats to people are phishing attacks, where an email may be sent to thousands of Internet users requesting them to access fake websites which could be replicas of well-known trusted websites. Many people enter their personal details in the belief that the sites are authentic when they actually came from a hacker's computer. It is taken for granted that Middle Eastern cyber criminals are increasingly targeting innocent UAE residents with advanced hacking methods such as phishing scams. This has led to increased IT security in major operators such as telecom companies, banks and UAE government entities. However, people are the weakest link in any security system and are still unprotected.

Governments need to play a leadership role in instituting a cybersecurity culture amongst nationals through approaches that include training and awareness, culturally sensitive cybersecurity policies and education. Meanwhile, Seibert (2002) looks at culture as an organized group of learned responses with ready-made solutions to problems faced by people through interactions with others in the same society. This bond of interaction compels them to consider cultural awareness when designing cybersecurity training and awareness programmes. It is further revealed that culture shapes how people in a society respond to the effects of cyber-attack.

Unfortunately, over 85% of the UAE population is foreign, which implies that several cultures and cultural norms have been imported into the region. Such people come from different regions, Asia, Africa, Europe, and the Gulf Cooperation Council (GCC) countries, among others. As a result, a multi-cultural society has been created in the UAE which necessitates a culturally sensitive cybersecurity training and awareness programme.

Whitmer (2007) developed a cultural sensitivity and awareness checklist for the medical field, but this checklist can be extended to culturally sensitive cybersecurity awareness campaigns. It includes cultural identification, language barriers, selecting a communication method that suits the target society, if possible incorporating a language translator in the session who understands beliefs such as religious and spiritual beliefs and trust, among others.

Different cultures have different training and awareness needs. Therefore, all cyber and information security training programmes should be tailored to the cultural setup of different communities in the region by carrying out a Pre-Training and Awareness Needs Assessment for different groups of individuals or cultures in the region. This would aid the design of appropriate training and awareness programme with clearly defined roles and responsibilities. Awareness programmes need to teach people information security issues such as confidentiality, integrity, availability and non-repudiation, the need to be aware of what needs to be protected. More still, they need to understand why they need to take cyber and information security seriously, why they should protect the critical national infrastructure, who the enemy in cyberspace is, what they gain from proactive participation in the security of their organizations and communities, how a secure environment assists them in the

accomplishment of tasks and finally why they are key stakeholders in the fight against cyber threats and cyber terrorism.

As organizations expand the use of advanced security technologies, hackers attempt to break into their internal security by using the weakest links or less-informed computer users. Users are the biggest security threat to the IT-security of any organization and therefore continuous training and awareness programmes are needed to help change their view of information security in the organization. Business success depends upon the continuity of operations and information provided to the business processes by information systems. The growth, excellence and efficiency of the business could be damaged by threats to and misuse of information. But awareness programmes would help in setting measures and ways of educating users in how to behave and benefit from information without jeopardizing its confidentiality, integrity and availability. Lack of awareness and mishandling of information could expose it to competitors or corruption.

Cybersecurity training and awareness help individuals in decision making especially during uncertain situations and promotes a security-aware culture within organizations, hence reducing human error which could pose a major threat to the security of most organizations. However, technical solutions are unlikely to prevent security breaches and cyber threats within the government entities in UAE. Therefore, we need to introduce and maintain a culture where positive security behaviours are valued. The usability challenges associated with information security need to be well understood and resolved. This means that security functions need to be meaningful, easy to locate, visible and convenient to use. It is important to acknowledge the influence of individual cultural differences, personality traits, cognitive abilities, bias and heuristics which all affect how individuals perceive

security risks. These are important because they explain why individuals make certain decisions and why specific behaviours may be observed. The culture and climate that people come from has a significant impact on values, attitudes and behaviours as well as providing a great impact on the way they see cybersecurity issues in the community and within their organizations.

Furthermore, Kruger et al. (2011) looked at how cultural factors impact the security knowledge and behaviour of different people in society. It is argued that cultural differences may manifest themselves at different levels of security awareness. The authors assessed the level of awareness, knowledge and behaviours amongst students in two selected universities in South Africa. Their main objective was to identify how cultural differences affect students' understanding of security issues in society. Their findings revealed that some cultural factors such as one's mother tongue and place of origin show a significant impact on the awareness levels of security issues among selected students. It is therefore worthwhile to perform a study to investigate the validity of these findings and confirm that peoples' culture cannot be taken lightly when designing appropriate cyber and information security training and awareness programmes in the UAE and throughout the globe.

The idea has been proposed that informal behaviour and acts of communication have a fundamental role in disclosing the characteristics of people. It is stated that the process of communication creates a central hub in any information system. Furthermore, patterns of learning and culture as well as norms form constituent elements of informal behaviour; therefore, complete management of information security can only be ensured if the behavioural aspects of individuals and groups have been well understood. This necessitates establishing the validity of these findings, especially in a multi-cultural environment such as the United Arab

Emirates where the largest percentage of the active labour force comprises immigrants from several countries, notably from Asia, Africa and Europe.

As a preliminary, the researcher conducted a pilot study to investigate the role that culture plays in cybersecurity. In this study a total of fifty (50) employees was randomly selected from a mid-sized organization in Abu-Dhabi (UAE) representative of the study population, and divided into two groups. The first group, comprising employees from similar cultural backgrounds (in India only) was treated to a cybersecurity training programme that was culturally sensitive conducted in their first language (Hindi), while the other group, consisting of employees from a multitude of different cultural backgrounds (Ugandans, Philippines and Nepalese) undertook a generic training programme conducted in English. A pilot survey was conducted following the above treatment. The pilot involved the provision of pre-and-post-training assessments with the help of questionnaires tailored to cyber and information security awareness especially of various issues to do with the region. Details of this survey are discussed in Chapter Three of this thesis.

It is claimed that governments develop security policies which specify the correct behaviour by employees even when they are not aware of the risks involved and do not fully understand the correct security behaviour within their society (Humaidi and Balakrishnan, 2013). Furthermore, the authors argue that the cultural systems of a society shape a variety of their psychological processes. The values that distinguish a country's culture can be categorised into individualism versus collectivism and power distance, among others. For instance, in the case of individualistic cultures such as Western ones, people tend to describe themselves in terms of their internal attributes, for example, goals, preferences and attitudes, while in more collectivist cultures such as those typically found in the Middle East,

individuals tend to express themselves in terms of their relationships and social group memberships. These individuals tend to avoid behaviours that cause social disruption. The behaviour of people can be changed by influencing what they consciously think about or by shaping the behaviour that is focused on more automatic processes of judgement and influence without changing people's thinking. It is revealed that influential tactics in specific situations may be counterproductive, hence invoking fear amongst in many different people in a society. Too many messages concerning certain security sensitive issues may hinder behavioural change within a multi-cultural setup.

2.7.2 Effective Training Methods

According to Siponnen, (2000), several methods of conducting cybersecurity training exist, for instance, "selling" information security to people through campaigns which provide good measures for improving people's attitudes although they may lead to unwanted results in terms of motivation and attitude. For this reason, they should be used carefully together with awareness programmes to provide good incentives for end users and for refreshing people's minds. Education should increase people's insights and answer the question, "why?" – this should increase motivation. Training should increase skills and competence and corresponds to "how?" Since the "why" part is important, employees should not be content with answers such as "you just have to do it", "this is our policy", etc. Their motivation and attitude are not likely to improve this way. The creation of an information security awareness programmes as a means of minimizing end-user errors requires a systematic approach.

Several cybersecurity awareness campaigns have been carried out globally to alleviate the cyber and information security awareness problem For instance, a cyber-streetwise campaign (2014) was carried out in the United Kingdom (UK) to concentrate on online users at home and some business ventures. In this campaign businesses were advised to adopt five basic measures to boost their online security and safety, for instance, the use of strong passwords, installation of strong antivirus software, and checking privacy settings on social media, patching systems whenever new updates became available, among others. In this campaign positive messages were used to influence the behaviour of online users.

Similarly, a parents' corner campaign was carried out in Africa with the intention of coordinating the work done by governments, industries and civil societies with the objective of protecting children and educating parents online. It emphasized that "people are not always who they say they are", the need to think before posting anything online and also that "friends must protect friends", among others. All these efforts in the UK and Africa provide an insight into solutions to online risk and behavioural change for UAE citizens online and for Abu Dhabi's government entities. It is extremely important to decide the target group of an awareness campaign, match the cultural theme of the message recipients and their cognitive and motivational characteristics with the intended contents. However, simple transfers of knowledge and awareness campaigns alone may not be sufficient to end the entire problem in the UAE. Therefore, an appropriate framework incorporating all other mechanisms would be greatly valued if it allowed the government to combat the ever escalating problems of cyber and information security. The government needs to organize security campaigns, avoid tactics that may cause fear among users, emphasize security education and provide a feedback

mechanism for obtaining the real-time concerns of people as well as instituting an online security culture amongst all UAE residents.

Meanwhile, Rezgui and Marks (2008) provides an insight into a study by EDUCAUSE which found that higher education organizations with information security awareness programmes were considered more successful and more advanced in information security than those without. 39% of the higher education programmes examined in the USA had an information security awareness programme. 75% viewed their information security awareness programmes as among the top three in this area. Based on this study of information security awareness programmes, the authors made recommendations that could be applied to higher education in the UAE.

(a) Establish information security policies and procedures that are tailored to the government policies which should be achievable and understandable.
(b) Conduct campaigns of best practice in information security awareness and advertise information security awareness and materials throughout the campus.
(c) Train all users in information security best practice. While training should be regular, basic training for all users should be compulsory.
(d) Practice reward and punishment management
(e) Carry out continuous evaluation.

In the meantime, Herath and Rao (2009) conducted a study on the role of penalties and perceived effectiveness on encouraging information security behaviour in organizations. To do this, they developed a framework that evaluated the relative importance of three incentive mechanisms: penalties, social pressure and perceived

effectiveness. They observed that prevention measures are a useful primary strategy for reducing computer crime, but as the level of punishment increases, individuals become less likely to carry out the desired behaviour. Increasing the level of punishment from verbal warning to the employee to the threat of job loss or heavy fines would seem to prevent wilful breach. They hypothesized therefore that "Increased severity of penalty will be positively associated with intentions to comply with organizational security policy."

Furthermore, they observed that not only the promise of penalty but also the certainty of it could have an impact on the security misbehaviour of an organization. For this to be effective, a set of monitoring and detection mechanisms is necessary to make certain that employees are acting according to information security policies. Monitoring can be done through a combination of activities such as random walks, computer history logs, network logs etc. If the employees are aware of monitoring and detect the efforts being made, they are more likely to obey policies. Leach (2003) divides the factors that influence security behaviour into two distinct groups. The first group are those that influence the users' understanding of what behaviour the company expects from them. The second group of factors are those that influence the user's personal willingness to constrain his behaviour within the accepted and approved norms. The user's understanding of which behaviours are expected of him is formed from what they are told; what they see being practised by others around them and their experiences deriving from decisions they have made in the past. What the users are told makes up the company's body of knowledge. The effectiveness of the body of knowledge in conveying what constitutes security behaviour varies according to its accessibility; completeness; the clarity of the stated security values; and the uniformity of those values.

What employees see is heavily influenced by the behaviour of their peers. They build their security attitudes and set their own security behaviour according to:

i. The values and attitudes demonstrated in the behaviour of senior managers.
ii. The consistency between the companies' stated values and the evident behaviour of their peers.
iii. Whether other company practices, e.g. HR, reflect its security values.
iv. Whether the company demonstrates that good security practices are important through a system that monitors security behaviours, rewards good and punishes bad.

Users' security common sense and decision making skills are seen over a period of time. Each person builds his own personal history of security decisions according to the feedback received.

The factors that influence the user's personal willingness to constrain his behaviour within these norms and his willingness to conform are affected by personal values and standards; the users own sense of obligation and the difficulty in complying.

Most employees believe in the high value of principles and agree to shared values and sensible rules. Tensions arise when there is conflict between individual values and company values. Employees feel a psychological pressure to behave according to company expectations, to limit their behaviour willingly and to stay within the bounds of accepted practice. If a member of staff feels that he is well treated, recognized and rewarded, then he will gladly respond in kind and act in the company's best interests. Another factor is whether the company makes it easy to

comply with its standards and procedures and whether there are temptations of personal gain for people who do not comply. Even when staff recognize that security controls are implemented for good reasons, they have very little tolerance for controls that are not effective, efficient or clear. The author identified the following keys to better security behaviour:

(a) Behaviours demonstrated by others - What people see in practice around them influences their attitude and behaviour more powerfully than what they are told.

(b) User's security common sense and decision making skills - A user's own security decisions, once made, become a part of his personal body of knowledge and are carried into the future.

(c) User's psychological contract with their employers - If a company ensures that its overt behaviour supports rather than opposes its body of knowledge, and it helps staff to develop and strengthen their security common sense, it will reduce the number and seriousness of users' security errors.

Rotvold (2008) conducted a study to discover the current state of security training within organizations by surveying 144 organizations of different sizes. Sixty percent of the organizations surveyed reported that their organizations offered security awareness training. Of these, 44.7% reported that training was mandatory and attendance was tracked 72.8% of the time. Given these reported numbers, the actual percentage of employees receiving security awareness training may have been quite low. Training was most frequently offered once a year (45%) and the training was conducted by IT staff 58% of the time, followed by management, which conducted the training 28% of the time. The top delivery methods for security awareness training

were face-to-face sessions (54%), e-mail messages (53%), online training (47%), presentations (32%), newsletters (29%), and posters/flyers (28%). The most common general topic in information security training was security policy. The top training topics were "acceptable use (89%), e-mail (85%), passwords (78%), backup and recovery (71%), antivirus (70%), software installation and licensing (67%) and disaster recovery (58.2%)".

A study of the effectiveness of user awareness and training on cybersecurity matters in Australia found that "information security awareness programmes and campaigns can work to embed a collective culture of personal belief system that promotes compliance with computer security policies, procedures and protocols" (Nigel and Rice, 2011). It is this "personal belief" that Liedtka (2000) calls "behavioural process" which is the internalization of the cognitive process that leads to the increase in awareness and attitude changes needed for addressing the information security issues raised. This "personal belief" shift can be effective only where the strategic planning approach applies both the "cognitive process" that creates a "gap" or awareness of the present status and the future expected status of the cybersecurity situation of the firm. The first part will be a "top-down" push of information security which begins with a proper regulatory framework, progresses to executive decisions that create proper information security policies for the firm and ends with user awareness that brings about the desired "personal belief" shift in the user. These components work together to create enhanced protection from cyber-crimes.

Meanwhile Abawajy (2014) emphasizes that as the number and frequency increase of cyberattacks designed to take advantage of unsuspecting personnel, the significance of the human factor in information security management should not be

underestimated. Therefore, information security awareness programmes geared towards human related vulnerabilities are of paramount importance. His study analyses the effects of various methods of information security awareness, training and delivery used to improve end users' awareness of cyber and information security related issues by looking critically at such methods as web based training material and other training, with a major focus on determining the method most preferred by the end users. Further analysis was put into text based, game based and video based delivery schemes to determine user preferences. The study findings reveal that a combination of such methods would yield greater results and it was stressed that state of the art technology based security solutions alone would not provide overall enough security measures to defend critical organization assets from a wide range of ever changing security threats. Managing the human side of information security should be just as carefully done as the technical side. Therefore, reducing human related security vulnerabilities is of paramount importance to the organization's IT security posture.

Abawajy (2014) analyses several other delivery methods, which include electronic resources and paper resources, instructor led delivery methods that involve formal presentations, seminars and workshops facilitated by government, local and external parties, online delivery methods such as email broadcasting, blogging, simulation based and multimedia techniques, among others. The survey reveals that only 5% preferred the game method, 50% preferred video based delivery methods while 33% preferred the text based model of delivery. The drawback is that most of the respondents preferred the video delivery of data followed by text based data transfer. Video data delivery consumes most of the bandwidth and could cause a major blow in case of cyberattacks as indicated by Figure 4 below.

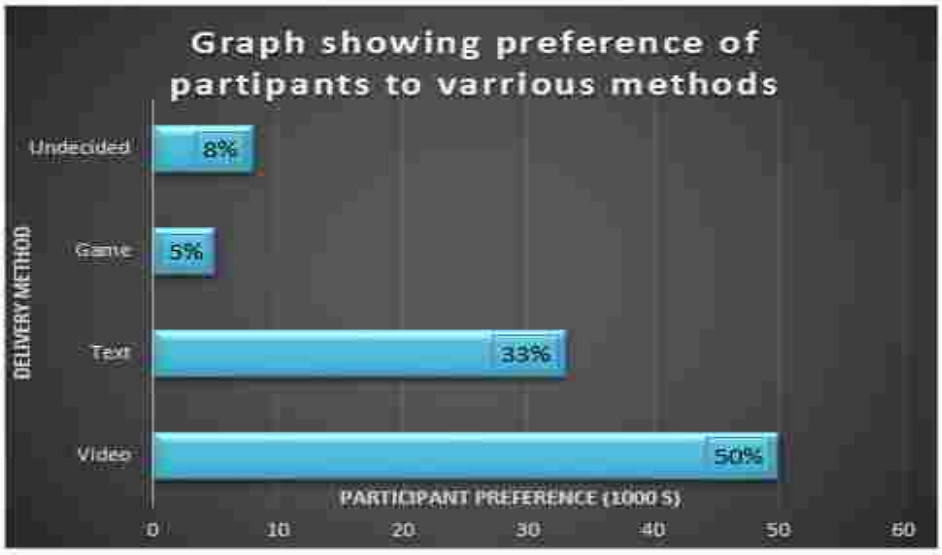


Figure 4: Information Delivery Techniques. Source: Abawajy (2014)

Other work was conducted by (Knapp, 2009), who identified the correlation between user information security awareness programmes and perceived security effectiveness. Their findings reveal that programmes need to make all the employees of an organization share responsibility for the security of information and information systems. Employees need to understand their responsibilities, organizational policies and procedures to protect a government organization's critical assets. Abawajy (2014) though agreeing with this claim also stresses that security awareness training provides the most cost effective method for handling cybersecurity issues globally. Since employees are the weakest point in any security programme, organizations should design appropriate cybersecurity training and awareness programmes for their employees to ensure the effectiveness of the available security defences and technologies.

2.7.3 Results of Effective Training Programmes

Evidence has been provided in the literature for the importance of user training and awareness, together with other factors for cybersecurity effectiveness. An organization may have implemented the best technology and supported it by the most experienced technical team, but without effective user awareness and training programmes, its cybersecurity defences may still fail. The actions of a single user can compromise the data and infrastructure of the entire organization. A successful user training and awareness programme is said to comprise the following results and traits:

(a) Users who are committed to the use of strong passwords as a matter of routine.

(b) Users who exhibit behaviour and attitudes which are aligned to the organization's overall cybersecurity policies, procedures and guidelines.

(c) Users who possess general common sense in their security behaviour. For example, they do not open email attachments with an executable file; they back up their important files with a predefined routine schedule; they connect personal devices such as smartphones, mobile phones and other electronic devices to corporate networks; they do not email a highly sensitive document outside the organization.

From these arguments, the following hypothesis is formulated: *H4: There is a positive relationship between cybersecurity training of staff and cybersecurity effectiveness.*

Next we discuss how strategic planning contributes to an effective cybersecurity programme.

2.8 Strategic Planning and Cybersecurity Effectiveness (H5)

2.8.1 Strategic Management Theories and Principles

Several statistical studies reveal a positive association between strategic planning and organizational performance. For instance Brews and Purohit argue that the degree of instability of the environment increases the amount of planning a firm does. They infer that "planning increases as instability increases" (Brews and Purohit, 2007). The rapid increase of cyber-criminal activities worldwide presents a kind of "unstable" environment which requires strategic planning (Grant, 2003). Such instability in cyber-crime is assumed because attackers who commit cybercrime can be anywhere in the world when their actions cause damage to an organization's information and communication infrastructure (Rees, 2011). An organization's ability to deal with such attacks requires flexibility and the capacity to respond quickly to rapidly changing situations. Therefore, Abu Dhabi's government entities need to take proactive measures to protect critical infrastructure from such illegal activities speedily. The organizations that would prevent the effects of cyber-crime and malware attacks are those that "anticipate and address environmental turbulence through strategic planning" (Rudd, 2008).

Given that the situations where most businesses and government entities face many noticeable threats such as cyber and information security attacks on critical national infrastructure, it has become necessary for entrepreneurs, top management and the UAE government to dedicate greater effort and research to the explanation and choice of the most adequate strategies and security frameworks. Doing so would help respond to such critical challenges and ensure improved security thus making investment in the region more competitive and the entire government safer. In the

effort to construct robust and effective security frameworks and clear strategies, we need to analyze and reason out many important issues.

Since cyberattacks can seriously disrupt or even paralyze segments of critical infrastructure, governments including that of Abu Dhabi need to devise strategies to combat their effects. This can be achieved through appropriate strategic management theories and the application of principles or frameworks that guide the control and prevention of these attacks. According to Finland's Cybersecurity Strategic Report (2013) government entities should mobilise the highest level of cybersecurity management to provide political guidance and strategic guidelines. The authors of this report argue that cybersecurity management represents strategic sensitivity, collective commitment and resource flexibility from a government. They further reveal that in order to prevent cyber threats that could endanger the security of the state, it is important to review legislative restrictions as well as those arising from international obligations. Such obstacles include obligations related to data protection, disclosure and the exchange of information between authorities by paying more attention to the basic rights of privacy, confidentiality and the integrity of electronic communications. They also propose an annual review of cybersecurity strategies by security committees but they provide no insight into the best management principles and practices for performing such a review. Our hope is that the findings of this thesis will contribute to the best management principles and practices for reviewing cybersecurity policies and strategies periodically by the UAE Government entities and Abu Dhabi's government in particular.

Elbanna (2010) provides a detailed discussion of strategic planning in the UAE. He focuses mainly on the importance of Strategic Planning to departments in the public and private sectors and the development of a profile of organizations in the

UAE with respect to their practices of strategic planning and management. However, he does not consider the inclusion of cybersecurity threats in the strategic planning and policy making topics. This creates a gap that we need to fill with the findings of this study. Furthermore, Lydon (2013) claims that cyberattacks on industrial operations have become of great concern, although industry management increasingly demands real-time communication between automation and business systems. From this submission, the requirement for robust management systems and theories to shield these important systems from the cyberspace enemies becomes important.

At the 4th Cybersecurity framework workshop, held in September 2013 at the University of Texas, Dallas, it was agreed that an organization's management of cyber-risks required a major focus on key functions such as "Know", "Protect", "Detect", "Respond" and "Recover" as a major practice to combat cybercrime. Their framework from the contributors recommended incentives such as cybersecurity insurance, and grants for public recognition and cybersecurity research. The European Network and Information Security Agency report (ENISA, 2012) notes that several member states have developed cybersecurity strategies while others had brought their strategies close to publication. Some of the completed frameworks identified by the reports include Estonia, Finland and Slovakia in 2008.

The strategy guides the procedure for protecting critical information structures. It explores existing regulations to clarify whether and where any additional powers are required to secure IT systems. For instance, to mention Germany alone, it provides basic security functions certified by the state and also supports SMEs by setting up a new task force, among several other reported initiatives.

Gercke (2014) makes a detailed report on cybercrime to guide both developed and developing nations towards the co-ordination of national legal frameworks and an appreciation of the growing cyber threat to the stability of the state. He provides detailed information on the way in which crimes are committed and the activities undertaken by International and regional organizations in fighting them. This report contains a detailed analysis of the legal approaches, procedure laws, digital evidence and the responsibility of the Internet providers, as stated in the ITU Global Cybersecurity Agenda (GCA). The author focuses on strengthening international cooperation in the fight against cybercrime, coordinating financial support for training activities, the organization of meetings of law enforcement experts, strengthening dialogue with industry and monitoring the changing threats from cybercrime to evaluate the need for further legislation. Unfortunately the main focus of this entire report was on the United States Government and Europe, leaving out other important regions such as the Middle East. Given that the world economic centres have been moving eastwards, most of the cyber and information security vulnerabilities have shifted largely in the same direction. We therefore focus on the existing cybersecurity defences in the Gulf States while putting major emphasis on Abu Dhabi's government entities, with the aim of filling any existing gaps that may be cited regarding cyber and information security.

According to the latest world internet statistics, the United Arab Emirates reached the tune of 91.9% by the end of 2016 (World Internet Statistics, 2016). This percentage places the country third of all the Middle Eastern countries and seventeenth globally in terms of Internet usage. Furthermore, the report shows that the UAE had the highest rate of smart phone penetration in the world. Such statistics present a major concern to national cybersecurity and require an urgent response

from government, especially in terms of developing frameworks for appropriate prevention of cyber-crime in the region. It is further revealed that UAE government websites were attacked in July 2013, but that this attempt was successfully tackled by the UAE Emergency Response Team (ae-CERT) which managed to minimise the impact of these attacks. At the same time, it reveals a weakness in the existing cybersecurity defences and security strategies in place. Since the government has put more focus on delivering services to all residents mainly through e-government portals, more attention should be given to securing cyberspace, possibly requiring strong cybersecurity frameworks to be prepared for the government entities.

Lydon (2013) argues that, despite the rapid increase in the use of Information and Communication Technologies (ICTs) and the expansion in Internet access, many political, legal and societal aspects of cyberspace have not been fully understood by most governments and military bodies. They show massive dependence on networks which are major sources of vulnerability. The report reveals that many non-state actors in cyberspace, such as politically motivated groups, have expanded to complicate the many government efforts to end cybercrime. The report did not suggest a framework for cybersecurity defences which could be applied by government entities in this fight. In a later section, we review some of the best practices from other countries to develop the best strategy for Abu Dhabi's government entities and ensure the effective implementation of our proposed framework.

This section of the literature review argued that, since cybersecurity issues are issues for management, there must be a relationship between the role of cybersecurity strategic planning and the cybersecurity effectiveness of Abu Dhabi's government entities. We therefore propose the following hypothesis: *H5: There is a*

positive relationship between the presence of cybersecurity strategic plans and cybersecurity effectiveness.

People are the new attack vector for any organization; therefore they need to formulate the first line of defence for any security vulnerabilities. It is not easy for users to be aware of all the potential cyber and information security pitfalls at work. Even if they follow the right security protocols, they usually forget about the simplest targets for cyber intrusion, such as Wi-Fi connected mobile phones, tablets, computers and IT devices of all kinds used to access corporate data. Therefore, continuous user awareness programmes need to be in place to remind employees of their role in ensuring an effective cybersecurity programme for their organization, as discussed further below.

2.9 Role of Cybersecurity User Awareness Programmes (H6)

Employee awareness is a fundamental component of every programme in an organization. This comes down to how organizations engage their employees and generate awareness through appropriate communications programmes. Effective security awareness demands top-down commitment and communication, a tactic that is often lacking in government entities. While information security training and awareness is a minor topic in information security research, it plays a critical role in any organization's defence against cyber-attack. Therefore, as organizations expand their use of advanced security technologies, hackers attempt to break into their security through the organization's weakest security link, the less-informed computer user (Whitmer, 2007). Users are the biggest threat to the IT security of any organization, therefore, continuous cybersecurity awareness programmes must be run to change their perception of cyber and information security. Furthermore, cultural

and attitude changes in the operations of government employees are required to make IT security and the ethical use of IT resources as ubiquitous as technology, since it involves changing the way that employees perceive IT security (Aloul, 2010).

Siponnen (2000) defines information security awareness as "a state where users in an organization are aware of their security mission". A more comprehensive definition is given by (Kritzinger and Smith, 2008) who state that "information security awareness is about ensuring that all employees in an organization are aware of their role and responsibility towards securing the information they work with". Meanwhile, Rezgui and Marks (2008) explore the factors that influenced user security awareness at Zayed University in the United Arab Emirates. Their main intention was to identify how "thoroughness, cultural assumptions, beliefs, and social conditions" affected the way that staff and students behaved towards information security. Overall, the authors infer that while the university placed more emphasis on perceived external threats, there were signs of "lack of information security awareness in the institution indicated by the widespread acts of user errors, software failures, social engineering problems and data leakage problems". They assert that these problems were likely to have had a direct relationship with the lack of information security awareness programmes at the university. As a result of this discussion, we propose the following hypothesis:

H6: *There is a positive relationship between awareness of users about cyber security and cybersecurity effectiveness.*

Next we discuss the importance of legislation in strengthening an organization's cybersecurity programme.

2.10 Regulatory Framework and Cybersecurity Effectiveness

Regulatory frameworks allow the establishment of laws and regulation necessary for ensuring that public and national interests are protected. This is especially important for critical national infrastructure such as major communication lines (e.g. power smart grids, transport systems and public institutions) among others. National laws on privacy, the confidentiality of personal information and data provided to financial, health and government entities can be enforced only by ensuring compliance among departments and nations. In addition, international cooperation is required to effectively deal with cyber and information security problems. For example the European Cybercrime Centre was created in Europe to serve as the continent's information hub on cybercrime through the development of cutting edge digital forensic capabilities that support investigations for the EU and capacity building to fight cybercrime through training, awareness raising and the delivery of best practice on cybercrime investigations.

Regarding the UAE, it was not until 2006 that its Federal Government came up with a law against cybercrime Federal Law No. 2, (2006). This law focused mainly on the prevention of Information Technology Crimes. It came into existence at a time when issues of information security were being recognized as a global threat which required each country to legislate against cybercrime (Al-Bawaba, 2012). The International Convention on Cybercrime, which the UAE law complies with, was established to harmonize cyber-laws among different countries, Council-on-Europe, (2002). In the case of the UAE, Federal Law No. 2, (2006) was amended in 2012 to incorporate measures that support the investigation and prosecution of cybercrimes. The new law criminalizes the use of any information communication

and technology (ICT) tools or the World Wide Web (Internet) to commit an array of crimes, punishable by imprisonment and or a fine from government through the law enforcement departments and the monitoring team. The Articles in the Federal Legal Decree No.5, 2012 on cybercrime covers content, conduct commercialism and contact. Some of the primary offences include breach of privacy, defamation, publication of illegal content, hacking and phishing attacks. Others include identity theft, credit card fraud, and money laundering and threatening national security. It is further reported that the United Arab Emirates government regularly examines the Internet to blacklist all websites that may contain sensitive material such as pornography or child abusive contents, improper religious statements, racial statements, gambling materials, terrorist activities and anti – Islamic statements (Al-Bawaba, 2012; Seibert, 2002).

In the USA laws established following the crash of the giant Enron Company late last century have resulted in executives being held fully responsible for compliance to the laws and regulations that pertain to information security. If a cyber-attack results in the loss and release of private health information, for example, executives must demonstrate that both "due care" and "due diligence" were taken to protect this information, for the failure of which they will be held personally responsible and liable (Nigel and Rice, 2011). It is senior management's responsibility in this country to ensure that their organizations are fully compliant with the UAE Federal Laws on cybersecurity so as to demonstrate "due diligence" and "due care". In this thesis, we ask if existing government entities have incorporated awareness of the federal law in their strategic plans. While these laws form one basis for cybersecurity policies to be established in the corporation, further

steps must be taken to ensure that all employees of the company are aware of the issues surrounding cybersecurity.

The UAE government has also established other agencies to support efforts to prevent cybercrime. The national security awareness campaigns launched in November, 2007 by the ae-CERT to protect citizens and information online and provide an online identity platform tried to safeguard some of the government critical information by blocking most of the immoral and illegal websites from access in the region. This mechanism has temporarily reduced the issue of child abuse and pornography. Furthermore, on 22nd July, 2013 the Telecommunications Regulatory Authority (TRA) successfully defended users from a series of cyberattacks that targeted some government websites. Meanwhile, the Computer Emergency Response Team ae-CERT managed to neutralize the problem with minimal damage. However, popups, phishing attacks, denial of service, ignorance of users about security threats, among others, remain a major challenge that require urgent government intervention.

The Telecommunications Regulatory Authority (TRA) is mandated to implement the Internet Access Management (IAM) policy on behalf of the UAE government by monitoring the online content available to users in the UAE and thereafter to alert the teams for website maintenance and implementation of the traces and possible impact of anything that might create a security vulnerability in any portal. The content proscribed by the IAM policy includes various forms of malicious code and any Internet content relating to terrorist cybercrime, among others. The TRA in its IAM enforcement role monitors advertisements online, including the advertising of medical products and services. The TRA also regulates the services of the major telecommunication operators in the UAE who are licensed to provide users with access to the Internet. This is done through appropriate

licensing clauses aimed at blocking online content that might be regarded as offensive or show traces of malicious codes. A widely reported example of such incidents was in 2009, when the TRA banned access to a cartoon clip on YouTube which was alleged to contravene religious and nationalist sentiments.

Another agency that was recently established to oversee electronic security is the National Electronic Security Authority (NESA). NESA is a federal authority responsible for developing, supervising and monitoring the implementation of cybersecurity in the UAE's strategies, policies and standards. Their major role is to safeguard the UAE online environment and contribute to the collective achievement of national goals. It is committed to ensuring that all UAE government bodies are made fully aware of their responsibility to meet the requirements of the stated polices of national interest. The regulation establishing this agency is Federal Law No. 3, 2012, also known as the E-Security Authority Law, which was created as a further reinforcement to the Federal Legal Decree No. 2, 2006 on cybercrimes and other regulations and programmes, including the establishment of the UAE Computer Emergency Response Team (aeCERT) and various public awareness campaigns in the region (Lydon, 2013).

The UAE government through support departments such as NESA has also established special cyber-crime units to confront cybercrime in and beyond its territorial jurisdiction. Furthermore, the government established dedicated police departments committed to solving high-technology crime in the UAE. Other measures taken to challenge cyber-crime in both public and private sectors include but are not limited to public awareness and the adoption of common agreements with other countries, especially the GCC member countries, the European Union and the

United States. If the cybersecurity problem is to be solved across Abu Dhabi's government entities, strict legal action against any form of malicious threat or crack in information security should be implemented by the government authorities concerned. In addition to regulation, there is a need to ensure that appropriate cyber and information security frameworks are in place to help the government to implement policies across various departments in the Emirate of Abu Dhabi.

Even with these new agencies and regulations, in the present technological and social atmosphere, the UAE has suffered numerous challenges in the process of striving to fight its cyber and information security problems in the region. One challenge is to determine how cybersecurity investigations should be conducted. Even with the governments' computer law crimes, there are few prosecutions for loss or damage caused by cybercrimes.

Most offenders take advantage of the anonymity of cyberspace to conceal their identity. Moreover, it is challenging to apply these laws effectively in prosecuting cases without deep insight and actual evidence of digital crime. However, the Internet-of-things penetrates beyond territorial borders and so legislators may not have full control over some criminals if they were protected by laws in other territories. Cybercrime investigators need to acquire credible digital evidence so that courts of law can prosecute the perpetrators (Vacca, 2002). A number of models and frameworks exist to allow a choice of strategies for cybersecurity effectiveness and readiness in various organizations. Some of these models are discussed in the next section.

2.11 Existing Cybersecurity Models and Frameworks

This section of the literature review sets the theoretical foundation for proposing a cybersecurity framework. The use of "edge" devices, cloud applications and the increase of regulatory requirements have created a need for most organizations to advance their security frameworks and re-think traditional approaches in order to stay ahead. Organizations need new strategic frameworks to address numerous trends across the IT landscape that will secure data, mobile devices and cloud computing environments, among others. The major challenge is to address disruptive technologies and trends, for example, everything connected with social computing and at the same time manage inherent risks (Burgers et al., 2013; CGI Group Report, 2014).

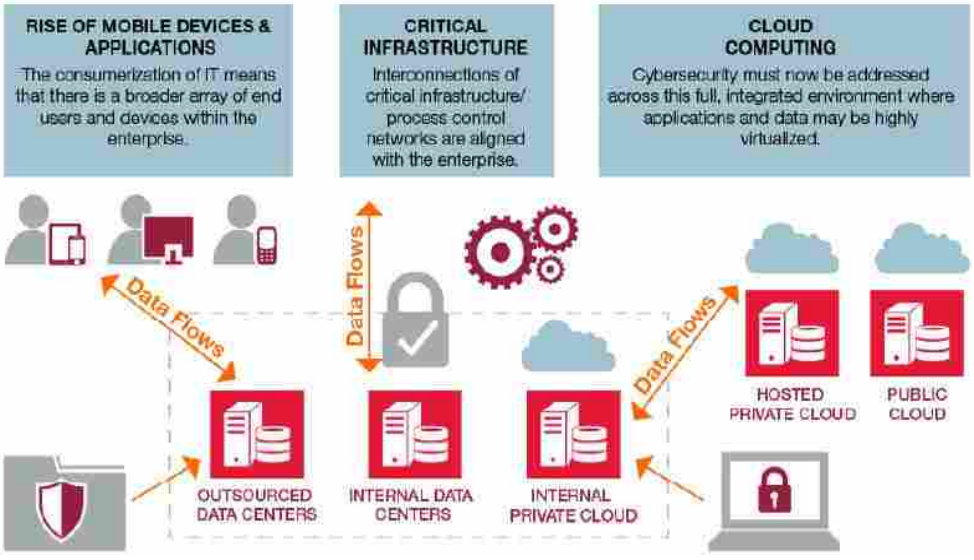


Figure 5: Porous Security Perimeter Source: (Source: CGI Group Report, 2014, page 5)

Figure 5 illustrates an intensively connected IT infrastructure environment, which combines data flows from mobile devices, critical infrastructure and cloud

computing. All these combined deliver sensitive data to internal and outsourced data centres along a common backbone which could be vulnerable to attacks. Such highly connected and distributed network environments require frameworks that provide mechanisms for protecting critical data. This is a typical layout for an interconnected UAE government department that uses the e-government portal to offer services to the public.

Meanwhile, Nambiro et al. (2014) assessed the cybersecurity problem in selected ministries for the Government of Kenya. The authors provide both descriptive and inferential analysis of cybersecurity assessment in a typical government setup. They claim that cyberattacks are highly sophisticated to the extent of troubling many organizations in identifying where the greatest vulnerability lies. They further reveal that Kenya, together with other African governments, lacks its own global networks and is thus very vulnerable to cyberattacks since they have to use communication platforms under the control of external authorities. While this study provided useful insights into the way that IT personnel can respond to cyberattacks, it does not address the problem of dealing with typical users. There is need to put in place an all-embracing model that considers the requirements of different categories of people in a single robust framework for cybersecurity effectiveness. In this dissertation, we develop a cybersecurity framework that considers all users regardless of technical ability.

Their study reveals that 72.1% of the respondents agreed that their organizations did not have secure cybersecurity infrastructure and 62.8% did not conduct risk assessments or IT security audits. They go on to propose a cybersecurity assessment framework based on Karl Pearson correlations between the cybersecurity challenges and cybersecurity state as indicated in Figure 6 below.

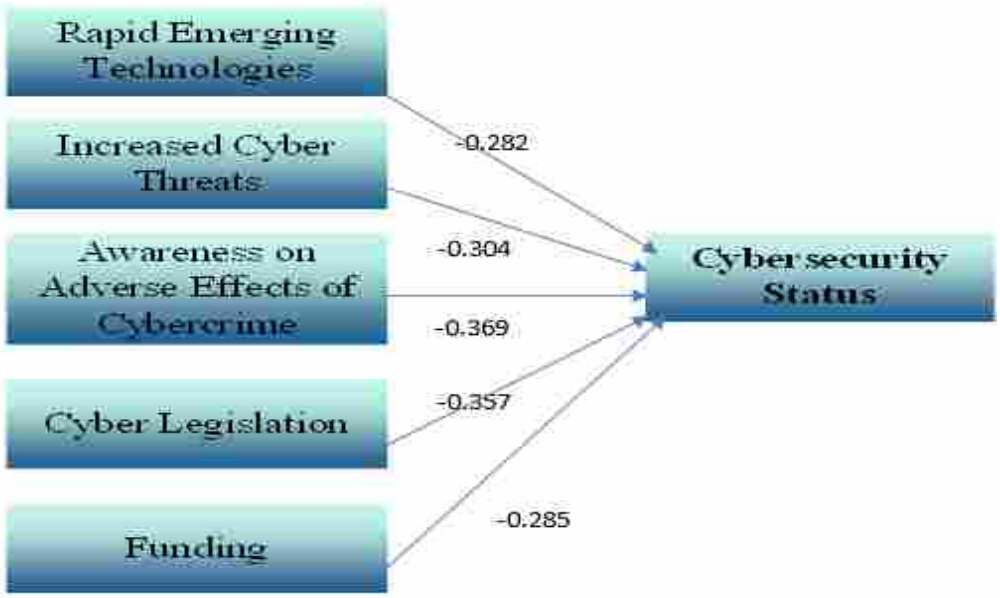


Figure 6: A Framework for Assessing Cybersecurity Challenges

Results from their study reveal that lack of awareness of cyber and information security issues formed the greatest threat to the effectiveness of cybersecurity in many organizations and government entities. This was followed by insufficient cybersecurity legislation, inadequate funding and hastily changed technologies all informing the cybersecurity status of the organization. The authors argue that so long as cybersecurity frameworks fail to emphasize adequate legislation as well as cybersecurity training and awareness, organizations or government entities will be highly vulnerable to different forms of attacks (Nambiro et al., 2014). The cybersecurity assessment framework above proposed for the Kenyan Government may be applicable as well to the UAE government in prioritizing and emphasising the most urgent security issues across the Emirates. This would provide a sense of direction to government planners and legislators when they allocate resources and compile the government security budget across all departments.

As already addressed elsewhere in this thesis, it should be noted that the application of strategic management tools to prepare for and respond to uncertainties resulting from cybersecurity risks against UAE government entities also raises awareness of the risks. These then lead to actions being taken organizationally to prevent such attacks. Furthermore, cybersecurity attacks are usually against critical national infrastructure, implying that senior management has the responsibility of demonstrating both “due care” and “due diligence” as established in Federal Law No. 2, 2012 (Al Bawaba, 2012).

Abraham and Nair (2015) also developed a predictive framework for cybersecurity analytics by applying an attack graph mechanism. Their main aim was to incorporate informed risk-management decision taking in the dynamic attributes associated with vulnerabilities that might change over time. They assert that the most challenging issues regarding security in government systems is their failure to develop mechanisms to combine the security of all systems in a network in order to assess the overall security of the interconnected network. In their study, they point out situational awareness as a universal concept needed to provide organizations with the ability to identify, comprehend and forecast the integral features of a system. They propose a situational awareness model below to address this concern as illustrated in Figure 7 below.

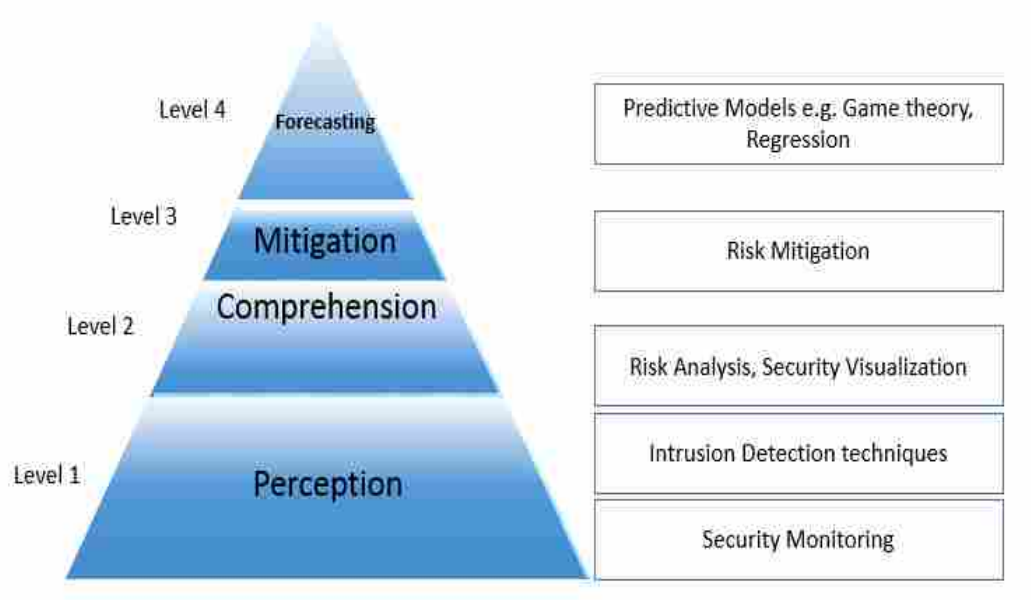


Figure 7: Cybersecurity Situational Awareness Model. (Source: Abraham and Nair, 2015)

The situational awareness model proposed in Figure 7 above splits the cybersecurity problem into four major levels (Levels 1-4). The illustration on the left represents a specific action that could be performed after a cybersecurity incident while the table on the right suggests technological strategies which could be applied to each level. For instance, Level-1 deals with the identification and interpretation of cyberattacks through the application of intrusion detection techniques and other security monitoring tools; Level-2 deals with techniques to understand and analyse the cybersecurity problems through the application of security visualization tools and risk assessment techniques; Level-3 considers mitigation of the cybersecurity risks once the problems emerge. Finally, Level-4 forecasts incidents by using predictive models that suggest appropriate corrective and preventive actions by management and higher authorities in different organizations. This situational awareness model may also be useful to the Abu Dhabi's government entities.

Previous studies show that attackers have radically reviewed their approaches and therefore developed ways of exploiting the vulnerabilities of most recent technological innovations through “Zero day” attacks. As a benchmark, governments need to put in place security teams to focus on activities beyond the expected or predefined. It is also important to deploy mechanisms for predicting vulnerability trends and all forms of anticipated security gaps through stochastic models and observing the life cycles of attacks (Bass, 2000).

Other work on situational awareness reveals that situational awareness plays a major role in an organization’s decision making process. For instance, Evangelopoulou et al. (2014) analysed the safety techniques of applications to the networking environment by concentrating on network Intrusion Detection Systems and the human factors involved. The proposed three levels in situational awareness are Perception, Comprehension (to give a more comprehensive picture of what is happening by combining existing knowledge and new information) and Projection (which deals with the ability to make predictions based on knowledge assimilated). Other factors that may influence situational awareness such as experience and knowledge were also looked into. These writers add that efficiency, safety and security are the primary goals in this regard, causing a need for situational awareness measurement. Some of the most commonly used situational awareness techniques identified are Situational Awareness Global Assessment Techniques (SAGAT); the use of Simulations, Situational Awareness Rating methods (SART); the use of Rating Scales (1 – 7) and a Situation Present Awareness Model (SPAM). Such situation awareness techniques can be applied to Abu Dhabi’s government entities to assess how far people understand the cybersecurity situation. If more people

understood this, they would be ready to provide the correct responses to the cyber and information security challenges affecting their organizations.

Situational awareness techniques may also aid the participants in evaluating their situational awareness level and therefore increasing the quality of service (Ahn et al., 2013). For instance, Simulators can be used in the aviation industry and practices to measure the awareness levels of flight captains; or health informatics for training and evaluating medical practitioners, among others. Similar techniques can be applied to Abu Dhabi's government entities to evaluate the readiness of the trained cyber and information security professionals in cases of cyber incidents occurring, to enable them to take preventive and corrective action. Furthermore, the situational techniques can be implemented for cyberattacks by using receiver operated characteristic analysis, based on recognition of an attack, faulty perception of a current attack and the perception of no attack.

The National Institute of Standards and Technology (NIST) developed a voluntary risk-based cybersecurity framework which involves a set of industry standards and a set of best practices to help organizations manage cybersecurity risks. The subsequent framework was created through collaboration between the government and the private sector and uses a common language to address and manage cybersecurity risk. This is done in a cost-effective way based on business needs but without placing additional regulatory requirements on businesses. Its major focus is on business drivers of cybersecurity activities and it considers cybersecurity risk as within the organization's risk assessment process. In the present study, we incorporate some of these good practices in the NIST framework and several other frameworks globally, as discussed in the literature, in order to formulate a framework for evaluating cybersecurity effectiveness in Abu Dhabi's government entities. The

framework for critical infrastructure support was released in February, 2014 after President Obama's Executive order 13636 of 2013 to formulate a framework that harmonizes consensus and standard industry best practices to provide a flexible and cost effective approach to enhancing cybersecurity and assist business owners or operators to manage cybersecurity risks (Shackelford et al., 2014).

The fact that cyberattacks can seriously disrupt or even paralyze segments of critical national infrastructure implies that an offensive posture or action is required to confront the many forms of cyber and malware attack. Furthermore, appropriate strategic management theories and principles are needed to guide the control and prevention of these attacks (NIST, 2014). To this end, we have analysed the risk management process in a typical organization from executive, business and implementation levels through a life cycle assessment, as shown in the Figure 8 below:

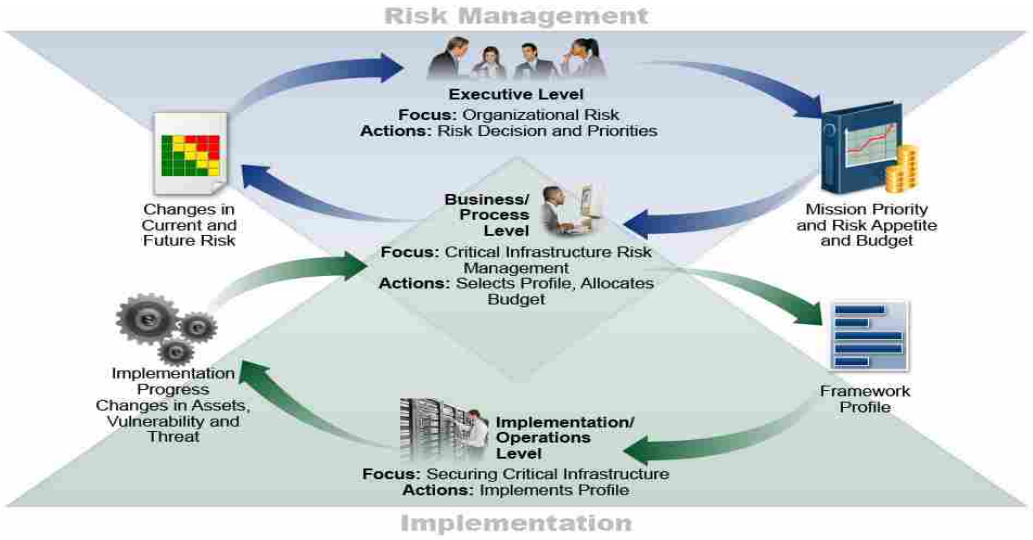


Figure 8: Decision Flows in an Organization. (Source: NIST (2014) Framework Report)

The decision flows presented in Figure 8 above show that the executive level staff communicates priorities, available resources and overall risk tolerance to the business/process level. The business / process level inputs this information into the risk management process and then collaborates with the implementation or operations level to communicate the business's needs and create a profile. The implementation or operations level in return communicates the progress of profile implementation to the business/process level. Meanwhile, the business/process level uses this information to perform an impact assessment. Therefore, understanding cybersecurity risks presents management with an opportunity to make informed decisions and devise relevant corrective and preventive actions for the entire organization. Several authors have advocated inclusion of the NIST technology framework in cybersecurity strategies due to its technological capabilities and risk based approach to information security, as detailed in the next section.

2.11.1 NIST Technology Framework and Cybersecurity Effectiveness

Shen (2014) reveals that the NIST framework is flexible, technologically neutral and can be used by organizations of any size, level of sophistication or degree of cyber risk. The author adds that the framework is based on Tiers separated from the core to provide organizations with a means of ranking their own cybersecurity management practices. The Tiers range from Tier1 (Partial) to Tier 4 (Adaptive), representing increasing levels of rigour and sophistication in an organization's cybersecurity practices. It is claimed that organizations can use the framework to provide a basic review of their cybersecurity practices by comparing their present cybersecurity activities with those outlined in the core of the framework; this will allow the establishment or improvement of the existing cybersecurity programme.

For instance, they can create a current and target profile, communicate cybersecurity requirements with stakeholders through a common language and identify opportunities to revise or create new standards, guidelines and practices. Thus, the framework is applicable to legislation, contracts, insurance and litigation.

Furthermore, the framework is voluntary and was published as a living document to allow updates and reviews globally with the aim of improving it to keep pace with ever changing technology, threats and environmental needs. In this study, we integrate this framework with additional strategies to generate a new frame for Abu Dhabi's government entities. The NIST technology framework is illustrated in the Figure 9 below.

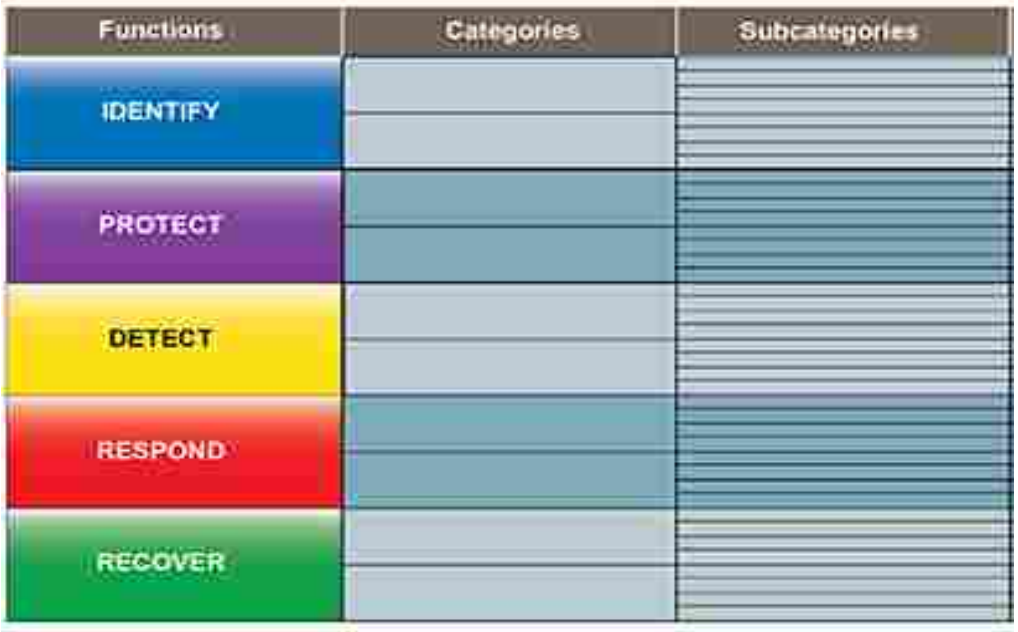


Figure 9: NIST Technology Framework, Source NIST, (2014)

Figure 9 above shows the NIST technological framework proposed to resolve cyber threats through identification, protection, detection, response and recovery from cyberattacks. For instance Shackelford et al. (2014) affirms that the NIST Framework harmonizes industry best practices by providing a flexible and cost

effective approach to enhancing and assessing the cybersecurity of an organization by providing five key functions, namely, (i) Identify (What assets need protection?) (ii) Protect (What safeguards are available?) (iii) Detect (What techniques can identify incidents?) (iv) Respond (What techniques can contain the impact of incidents?) (v) Recover (What techniques can restore capabilities?) as illustrated in Figure 9 above. The framework further provides implementation tiers to illustrate how organizations can manage cybersecurity risks in their enterprise risk management practices,

The NIST framework is not a checkbox compliance exercise but a result of work conducted by over three thousand (3000) business leaders and IT experts over a period of two years with the aim of securing critical infrastructure as compared to high existing standard such as COBIT, SAS, COSO and ISO 27001. Furthermore, Ola (2015) emphasizes that every Small and Medium-sized Business (SMB) needs to use the NIST cybersecurity framework, since it allows organizations to assess risks based on industry best standards and practices, which helps them prioritise cyber investment decisions and their management of cyber risks. They stress that C-level management must participate and take a central role in identifying cyber risk. Additionally, the (Price, 2014) report shows that the framework offers potential advances to organizations across industries by offering voluntary guidelines for taking a risk-based approach to cybersecurity. They could proceed by integrating leading industry practices developed by internationally prominent bodies such as the ISO and offering benefits beyond improved cybersecurity for example, effective collaboration and the communication of security posture with executives to improve cybersecurity practices and threat intelligence. Therefore, if organizations adopt the NIST framework at the highest possible risk tolerance level, they would be better

positioned to comply with cyber and privacy regulations. It is therefore evident that integration of the NIST cybersecurity framework with the additional strategies proposed in the present study would provide a stronger platform from which to evaluate the cybersecurity effectiveness of the Abu Dhabi's government entities.

Teodore et al. (2015) reveals that the NIST technology framework provides a platform for evaluating critical infrastructure and predicting cybersecurity risks by providing a set of core activities required for implementation. They assert that human resources, processes and technology form a major pillar supporting an organization's cybersecurity. However, the authors also reveal some drawbacks to the framework: the failure to provide a standard reference for organizations to follow and the concealed cybersecurity maturity gaps in for example employee skills, among others, may hinder its effectiveness.

The researcher hopes that proposing a new framework that incorporates key factors proposed in this study like cybersecurity training, cybersecurity awareness, the role of management, laws and regulations, qualifications of the information security staff and experience of users, among others, would yield a stronger framework for assessing cybersecurity effectiveness in Abu Dhabi's government entities.

It is revealed that, even if the cited incentives in the use of the framework existed, their effectiveness in improving critical infrastructure cybersecurity would need continuous refinement with future versions integrating new strategies such as legal requirements and the government's role. The cybersecurity framework proposed in this research draws from other frameworks and models reviewed in literature such as NIST in addition to several factors to contribute a new framework for evaluating cybersecurity effectiveness of Abu Dhabi government entities. The

framework does not consider human and organizational factors like, culturally sensitive training and user awareness programmes, support from senior management, presence of experienced and competent staff and modern technological countermeasures all in an updated framework coupled by the use of strategic management tools to create conditions for enhanced information security across the different entities. Therefore, the study intends to strengthen the human and organizational factors discussed in literature together with the risk based technological strategies proposed in the NIST (2014) technology platform to formulate a strong framework and checklist for evaluating cybersecurity effectiveness of Abu Dhabi government entities. Meanwhile, the International Organization for Standardization (ISO), the International Electro technical Commission (IEC) and the UAE's National Electronics Security Authority (NESA) in collaboration with the Abu Dhabi Systems and Information Centre (ADSIC) proposed more standards with several strategies for evaluating cyber and information security status in organizations as briefly discussed in the next sections.

2.11.2 The ISO 27000 Information Security Management Standards

The ISO 27000 family of standards offers a set of specifications, code of conduct and best practice for organizations to ensure strong IT service management. It includes standards like ISO/IEC 27001: ISMS which offers specifications for an effective Information Security Management System, ISO/IEC 27002, which provides the code of conduct and the recommended best practice by detailing 114 security controls organized into 14 sectors and 35 control objectives as well as the ISO/IEC 27005 which provides guidelines for Risk Management. These standards were developed by the joint committee of the International Organization for

Standardization (ISO) and the International Electro-technical Commission (IEC) with the objective of defining requirements for successful ISMS delivery through a process based approach by Establishing, Implementing, Monitoring and Maintenance of an ISMS grounded on a Plan Do Check Act (PDCA) model. However, many organizations lack mature management systems with little knowledge on Information security governance and evaluation of existing mechanisms coupled with the lack of skilled resources to conduct risk analysis to enable the implementation as well as maintenance of strong Information Security Management System justifying the need for a simpler framework to address such concerns. Further, the ISO 27001 standard allows organizations to explicitly asses their internal processes with a major aim of presenting to International bodies for certification. This approach implies that organizations focus mainly on jumping the bar for international competitiveness ignoring performance evaluation of their internal cybersecurity systems by limiting the scope to operational standardisation of those well performing functional units other than evaluating the strength of their organization-wide Cyber and Information security defences, policies and frameworks with senior Management taking a lead. This is a major focus of this study research theoretical framework were the research proposes a simpler framework that Abu Dhabi government entities can embark on to evaluate and address the missing link in the performance of cybersecurity systems. In the next section we briefly discuss the ADSIC II and NESA information security framework guidelines in comparison to this study.

2.11.3 The UAE National Electronics Security Authority (NESA) Standards

The UAE Federal Law No. 3 and No. 5 of 2012, established the National Electronic Security Agency (NESA) as a federal body tasked with protecting the

UAE's national critical infrastructure and improving National Cybersecurity through development of standards, policies and suggestive legislation as well as guidelines for securing digital data in all critical sectors of the UAE economy. These standards were developed with a benchmark on major International standards for information security like the NIST (2014) Special Publication 800-53: recommended security controls for federal information systems & organizations, ISO/IEC 27001: ISMS and ISO/IEC 27002 code of practice for information security management. Compliance to these standards is mandatory and is determined by ADSIC whose primary responsibility is to check compliance to the standards by all government entities in the emirate of Abu Dhabi.

NESA's threat based approach to information security is managed by mapping controls to the 24 most recent threats gathered from industry reports since 2012, Alqatawna (2014). Controls in the framework were ranked as P1 representing the highest to P4 representing lowest impact with definitions for both Management and Technical oriented controls across 12 domains as shown in Figure 10 below.

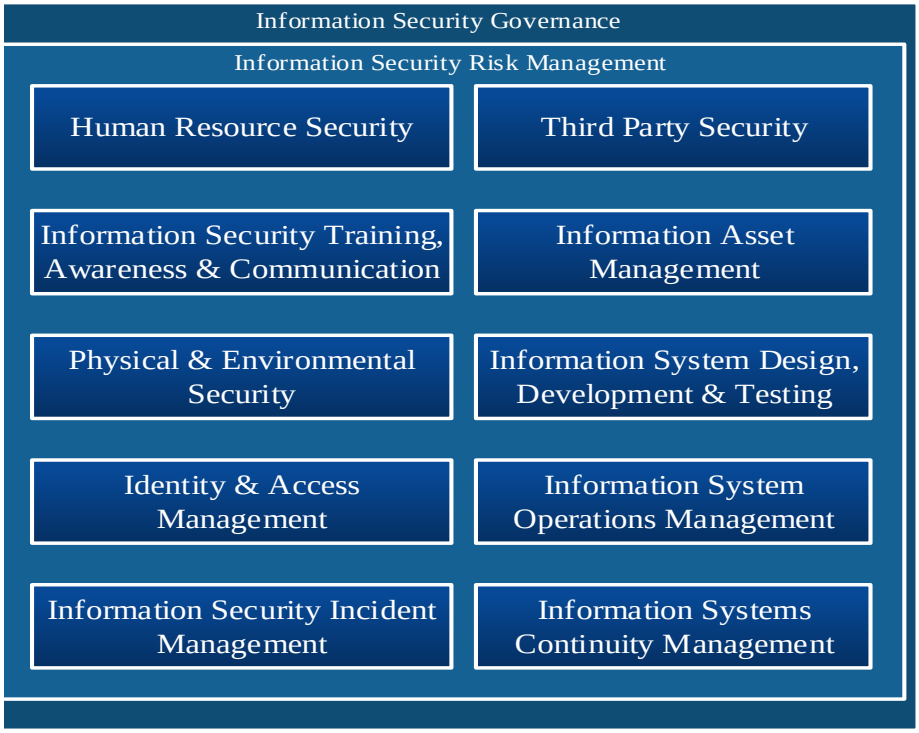


Figure 10: NESA Information Security Standard
Source: ADSIC standards Ver 2.0, Page 5

From Figure 10 above, the NESA framework on information security incorporates a domain on Awareness, Training and Communication of information security issues to all stakeholders and emphasizes the recruitment of well qualified Information security professionals to the level of CISO in every government entity. This is in support of this study, however, the checklist developed by ADSIC to implement the proposed framework in Figure 10 is very long and rather complex the 12 domain controls distributed on over 300 pages which makes it very difficult for organizations to implement or quickly asses their cybersecurity systems and provides little input towards evaluating relationships between competence of staff, role of management, level of technology and strategic planning as compared to cybersecurity effectiveness of Abu Dhabi's government entities. This study is intended to bridge this gap by contributing a simplified framework and checklist

specifically for assessing the effectiveness of organization wide cybersecurity systems for Abu Dhabi government entities.

Meanwhile, the Software Engineering Institute (SEI) at the Carnegie Mellon University developed a model for software development as early as 1980s. This model was named the Capability Maturity Model Integration (CMMI) developed with the aim of formulating a path for improving organizational software development processes. The model was formally published in 2002 as CMMI Ver 1.1. (Dong-Young and Gerald, 2010). The CMMI model is widely applicable to government entities especially when conducting process based assessment for stable and mature improvement. The model provides a framework mainly used in software development and maintenance processes based on actual practices that reflect the needs of individuals performing software process improvement through a hierarchy of five maturity levels that lay successive foundation for continuous process improvement, the maturity levels include; 1) Initial, 2) Managed, 3) Defined, 4) Quantitatively Managed, and 5) Optimizing. These levels are further broken down into several process areas to reflect areas where an organization needs to focus more in case of operational process improvement. This research borrows the five maturity levels from the CMMI model to generate a scoring and measurement technique based on Likert scale (1-5) for assessing and interpreting organizational cybersecurity effectiveness in terms of the six factors identified for organizational cybersecurity effectiveness in Abu Dhabi Government entities. The modified CMMI model applicable for this study is as seen in the Figure 11 below:

Figure 11: Modified Capability Maturity Model Integration (CMMI) Model

The researcher modified the Capability Maturity Model Integration (CMMI) in the Figure 11 above to come up with a measurement and scoring scale which Abu Dhabi government entities can use to verify the level of cybersecurity effectiveness (CSE) in their organizations through which Level 1 indicates that the organization has taken initial steps towards implementing measures that contribute towards CSE; Level 2 indicates that these measures are repeatable and; Level 3 indicates that these CSE measures are defined and can be referenced, Level 4 shows that the organization has a well-managed CSE operations while the highest level of CSE in an organization is Level 5 which will demonstrate the department has fully complied with all the factors for cybersecurity effectiveness.

From the above discussions, the researcher has identified several factors and strategies for ensuring an effective cybersecurity system. Based on that, the following hypotheses are proposed for this study:

2.12 Research Hypotheses

H1: *There is a positive relationship between the competence/knowledge of staff and cybersecurity effectiveness.*

H2: *There is a positive relationship between senior management support and cybersecurity effectiveness.*

H3: *There is a positive relationship between level of technology and cybersecurity effectiveness*

H4: *There is a positive relationship between cybersecurity training of staff and cybersecurity effectiveness.*

H5: *There is a positive relationship between the presence of cybersecurity strategic plans and cybersecurity effectiveness*

H6: *There is a positive relationship between awareness of users about cyber security and cybersecurity effectiveness*

Furthermore, the researcher has identified and responded to several issues and problems hindering the effectiveness of organization's cybersecurity programmes. These problems are presented in the research gap illustrated in the next section.

2.13 Research Gap

Several cyber and information security frameworks and models reviewed in literature, provide detailed insights into the research problem and the techniques for combating existing information security challenges wherever they occur. For instance, Nambiro et al. (2014) proposes a cybersecurity status assessment framework for government ministries in a developing country by applying Karl

Pearson correlation coefficients. However, implementation details for this framework provide no clear description of its defence capability. While the NIST (2014) Technological Framework has been highly rated, particularly for providing appropriate technological cybersecurity defences to organizations globally (Shackelford et al., 2015; Teodoro et al., 2015; Price, 2014; Sage, 2015; Hiller and Russell, 2015; and among others) it fails to include other important factors to ensure a strong cybersecurity evaluation system. The framework presents a technologically centred model whose major focus is on the business drivers of cybersecurity activities and the consideration of cybersecurity risk as part of an organization's risk assessment process. The framework is a risk-based compilation of the guidelines designed to help organizations to assess their current capabilities and draft prioritised roadmaps for improved cybersecurity practices. The authors of the framework had as their major goal the improvement of risk based security, but they did not did not fully address other critical strategies concerning cyber and information security challenges to organizations such as culture sensitive user training and awareness programmes, support from existing laws and regulations, support from senior management and the competence level of information security staff. Even though we agree that the NIST technology framework provides a strong technology centred and risk-based approach through the five key functions (Identify, Protect, Detect, Respond and Recover) the researcher argues that other non-technologically focused strategic factors are very critical for organization's cybersecurity system and therefore cannot be taken lightly when evaluating cybersecurity effectiveness of an organization. The researcher therefore proposes a cybersecurity framework, together with a checklist, that incorporates all these human and organizational factors that are strategically important for cybersecurity effectiveness of Abu Dhabi's government entities.

2.14 Conclusion

In this study, we have critically reviewed the literature concerning the cybersecurity landscape globally, including technologies, strategic planning methodologies and several cybersecurity frameworks and models, together with some strategies for an effective cybersecurity system. Most of the authors concentrate on technological and situational awareness mechanisms for evaluating cybersecurity effectiveness and eliminating associated risks (NIST, 2014; Burgers et al., 2013; Abraham and Nair, 2015; and Nambiro et al., 2014). However, these mechanisms provide little help for the ever-increasing number of uninformed users, analysis of the existing legal framework and its implication for cybersecurity effectiveness or consideration of senior management's role in preventing cyberattacks. We have studied the existing literature on the concept of cybersecurity from a broad perspective through the discussion of several studies and frameworks concerning cybersecurity defences, major attacks on organizations' critical infrastructure, technologies for implementation, and prevention of these attacks, the role of cybersecurity education, and training and awareness. Based on the above discussions in the literature, it is evident that several gaps exist regarding cybersecurity and effectiveness and therefore we propose further investigation and analysis of the phenomenon. In the next chapter we present the methodology used to conduct further research for the study.

Chapter 3: Research Methodology

3.1 Introduction

In this chapter, we present a comprehensive study and the approach taken to the research problem concerning the evaluation of cybersecurity effectiveness in Abu Dhabi's government entities. The principal objective is to discuss how the underlying study has been conducted, how the data were collected, analyzed and validated through reliability statistics. This chapter is presented according to the design illustrated in the flowchart in Figure 12 below:

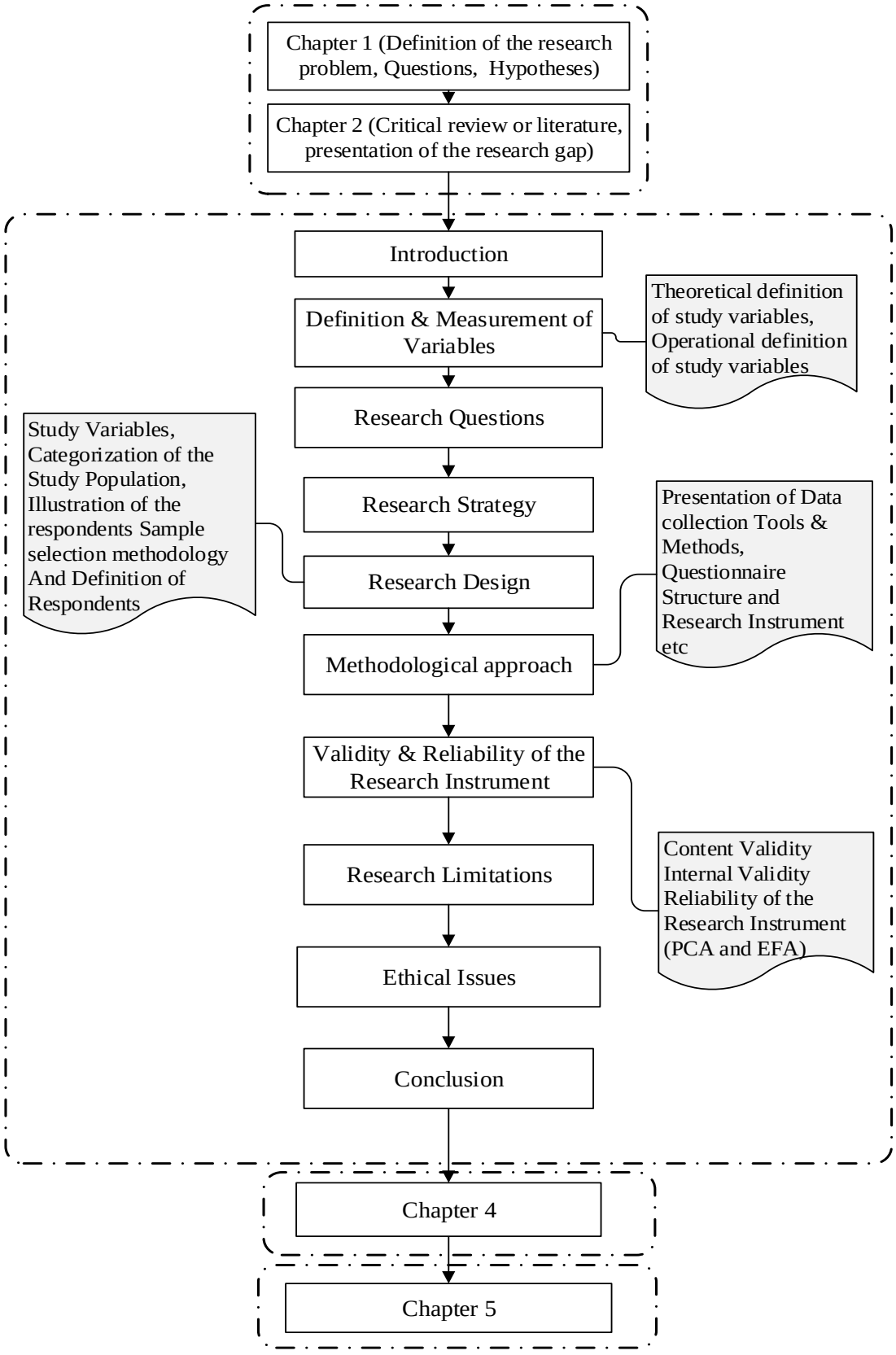


Figure 12: Design of Chapter Three

Well defined theories and frameworks on cybersecurity in the UAE, the GCC and elsewhere were consulted through which a detailed review of related literature was conducted to generate a conceptual model. The following hypotheses were formulated for this study:

H1: *There is a positive relationship between the competence/knowledge of staff and cybersecurity effectiveness.*

H2: *There is a positive relationship between senior management support and cybersecurity effectiveness.*

H3: *There is a positive relationship between level of technology and cybersecurity effectiveness*

H4: *There is a positive relationship between cybersecurity training of staff and cybersecurity effectiveness.*

H5: *There is a positive relationship between the presence of cybersecurity strategic plans and cybersecurity effectiveness*

H6: *There is a positive relationship between awareness of users about cyber security and cybersecurity effectiveness*

From the above hypotheses we formulated a study framework to guide the research process and the analysis of the relationships between variables. The latter, together with the literature review laid a foundation for discussing and formulating a cybersecurity framework which was used to assess the effectiveness of the cybersecurity strategies used by Abu Dhabi's government entities. The formulated study framework can be seen in Figure 13 below:

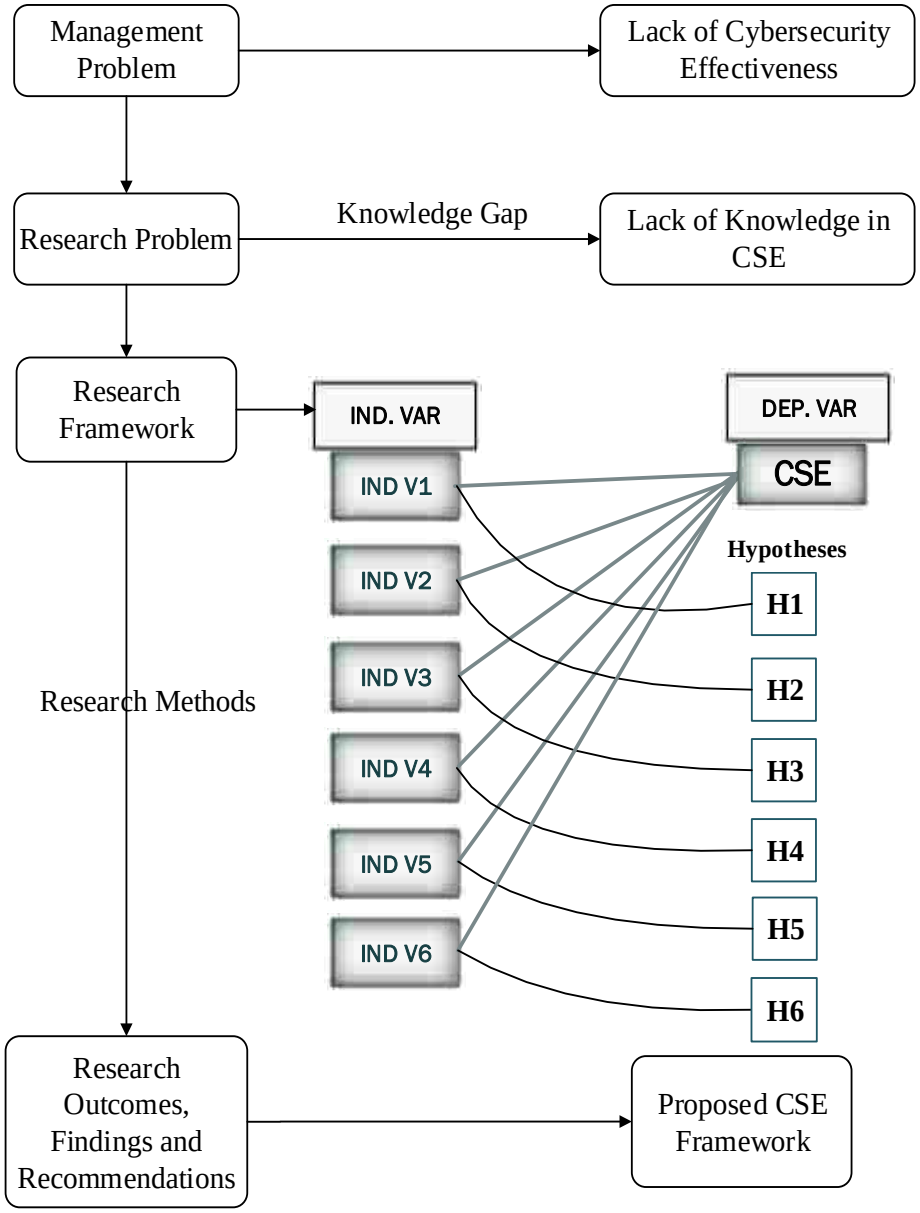


Figure 13: Proposed Study Framework

From Figure 13, the lack of Cybersecurity Effectiveness (CSE) has been identified as the key management problem facing organizations worldwide and Abu Dhabi's government entities in particular. This lack of cybersecurity effectiveness creates a knowledge gap in the organizations and is hence a researchable problem for this study. To fill it, a research framework was formulated, based on a theoretical foundation in the literature upon which a number of independent variables were

formulated against the dependent variable Cybersecurity Effectiveness (CSE). Analysis of these relationships between variables contributed to several outcomes, findings and recommendations including the proposed Integrated Cybersecurity Framework for Abu Dhabi's government entities. The variables used in the study were theoretically and operationally defined to provide an insight into the measurement of variables and our expectations of the study results.

3.2 Definition and Measurement of Variables

In order to guide the analysis of the study all the variables in the study framework and research hypotheses were theoretically and operationally defined with theoretical definitions based on the literature, and operational definitions which were seen from our perspective in analysing and measuring the variables to answer the research questions and deliver appropriate study results. A five point Likert scale was used for measuring responses in this research instrument. Below we define the variables considered in the study:

Independent variable 1 (INDV1): Competence of information security staff

Hypothesis H1. There is a relationship between the Competence/knowledge of staff and cybersecurity effectiveness.

3.2.1 H1 Theoretical Definition

Gilbert (1978) sees "competence" as a combination of practical and theoretical knowledge, cognitive skills, behaviour and values used to improve performance; or as a state of being adequate or well qualified, having the ability to perform a specific role. For instance, management competency may be determined in terms of systems thinking, emotional intelligence and having the skills to influence

or negotiate the highly technical cyber- and information security matters under review. This hypothesis focuses on the qualifications and experience of cyber- or information security staff employed in government entities and the way in which it impacts on their cybersecurity knowledge and skills as well as the effectiveness of their individual departments.

3.2.2 H1 Operational Definition

In this study, we strongly believe that staff with specialized qualifications and considerable amounts of experience (say, > = 5 years) in the cyber- and information security domain in a government department demonstrates more knowledge and understanding of cybersecurity issues affecting their organizations than do staff without specialized cybersecurity qualifications and with little or no experience in the security domain in a government department. That is, the higher the qualification and experience of cybersecurity staff, the higher the competence level. In this case we propose using a correlation technique to analyse this relationship.

Experience of cybersecurity staff should be based on the number of years served in government department while qualification should be based on an employee's attainment of internationally recognized cyber and information security certificates such as Certified Ethical Hacker, Certified Information Security Professional (CISSP), Certified Information Security Manager (CISM) and Cisco Certified Internetwork Expert (CCIE) Security, among others. Descriptive and Inferential statistical tests such as Mean and Standard deviations, Frequency distributions, Cross tabulations, ANOVA and linear regression analysis were conducted to test this study hypothesis. The ANOVA test was used to compare means of more than two groups on the continuous variable, post-hoc comparisons

were used to find out any significant differences between groups to check the condition for homogeneity of variance if p-value = 0.05. Further, linear regressions were conducted to find out the impact of staff competence on cybersecurity effectiveness (CSE).

Independent Variable 2 (INDV2): Senior management support

Hypothesis H2. There is a relationship between senior management support and cybersecurity effectiveness.

3.2.3 H2 Theoretical Definition

It is claimed in several studies that cybersecurity is a management issue that requires management intervention and commitment (Kritzinger and Van Solms, 2010; Al Bawaba, 2012; Rotvold, 2008; and Nigel and Rice, 2011). Therefore, management support to cyber and information security programmes in and outside the organization is predicted to provide higher effectiveness for it. That is to say, senior management needs to understand the cybersecurity risk and its implications for the organization to enable staff to make informed decisions at the earliest through strategic thinking and governance. Senior management support in this study context is operationally defined in the next section.

3.2.4 H2 Operational Definition

Senior management support is evaluated by the presence or absence of well qualified cyber and information security staff; presence of policies, procedures and strategic plans which have incorporated cybersecurity planning; and the presence of approved cybersecurity budgets among others. “The more the support from senior management, the more the cybersecurity effectiveness”. Descriptive and inferential

statistics like computations for mean and standard deviations, cross tabulations, ANOVA including Levene's test of homogeneity of variance at p - value (p = 0.05) to check if there exist any statistical significance between groups of departments. ANOVA and linear regression to be used in determining the influence of the participants' sector on the construct support from senior management, Multiple comparisons through post-hoc analysis using Tukey HSD test at p-value = 0.05

Independent Variable3 (INDV3): Level of technology

Hypothesis H3. There is a relationship between the level of technology and cybersecurity effectiveness

3.2.5 H3 Theoretical Definition

There is a claim in the literature that organizations that invest heavily and deploy strong cybersecurity technologies in their departments' critical infrastructure demonstrate greater cybersecurity effectiveness (Symantec, 2016; NIST, 2014; Gercke, 2014; and Hunter, 2013). Such technologies include the deployment of strong anti-virus software, firewalls, Intrusion Detection Systems (IDS), and Intrusion Protection Systems (IPS), among others.

3.2.6 H3 Operational Definition

The more organizations deploy strong cybersecurity technologies, the greater their readiness to combat cyberattacks and the greater the cybersecurity effectiveness. Therefore, government entities which deploy appropriate technology for detecting and preventing cyberattacks, will be more effective than those that do not deploy these technologies. From the responses obtained from the survey instrument, it is apparent that all the government entities in Abu Dhabi have invested

heavily in technology. As viewed from the standpoint of the NIST (2014) framework, a technology framework already exists for identifying, detecting, responding to and preventing cyber intrusion; hence the present study focused on adding other human and social factors to technology and measuring them to evaluate the cybersecurity effectiveness of all the departments. Descriptive and inferential statistics like computations for mean and standard deviations, cross tabulations, ANOVA including Levene's test of homogeneity of variance at p-value ($p = 0.05$) to check if there exist any statistical significance between groups of departments. An F-test at statistical significance $p = 0.05$ was conducted to determine the coefficient R^2 and determine its variation with the independent variable of cybersecurity effectiveness, ANOVA and Linear regressions also conducted to check statistical significance between study groups as related to the dependent variable cybersecurity effectiveness.

Independent Variable 4 (INDV4): Training of staff

Hypothesis H4. There is a relationship between the cybersecurity training of staff and cybersecurity effectiveness.

3.2.7 H4 Theoretical Definition

Effective employee training programmes in cybersecurity refers to programmes that provide staff with information, new skills, or professional development opportunities in the domain of cyber and information security. The literature mentions that staff who undergo appropriate cybersecurity training and awareness programmes demonstrate better understanding of cybersecurity issues and gain more job skills, leading to cybersecurity effectiveness in their organizations (Siponnen, 2000; Hight, 2005; Greitzer et al., 2007; Whitmer, 2007; Kritzinger and

Smith, 2008; and McCrohan, 2010). The researcher analysed and validated this theoretical claim.

3.2.8 H4 Operational Definition

The more cyber- and information security training programmes employees undertake, the more knowledge they acquire and the more effective they become; hence the cybersecurity effectiveness of their organizations. We compared the cybersecurity knowledge of employees who have attended the required training programmes to those who have not on a 5 point Likert scale. Descriptive and inferential statistics like computations for mean and standard deviations, cross tabulations, ANOVA including Levene's test of homogeneity of variance at p - value ($p = 0.05$) to check if there exist any statistical significance between groups of departments. ANOVA and Linear regressions were conducted for groups of departments to establish the relationship with the dependent variable, cybersecurity effectiveness (CSE). Further, we used Levene's statistical test to determine the homogeneity of variance and check the p-value within and between the departments or study groups and also compute the means and standard deviations so as to compare departmental sectors against the study construct and the independent variable.

Independent Variable 5 (INDV5): Presence of Cybersecurity Strategic Plans

Hypothesis 5. There is a relationship between the presence of cybersecurity strategic plans and cybersecurity effectiveness.

3.2.9 H5 Theoretical Definition

Strategic planning is an organization's process of defining its strategy, or direction, and making decisions on allocating its resources to pursue this strategy. Strategic plans help organizations to improve their cybersecurity arrangements (Elbanna, 2010; Grant, 2003; and Andrew, 2014), but departments that incorporate cybersecurity in their strategic plans would be more effective.

3.2.10 H5 Operational Definition

The more organizations incorporate cybersecurity into their strategic planning programmes, the greater their cybersecurity effectiveness. That is to say, if the management of a government department considers cybersecurity in all its strategic planning, policies and frameworks, then we expect more cybersecurity effectiveness in the department. Descriptive and inferential statistics like computations for mean and standard deviations, cross tabulations, ANOVA including Levene's test of homogeneity of variance at p - value ($p = 0.05$) to check if there exist any statistical significance between groups of departments. We considered inter-variable correlation coefficients for the different groups in the study population and conducted a linear regression analysis to check the statistical significance of the study construct at $p = 0.05$

Independent Variable 6 (INDV6): Awareness of Users

Hypothesis H6. There is a relationship between the awareness of users about cybersecurity and cybersecurity effectiveness

3.2.11 H6 Theoretical Definition

User awareness programmes are deliberate efforts by organization to influence user thinking and behaviour regarding cybersecurity issues. They are designed to create consciousness in users of the correct behaviours to support the organization's cybersecurity efforts. These programmes instil the security principles that help change user behaviour while helping the organization manage cybersecurity risks.

3.2.12 H6 Operational Definition

Employee awareness of department policies and procedures is a strong indication that the organization has an effective cybersecurity programme. That is "the higher the awareness of users about the organization's policies and procedures, the higher the cybersecurity effectiveness of the organization". Descriptive and inferential statistics were obtained through cross tabulations, post-hoc analysis using Tukey's HSD test, linear regressions and ANOVA test to determine the significance of the results of Levene's test for homogeneity of variance at $p = 0.05$. Smaller values of R^2 represent smaller variations in cybersecurity effectiveness against the factor.

Next, we discuss the research paradigm employed in this study.

3.3 Research Paradigm

Gallagher et al. (2003) define a paradigm as "a world view". The authors view it as a basic set of beliefs or assumptions which guide a researcher's investigation. It is envisaged that every researcher approaches research with many

interlocking and sometimes contradicting philosophical assumptions and standpoints. Yet a paradigm has been defined on the basis of aspects relating to social reality. Social reality is made up of the materials that construct the social world and impact on people's lives, providing them with opportunities and negotiating restrictions, such as individuals' motives and social interactions. Meanwhile Creswell and Miller (2000) indicates that the research design process begins with philosophical assumptions which enquirers treat as a foundation for making decisions when they carry out a study. That is to say, researchers convey their own paradigms, or sets of beliefs, to the research project, and these inform the conduct and writing of the study.

In conducting social science research, two principal and divergent traditions exist, namely positivism and social constructionism. The positivist approach in the natural sciences stresses the use of organized methods combining deductive logic from existing theories with precise empirical observations of individual behaviors, to formulate and test the study hypotheses. Social constructionism, however, focuses on explaining why people have different experiences (Hair et al., 2009). In the present study we employed the positivist paradigm since the logic is based on a critical review of existing theories and frameworks in the literature and in practice. It is proposed that the positivist paradigm underpins quantitative methodology owing to its deductive nature (Tubey et al., 2015). Meanwhile, the approach used for conducting research is discussed in the next section.

3.4 Research Strategy

Several strategies and frameworks in the literature were qualitatively assessed to generate empirical support in formulating a study framework for the present work (NIST, 2014; Nambiro et al., 2014; Shen, 2014; Burgers et al., 2013; and Abraham

Nair, 2015). A detailed discussion of the tools, the research design and the data collection methods is presented. In addition, the units of observation representing the study population, sampling technique employed, reliability and validity of the research instrument as well as the questionnaire used to gather findings of the study are discussed.

While the main strategy in this study was to use a survey approach for collecting data, first a pilot study was conducted in a mid-sized organization to establish the role of awareness programmes in cybersecurity issues among employees. This was necessary to validate whether culturally sensitive cyber and information security training programmes affect the design of appropriate cybersecurity programmes. The intention was to examine the relationship between employee training programmes and employee awareness programmes on cybersecurity effectiveness in organizations, with reference to research hypotheses H4 and H6.

Staff in a midsized organization were randomly divided into two groups. Group one consisting of Indians treated to a cybersecurity training program that is culturally sensitive conducted in Hindi while the second group consisting different nationalities from Uganda, Nepal, Pakistan and the Philippines undertook a generic one conducted in English. A survey was conducted following the treatments. Results showed a significant difference in the two dispositions. It was revealed that the group which undertook a culturally sensitive approach demonstrated better understanding of cyber and information security issues better than the generically trained group after a period of one month.

Following the pilot study, we chose the survey approach, since surveys are easy to manage, effective for a fairly large population and can be administered in

several ways, such as on line, on paper, via a mobile surveys or a mixture of these. Both online and paper surveys were administered to the target population of 946 respondents in Abu Dhabi's government entities to ensure optimum response rates. We employed a quantitative approach to analyze the strata and this formed the basis for a discussion of study results and findings. We analyzed the qualifications and experience (competence) of the information security staff in the Abu Dhabi's government entities, reviewed the existing user training and awareness programmes and the cybersecurity technologies deployed and examined their relationship with the cybersecurity effectiveness of the selected government entities.

Finally, we examined the relationship between the current laws, management support and cybersecurity effectiveness as well as the existence of supportive strategic plans to enhance cybersecurity effectiveness. After a detailed study of several cybersecurity defense frameworks, and drawing from existing frameworks such as NIST (2014) and Nambiro et al. (2014), the researcher proposes a framework that could be utilized by the Abu Dhabi government entities to evaluate their readiness to defend against cyberattacks.

3.5 Research Design

The research design presents a framework created to seek answers to the research questions above. It defines the study type (namely, descriptive or correlational) and sub-type (namely, a descriptive-longitudinal case study), research question, hypotheses, independent and dependent variables, experimental design, and, if applicable, data collection methods and the plan for the statistical analysis proposed. The design was seen as a blueprint for the logical structure of the research, which helped to identify the grouping levels of the participants and the data

collection techniques (Rovai et al., 2014). The relationships between the variables were studied without controlling participants or study conditions through experimental or non-experimental techniques.

Survey research was employed to present the findings of this study. It was structured analytically by presenting its dependent, independent and extraneous variables. The variables used in this study were classified as shown in the Table 2 below.

Table 2: Study Variables

Variable name	Type
Competence/Knowledge of cybersecurity Staff	Independent
Support from Management	Independent
Level of Technology	Independent
Training of Staff	Independent
Presence of Strategic Plans	Independent
Awareness of Users	Independent
Cybersecurity Effectiveness (CSE)	Dependent

3.5.1 Population of the Study

The study population consisted of all the 126 Abu Dhabi government agencies as listed on the e-Government portal (https://www.Abu Dhabi.ae). These agencies, which were the units of our observation, are organized into the types of service they provide to the public. The 8 service types are as follows:

Type 1: Social and Civic

Type 2: Culture and Recreation

Type 3: Department of Transport

Type 4: Economic affairs

Type 5: Health Authority of Abu Dhabi

Type 6: Education Department

Type 7: Public Order

Type 8: Science and Technology

From the target population of 126 we randomly selected at least two (2) units of observation from each of the eight categories or Types listed above. These units of observation (Departments) had the following characteristics. First, the smallest ones had up to 100 employees, the medium-sized ones from 100 – 500 employees and the large ones had over 500 employees. Second, some of the small entities had one or two branches only, while the larger ones had offices in all major urban centres of the Emirate. What was common to most of these entities was that their employees were mostly UAE nationals.

In total, 32 units of observation were randomly selected to represent the 8 types. The results obtained from these units of observation were generalized to the population of the 126 government agencies.

3.5.2 Respondent Sample Selection Methodology

In each of the 32 units of observation in the sample, the researcher aimed at administering the questionnaire to 30 respondents. The total number of respondents targeted was thus 960. The entities were categorized under the eight types of service offered (as seen above). The researcher in consultation with the 10 Experts in Abu Dhabi government entities selected on the basis of subject knowledge and experience and two academic professors selected the sources of data (respondents). These respondents were selected from each of the 32 entities with a major focus on managerial level and staff with the following titles: Executive Director (CEO or

GM), Department Manager (CIO/CISO, Consultant, IT Manager etc.) and Section Manager (Officer, Team member etc.). From the 960 questionnaires distributed to the entire population, a total of 535 was completed and returned. The actual respondents to the survey questions remain unnamed because of confidentiality agreements, which were needed to ensure their maximum cooperation with the research. Figure 14 below illustrates the sample selection methodology used in the study.

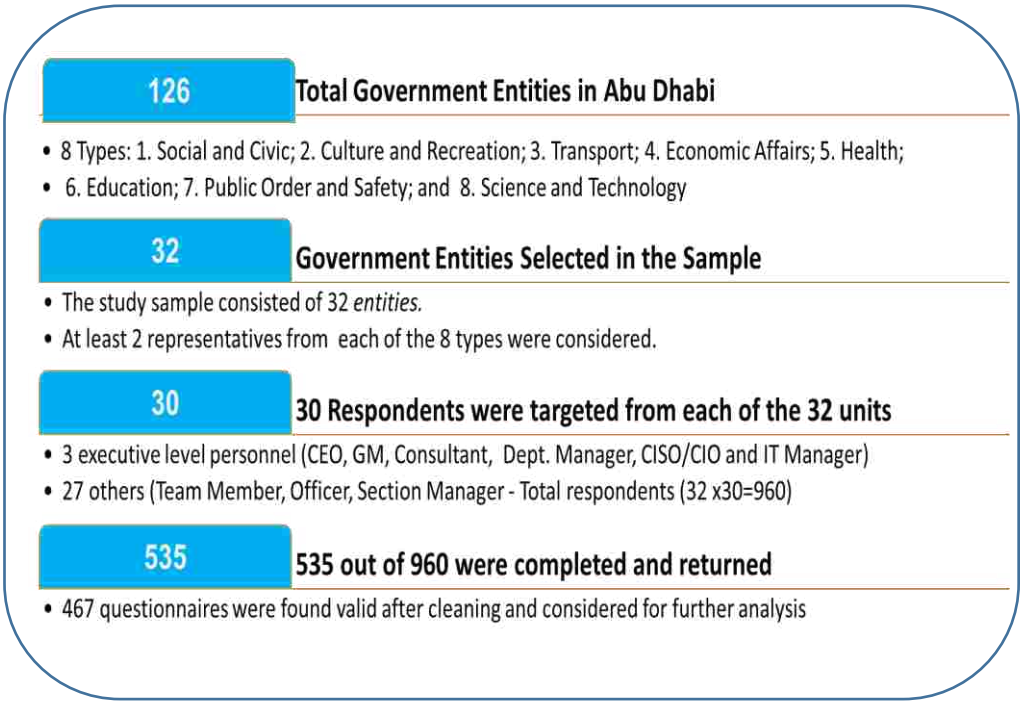


Figure 14: Sample Selection Methodology

From Figure 14, there are 126 government entities in the Abudhabi government (the universe of this study) divided into eight types. The researcher sampled 32 entities from the universe with at least 2 entities from each entity type to avoid sampling bias. Further, from each of the 32 entities in the sample, a minimum of 30 respondents was expected to answer the survey questionnaire. After administering the survey, 535 questionnaires were completed and returned from

which only 467 were clean for further analysis. The next section discusses how the respondents sample was selected to ensure objective responses.

3.5.3 Definition of the Respondents

Further, Table 3 and figure 15 below shows how the 960 targeted respondents were distributed across the 32 government agencies sampled for the study. These respondents constitute our target population (N= 960). From the 32 units of observation sampled, all the Executive Directors or equivalent (32), all CIO/CISO (32) and all IT Managers (32) were targeted. The total targeted from this group of senior management was 96. The remaining 864 included employees in other ranks or positions within the organizations, such as business, HR and operations from all the sampled organizations representing each of the 8 department types across the Emirate. From this targeted population, a total of 535 respondents in the 32 units of observation selected for the survey completed and returned their questionnaires to the researcher for further analysis as indicated in Table 3 below.

Table 3: Definition of the Study Population, Source: Primary Data

Department Types	Total Number of Departments (n1=126)	Departments in Study (n2=32)	Total Executive Director or Equivalent (n3=32)	Total CISO/ CIO	Total IT Managers n5=32)	Total Non-Management Staff (n6=27)	Targeted Population (n3+n4+n5)	Returned Questionnaires
Social and Civic	44	9	9	9	9	243	270	196
Culture and Recreation	19	4	4	4	4	108	120	72
Transport	9	3	3	3	3	81	90	44
Economic Affairs	22	5	5	5	5	135	150	62
Health	2	2	2	2	2	54	60	26
Education	6	3	3	3	3	81	90	49
Public Order and Safety	6	3	3	3	3	81	90	39
Science and Technology	8	3	3	3	3	81	90	47
Total N	126	32	32	32	32	864	960	535

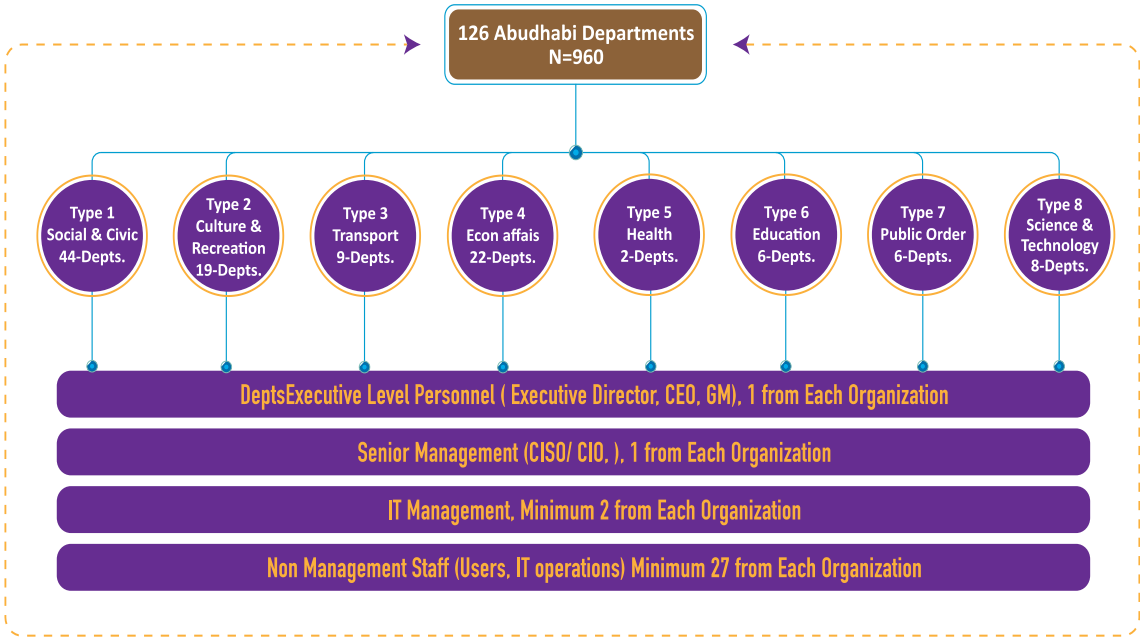


Figure 15: Distribution of the Study Population in Abu Dhabi

Several methods and techniques were applied to gather the research findings and analyze the study results. After a thorough cleaning of the study strata, 68 cases of missing values were detected in the final data coding sheet. These cases were removed before a final analysis, leaving a final complete data set of 467 for further analysis, as detailed in Chapter Four. Meanwhile, some of the tools and approaches in the study are discussed in the next section.

3.6 Methodological Approach

3.6.1 Research Instrument

A carefully written and structured questionnaire was used to gather responses from the target study population. It used a five point Likert scale to guide respondents in choosing the appropriate answers that would allow their views to be interpreted. This tool was selected for the present study since it allows respondents to record in numerical form the degree to which they agree or disagree with a series

of statements, making it easy to perform statistical analysis. The questionnaire used was structured into sub sections, each comprising questions relevant to a specific study hypothesis or area of focus, as detailed in Table 4 below.

Table 4: Questionnaire Structure

Questionnaire Focus area or Variable	**Test Questions (QN)**	**Target Hypothesis**
Demographic Data	QN1, QN2, QN3, QN5, QN6, QN7	Questions used to describe the study population and understanding participants backgrounds
Competence/ Knowledge of staff	QN4, QN8, QN9, QN10, QN11, QN12, QN13, QN14, QN15, QN17,QN18	H1: There is a positive relationship between the competence/knowledge of staff and cybersecurity effectiveness.
Support from Management	QN31, QN32, QN33, QN34, QN35, QN37, QN41, QN42, QN29	H2: There is a positive relationship between senior management support and cybersecurity effectiveness.
Level of Technology	QN19, QN20, QN22, QN23, QN24, QN25, QN26, QN46, QN47, QN48, QN49	H3: There is a positive relationship between level of technology and cybersecurity effectiveness
Training of Staff	QN54, QN55, QN56, QN58, QN59, QN60	H4: There is a positive relationship between cybersecurity training of staff and cybersecurity effectiveness.
Presence of Strategic Plans	QN37, QN38, QN39, QN40	H5: There is a positive relationship between the presence of cybersecurity strategic plans and cybersecurity effectiveness
Awareness of Users	QN4 (demographics), QN8 (demographics), QN40, QN50, QN51, QN52, QN53, QN57	H6: There is a positive relationship between awareness of users about cyber security and cybersecurity effectiveness
Laws and Regulations	QN18, QN30	

Table 4 above shows how the questionnaire items were distributed across the factors of cybersecurity with respect to the different study hypotheses and variables. The items used to measure the constructs were selected with inputs from the consulted 10 experts and in consultation with several international cyber and information security standards like (ADSIC II Information Security Guidelines, 2013, ISO / IEC 27001; 2013; ISMS standard, ISO/ IEC 27032; 2012; Cybersecurity Standard, NIST (2014) Framework guidelines and ISO / IEC 27035, International Standard for incident Management checklists).

An online version of this instrument was initially administered through Survey Monkey to a limited sample to obtain initial results that could be used to further improve the questionnaire before the actual field survey commenced. From the results of this limited study, it was determined that changes had to be made, to improve the clarity of the questions and the response rate of the target population. The corrections included adding an Arabic version and allowing for hard copies to be distributed. A copy of the survey questionnaire can be found in Appendix A of this dissertation. A further discussion of the questionnaire design can be seen in the next section.

3.6.2 Questionnaire Design

Questions in the research instrument were selected basing on review of previous studies, review of industry literature and input from cybersecurity professionals consulted across Abu Dhabi government entities. A total of 57 questions were developed considering the requirements of the different pillars or variables in the study. For example, questions for “Support from Management” had statements regarding the importance of setting aside a budget for cybersecurity;

while those ones concerning “Awareness of Users”, asked whether the respondent agreed with statements on the importance of regular planned cybersecurity awareness programs in the organization among others. Most responses in the survey questionnaire were scored on a 5 - Point Likert scale to capture responses of users to the different questions in which a score of 1 indicated “Strongly Disagree” and a score of 5 “Strongly Agreed”. These responses from the target population were coded into a Statistical Tool for further analysis, generation and Interpretation of results. For example consider the following tables showing how questionnaire items were selected by study variable. Other items can be seen in the Appendix B.

Table 5 and Table 6 below present a sample of how the questionnaire items were carefully selected to address the research questions and study hypotheses. For every question in the survey instrument, the researcher reviewed related literature and with consultations from 10 subject matter experts in cyber and information security and 2 academic professors identified questionnaire items to suit the study constructs and answer the research questions. A sample of such questions are as seen below.

Table 5: Showing sample Questionnaire Items for the Variable Competence/ Knowledge of Staff

Research Question	**Study Hypothesis**	**Literature highlights**	**Survey Instrument Questions**
1. Are the existing information security professionals in government entities well qualified and experienced to detect and stop cyber-attacks?	There is a relationship between the competence/knowledge of staff and cyber security effectiveness (H1)	It is claimed that only graduates with the right skills and experience will be able to resolve the ever rising level of international cyber conflict (Dale et al., 2011) As enterprises invest more resources in data protection, their main challenge still remains that of finding top-flight security practitioners with the right skills for the job (CSX, Feb, 2017) Organizations' cybersecurity teams continue to struggle to convince senior management of cybersecurity issues.	**Survey Questions:** 4. How many years have you worked in the government sector? 8. A cyberattack is a perceived threat to network security. 9. Our employees do not know when their computers have been attacked by a virus. 10. A cyberattack can be perceived as a threat to data and information. 11. A Virus attack is a type of a cyber-attack. 12. Untrustworthy employees or disgruntled IT insiders can initiate a cyberattack against the organization.

Table 6: Questionnaire Items for the Senior Management Support Variable

Research Question	**Study Hypothesis**	**Literature highlights**	**Survey Instrument Questions**
2. To what extent does senior management support the establishment and implementation of cybersecurity defense strategies	There is a positive relationship between senior management support and CSE (H2)	Senior management are required to exercise "due care" and "due process" in ensuring CSE of their organizations Haris, (2010). Prevention of cybersecurity is considered a strategic management issue, top management support improves effectiveness of organization's cybersecurity programmes through prioritization, funding and enforcement of security policies (Dutton and Duncan, 1987; Knapp, 2009) Senior management needs to take proactive measures in policy enforcement, budgetary support for cyber-security technologies and training programs (Deloitte Touch, 2016)	**Survey Questions:** 29. All Abu Dhabi government organization should have a budget allocated to strengthen cyber-security measures. 30. Our organization has invested adequate funds to promote countermeasures against cyberattacks. 31. Our organization has invested adequate funds towards increasing employee education as a protection from cyber-attacks. 32. Disaster recovery is not considered as a protection from cyberattacks, but rather a pre-determined plan in case of a cyberattack.

Table 6: Questionnaire Items for the Senior Management Support Variable (Continued)

Research Question	**Study Hypothesis**	**Literature highlights**	**Survey Instrument Questions**
3. To what extent does senior management support the establishment and implementation of cybersecurity defense strategies	There is a positive relationship between senior management support and CSE (H2)	Senior Management participation in information security initiatives has a significant effect on employee attitudes, behaviours and cultural values towards compliance with information security policies and strategies in place (Hu et al., 2012)	34. It is important to have cyber-security incorporated in organization's strategic plans. 35. All employees in our organization are aware of the strategic plan implemented to protect against cyber-attacks. 36. Senior management has an important role in developing information security policies for our organization. 37. The Head of Information Security of our organization reports directly to the highest official in our organization 41. It is important to separate the roles of IT management and Information Security management in our organization.

3.7 Analysis Tool

The study employed the IBM 21 Statistical Package for Social Sciences (SPSS) as the main data analysis tool, especially used for coding and interpretation quantitative data. This is because SPSS provides a mechanism for statistical analysis, including data access and preparation, graphics, modelling and analytical reporting. The tool provides the following advantages:

- Faster and easier basic function access, such as descriptive statistics (i.e. mean, standard deviation or median). Compared to Ms. Excel's built-in functions, SPSS provides these basic statistical elements in pull down menus in addition to a wider variety of graphs and charts which can create complex graphs, such as contingency tables.
- Easier to find statistical tests. While Excel has a wide range of statistical tests built-in, the pull-down menus in SPSS make for faster access.

3.8 Validity and Reliability of the Research Instrument

The research instrument used in this study was initially tested for validity and reliability to ensure inter variable consistency against the study constructs. A reliability test for variables was conducted by examining values of Cronbach's alpha (α: $0.5 \leq \alpha \leq 1$) and factor analysis in order to eliminate variables with low factor loadings against the required constructs and research hypotheses. A new instrument was generated after eliminating all questions that did not fit well in specific sections of the research instrument. Validation of the study provided a means to critically evaluate and objectively review the results of the main study on cybersecurity. The findings were presented to a panel of academic and industry experts, nominated

according to subject knowledge and experience in the security industry, who were asked to judge and comment on issues pertaining to the research problem. This presented an opportunity to obtain some independent views on the viability of the findings which enabled us to add value by decoding and interpreting unexplained phenomena. The intention was to eliminate all the questions that could not load well against the study hypotheses. Some of the techniques employed in this study include the following.

3.8.1 Content validity

The research instrument under consideration was further reviewed by three (3) experts in cybersecurity practice from different companies and two (2) academic professors from the UAEU to check the clarity of the questions. Unclear or ambiguous questions were revised and complex items re-worded. Furthermore, ineffective and non-functioning questions were omitted from the final survey instrument. Consultations were made with two more senior information security professionals from a mid-sized organization in Abu Dhabi to review the instrument and provide a level of expert support. In addition, more than one person was asked to conduct the field survey and data collection, to ensure investigator triangulation. Several surveys were followed up to mitigate the impact of unreturned questionnaires and to reduce dropout rates**.** Finally, the sequence of questions in the questionnaire was aligned with the study constructs.

3.8.2 Internal validity

Both manual and electronic versions of the research instrument were delivered to different respondents to help increase the response rate. Participatory

and collaborative measures were also employed to ensure that respondents reached a consensus, especially for the more technical and challenging sections of the instrument. Additionally, the sharing of ideas especially on the subject matter made them clearer to the respondents, which later ensured more accurate results.

3.8.3 Convergent validity

Convergent validity of the scale suggested that all items of the same scale should be related to each other (Zikmund et al., 2010). In order to establish convergent validity, the average factor loading of all items of the same scale should be greater than 0.70. Therefore, in order to establish convergent validity of the study scales, the researcher calculated the average factor loadings of all scale items used in the study. The results indicated that the average factor loadings of all scales were greater than 0.70 and thus convergent validity is established as presented in Table 7 below.

Table 7: Convergent Validity of Scale Items

Scales	Average Factor Loading
Competence of Staff	0.771
Level of technology	0.701
Support from mgt.	0.770
Training of staff	0.751
Strategic plan	0.763
Awareness of users	0.705
Cybersecurity Effectiveness	0.704

3.8.4 Reliability of the Research Instrument

Reliability measures the inter-item consistency of the instrument. The most common indicator to measure inter-item consistency is Cronbach's alpha coefficient. Ideally, the minimum value of Cronbach's alpha of a scale should be 0.70 or above (DeVellis, 2003). However, in case of short scales, the Cronbach's alpha value of 0.50 is also acceptable (Pallant, 2013). In our study, the Cronbach's alpha values of all scales are greater than 0.70 (see Table 8) and therefore reliability is established for all dependent as well as independent variables and we can rely on the data obtained using these scales.

A new instrument was generated after elimination of all questions that couldn't fit well in specific sections of the research instrument. Validation of the study provided the means to critically evaluate and objectively review the results of the main study on cybersecurity. Findings were presented to a panel of academic and industry experts, nominated according to subject knowledge and experience in the security industry to ascertain their thoughts and judgement on issues pertinent to the research problem. This presented an opportunity of obtaining independent views on the viability of the findings which provided a platform for value addition by decoding and interpreting unexplained phenomena.

Table 8: Reliability of Scales

Variables	Alpha
1. Cybersecurity Knowledge (CK)	0.921
2. Support from Management (SM)	0.926
3. Level of Technology (LoT)	0.899
4. Cybersecurity Effectiveness (CE)	0.747
5. Training of Staff (TS)	0.839
6. Strategic Planning (SP)	0.815
7. Awareness of Users (AU)	0.712

Detailed results from the reliability tests conducted and the Exploratory Factor Analysis (EFA) conducted on the study constructs are shown in Chapter Four of the study.

3.9 Research Limitations

Since cybersecurity presents a sensitive issue of discussion everywhere, most of the interviewees hesitated to reveal critical security information pertaining to their organizations. In addition, the researcher was limited to a few existing research studies and frameworks on cybersecurity especially concerning Abu Dhabi's government entities and even the entire UAE region. This study has been mainly confined to evidence gathered from other regions such as the USA, Europe and Africa, whose security status and or objectives may not be the same as in the Middle East or the United Arab Emirates. Other limitations of concern in this study included the fact that most of the highly security-sensitive government entities and/or C-level officers were difficult to access in time. As a mitigation strategy, the researcher designed two sets of surveys, one electronic and the other on paper for distribution to

each government department with the help of the research assistant and the Survey Monkey tool. This enabled us to gather feedback from a representative sample for data analysis and discussion.

3.10 Ethical Issues

The process of accessing the selected study population in Abu Dhabi's government entities was facilitated through personal contacts who acted as doorkeepers and obtained consent to use their departments as part of our case study. We made an initial informal request to access individual departments and followed it by a formal letter presenting the research topic and purpose of the questionnaire. Formal authorisation from the UAEU had been acquired; provided an introductory letter which was attached to all questionnaires for specific government entities. Once access had been officially obtained, the respondents were identified and contacted through formal emails to make arrangements to receive the survey instrument both in hard copy and online via the Survey Monkey tool. Each informant was apprised of the research under study and the purpose of the survey. Guarantees were given to all respondents that the data would be used solely for the purposes of the dissertation and that information would not be disclosed to any third parties but would be kept confidential. Furthermore, individual names would not be revealed after the completion of the survey instrument.

3.11 Conclusion

In this chapter, the research strategy, paradigm (positivism) and the data collection tools, approaches and methodology (quantitative), including the questionnaire structure and presentation of the research instrument were reviewed.

Further, the study population, the respondents' sampling methodology, sample design, definition of respondents and the research variables were defined. In the same chapter the reliability and validity of the research instrument were looked into, employing Cronbach's alpha test to assess the reliability of the measurement scale. It found all the study variables to be internally consistent with the study construct, having values of alpha > = 0.59; the details are presented in Chapter Four. Meanwhile, ethical research considerations were maintained for the entire study and a correct data collection process was followed. The survey instrument was sent to a sample of 960 respondents constituting the study population in the selected 8 departmental categories of Abu Dhabi government offices. Of these, 535 completed and returned questionnaires representing 56.6% of the population were further validated, yielding a final total of 467 questionnaires to be retained for data analysis after cleaning and the elimination of duplicated and incomplete questionnaires, as further discussed in the next chapter.

Chapter 4: Analyses and Interpretations of the Data

4.1 Introduction

In the previous chapter, we presented the main strategy and research paradigm considered for this study. Specifically, the chapter justified the positivist paradigm and the quantitative methodology that was used for analysing the variables identified for this study of the cybersecurity effectiveness of Abu Dhabi's government entities. Additionally, it also presented a definition of the study variables, the population, sample size and a discussion of the data collection tools and approaches. The validity and reliability of the survey items to scale were assessed, together with ethical issues.

This chapter now turns to a detailed analysis of the data collected from the study population with the aim of testing the identified study hypotheses, interpreting the study results obtained from these analyses and answering the research questions. We used the statistical package for social sciences IBM SPSS 21 in conducting the data analysis. In the first step, we cleaned the data by assessing their normality, dealing with missing values, identifying aberrant values and detecting outliers. In the next step, we performed exploratory factor analysis (EFA) and calculated the reliabilities of the scale values, followed by a discussion of the descriptive statistics. Finally, ANOVA, cross tabulation and linear regression were carried out to test the research hypotheses and interpret the results. The following flow chart in Figure 16 presents the design used for structuring chapter one.

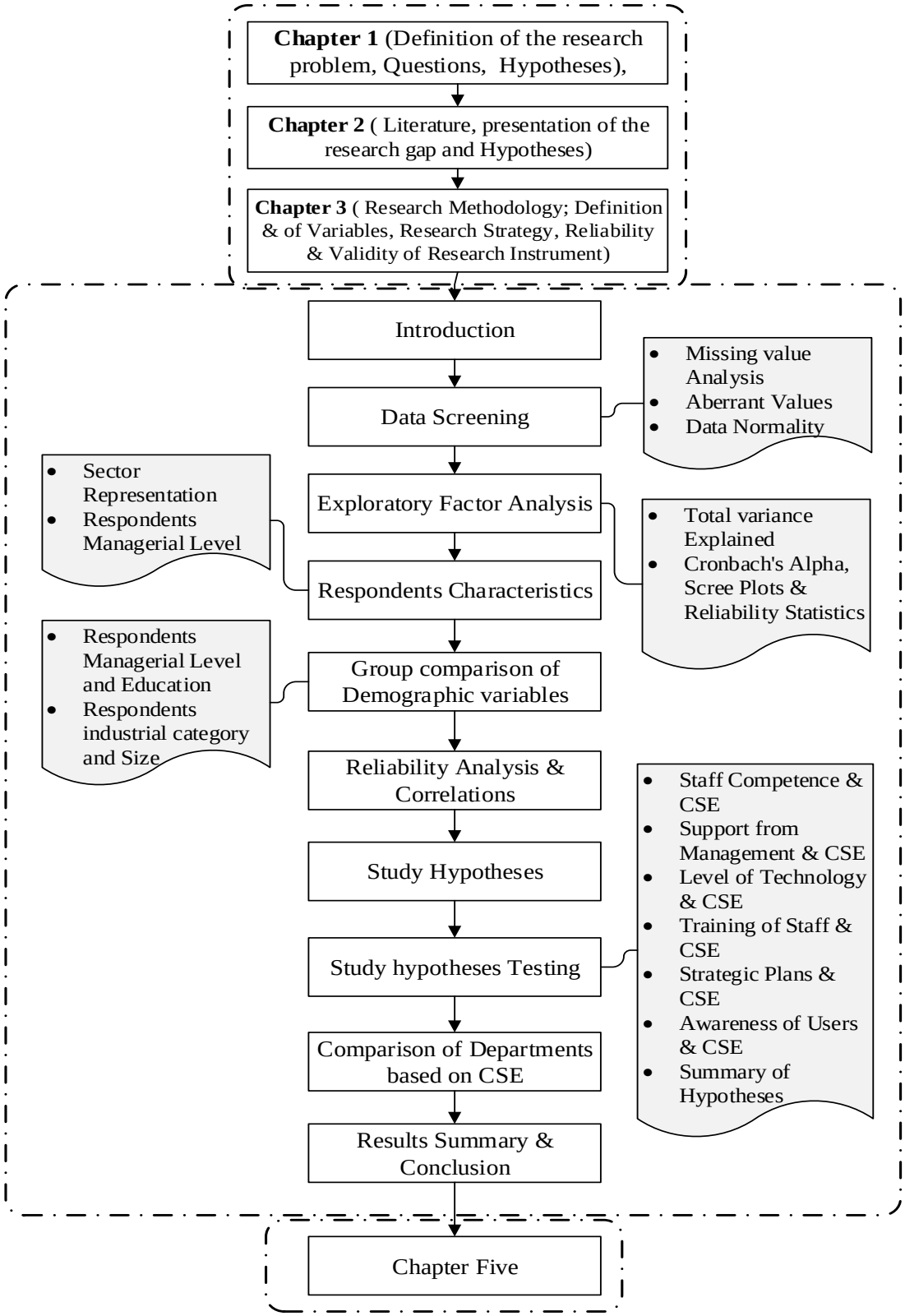


Figure 16: Design of Chapter Four

4.2 Data Screening

Before conducting the data analysis, the strata was cleaned to eliminate duplication and any form of errors due to missing or erroneous values. The screening process was performed through the following steps;

i. Dealing with missing values
ii. Identifying aberrant values
iii. Finding outliers/Assessing data normality

4.2.1 Missing Value Analysis

Missing values in a data set is a common phenomenon in social and behavioural sciences (Hippel, 2004 and Enders, 2001). Missing values in huge quantity are of serious concern in final data analysis and may generate biased and unreliable results and when some values are missing, certain statistical tests cannot be performed. Therefore, it is highly recommended to analyze missing values in a data set before conducting analyses (Tabachnick and Fidell, 2007).

All of the study variables have some missing data. From a total of 535 cases, the result of the missing value analysis showed that the last 68 cases had more than 60% missing data (Table 9). Given the large amount of missing values in these 68 cases, they were removed before conducting a final analysis. The rest of the missing values in some variables were nominal and were filled in by using the method known as “replace with series mean”. After removing the cases with many missing values and filling in a small number of missing values in the remainder, our data set became free of any missing values. All of the next analyses were performed on all 467 of the remaining cases.

Table 9: Case-wise Missing Value Analysis

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	00	467	87.28	87.28	87.28
	36	29	5.42	5.42	92.70
	41	09	1.68	1.68	94.38
	47	19	3.55	3.55	97.93
	50	11	2.05	2.05	100.00
	Total	535	100.0	100.0	

4.2.2 Aberrant Values

Aberrant values are those abnormal values that are beyond the normal range. For example items in the current study were measured on a Likert scale of 1 to 5 thus any value greater than 5 or lesser than 1 would be considered an aberrant value. Similarly the categorical variables are measured in terms of 1 and 2, so any value outside this range would be treated as an aberrant value. Aberrant values usually arise during data entry and may cause serious issues in data analysis because they influence the mean of the variable under scrutiny. Therefore it is of the utmost importance to carefully detect and treat these values before the final data analysis.

In order to identify the aberrant values in our data file, descriptive statistics was run with minimum and maximum values of the items. Very few aberrant values were found and they were corrected by identifying the relevant cases.

4.2.3 Normality of Data

Screening the normality of the data is essential for conducting robust statistical analyses. The normality of the data can be calculated either by statistical or graphical methods (Tabachnick and Fidell, 2007). The Kolmogorov-Smirnov test and the Shapiro-Wilks tests are often used to assess the normality of data. The reason is

that when the data under scrutiny are compared to a normal distribution with the same mean and standard deviation, a p-value greater than 0.05 confirms the normal distribution of the data. Although both techniques are used for normality tests, they become unwieldy and impractical when the dataset for graphical analysis is large. Thus, we chose the statistical technique to test normality, since the data file of the present study contains 467 cases.

In the first step Kolmogorov-Smirnov and Shapiro-Wilk tests of normality were applied. If the results from these two tests are significant ($P < 0.05$), then the data are not normally distributed. If, however, the results are non-significant ($P > 0.05$), then the data are normally distributed. The results of both the Kolmogorov-Smirnov and Shapiro-Wilk tests shown in Table 10, below, indicate that the values were significant ($P < 0.05$), confirming that these data were not normally distributed.

Table 10: Test of Normality

	Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
	Statistic	**Df**	**Sig.**	**Statistic**	**Df**	**Sig.**
CE_mean1	0.146	467	0.000	0.887	467	0.000
CK_mean1	0.119	467	0.000	0.926	467	0.000
RoT_mean1	0.092	467	0.000	0.964	467	0.000
SM_mean1	0.093	467	0.000	0.976	467	0.000
TS_mean1	0.105	467	0.000	0.933	467	0.000
AU_mean1	0.095	434	0.000	0.957	467	0.000
SP_mean1	0.090	467	0.000	0.981	467	0.000

Note: CK = Cybersecurity knowledge/competence; SM = Support from Management, RoT = Role of Technology, CE = Cybersecurity effectiveness, TS = Training of staff, SP = Strategic Plans, AU = Awareness of users.

In addition to the above tests, it was thought important to examine two measures of distributions, skewness and kurtosis. Skewness assesses the symmetry of the distribution. That is, if the distribution of the data is stretched to a right or a left

tail, then the distribution is considered “skewed”. A skewness value greater than +1 or lower than -1 counts as skewed distribution. Meanwhile, kurtosis checks whether the distribution is too peaked. Data distribution is considered too peaked if the kurtosis value generated is more than +1; if it is less than -1, we conclude that the distribution is too flat and if the values of skewness and kurtosis are close to zero then the data in question are considered normally distributed. In the present research, the normality of the data was examined using SPSS statistical software. As shown in Table 11, both tests revealed a p-value of less than 0.05, indicating that the data were not normally distributed.

Regarding the skewness measure, as reported in Table 11, below, it is approximately -1, which reveals that the distribution of the data was skewed and the kurtosis value of approximately +2 indicated that the distribution was too peaked. Therefore, both measures affirmed that the data of the present study were not normally distributed. The values of both skewness and kurtosis for all items fell between +1.5 and, -1.5 the recommended values. These values established the quasi normal distribution of the study’s data set.

Table 11: Values of Skewness and Kurtosis

	CE_mean	**CK_mean**	**RoT_mean**	**SM_mean**	**UTA_mean**	**SP_mean**
Skewness	-1.399	-1.043	-0.652	-0.323	-1.039	-0.411
Std. Error of Skewness	0.113	0.113	0.113	0.113	0.113	0.113
Kurtosis	1.131	1.225	1.429	-0.156	1.134	0.232
Std. Error of Kurtosis	0.225	0.225	0.225	0.225	0.225	0.225

Finally, the outliers in data were identified by using Mahalanobis distance measuring method, as suggested by Tabachnick and Fidell (2007). These writers argue that cases with a Mahalanobis alpha level of 0.001 should be considered as outliers. By following Tabachnick and Fidell (2007) guidelines, a critical chi-square value was calculated by using five independent variables. It was found that no case had less than 0.001 value, confirming that no outliers were found.

4.3 Exploratory Factor Analysis (EFA)

The first step in exploratory factor analysis is to check the adequacy of the data (Pallant, 2013). For this purpose two tests are commonly used by social scientists. These are Bartlett's test of sphericity and the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy. Bartlett's test of sphericity should be significant if $p < 0.05$, while the KMO value should be not less than 0.6 for good factor analysis. In the present study, the data fulfilled both these requirements, as shown in Table 12

Table 12 : KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.859
Bartlett's Test of Sphericity	Approx. Chi-Square	2681.508
	Df	190
	Sig.	0.000

Factor analysis was conducted on all the variables studied: "cybersecurity knowledge/competence", "support from top management", "role of technology", "awareness of users", "training of users", "presence of strategic plans" and "cybersecurity effectiveness". To present data more simply, Principal Component

Analysis (PCA) was used. Varimax rotation was adopted in order to minimize the chance of cross loading items on more than one factor. Following Comrey and Lee rule of thumb (1973), items having a loading of 0.45 and a cross loading higher than 0.32 were dropped.

Factor analysis was run on 57 cybersecurity items and combined into seven factors (Table 13). These factors were labelled "competence/knowledge of staff", "support from top management", "level of technology", "training of staff", "awareness of users", "presence of strategic plans" and "cybersecurity effectiveness". The first factor, "competence/knowledge of staff" contained ten items. Two factors, "support from top management" and "the role of technology" consisted of twelve items each. Eleven items combined to make up the fourth and fifth factors, labelled "training of staff" and "awareness of users". The fifth independent variable "presence of strategic plans" comprised four items. Finally, the dependent variable, "Cybersecurity effectiveness" had seven items.

Following Comrey and Lee rule of thumb (1973), four items in total were deleted due either to small loading value or high cross loading on more than one factor. Two items were eliminated from the "cybersecurity effectiveness" factor and two items were removed from the factor "support from top management". These two factors were left with five and ten items respectively and the fifty-two items were considered in the final results. A complete typology classification is given in Table 13.

Table 13: Exploratory Factor Analysis

Items	Component						
	1. Support from Management	**2.Competence/ Knowledge of staff**	**3.Level of Tech.**	**4.Training of Staff**	**5.Cybersecurity Effectiveness**	**6.Strategic Plans**	**7.Awareness of users**
SM2	0.862						
SM7	0.854						
SM8	0.843						
SM9	0.838						
SM1	0.837						
SM4	0.814						
SM3	0.770						
SM6	0.659						
SM10	0.624						
SM5	0.615						
CK2		0.843					
CK1		0.840					
CK5		0.780					
CK6		0.755					
CK4		0.755					
CK8		0.739					
CK7		0.732					
CK10		0.725					
CK9		0.678					
CK3		0.675					

Table 13: Exploratory Factor analysis (Continued)

Items	Component						
	1. Support from Management	**2.Competence/ Knowledge of staff**	**3.Level of Tech.**	**4.Training of Staff**	**5.Cybersecurity Effectiveness**	**6.Strategic Plans**	**7.Awareness of users**
RoT11			0.811				
RoT6			0.806				
RoT3			0.774				
RoT7			0.763				
RoT10			0.759				
RoT4			0.714				
RoT5			0.693				
RoT8			0.692				
RoT12			0.692				
RoT1			0.622				
RoT2			0.536				
RoT9			0.400				
TS5				0.835			
TS11				0.815			
TS7				0.774			
TS8				0.725			
TS4				0.695			
TS6				0.666			
CE3					0.750		
CE4					0.737		
CE7					0.717		

Table 13: Exploratory Factor analysis (Continued)

Items	Component						
	1. Support from Management	**2.Competence/ Knowledge of staff**	**3.Level of Tech.**	**4.Training of Staff**	**5.Cybersecurity Effectiveness**	**6.Strategic Plans**	**7.Awareness of users**
CE6					0.671		
CE5					0.667		
CE2					0.592		
SP3						0.819	
SP1						0.779	
SP2						0.730	
SP4						0.724	
AU9							0.801
AU2							0.728
AU3							0.652
AU10				0.462			0.590
AU1					0.352		0.357

Factor analysis is graphically presented in form of scree plot. Scree plots show the eigenvalues against all factors and helps to determine which factors to retain. In this case, the scree plot showed that the curve starts to flatten from factor seven onward. Further, the eigenvalue of all the factors after factor seven were below one. Therefore only seven factors were retained as indicated in Figure 17 below.

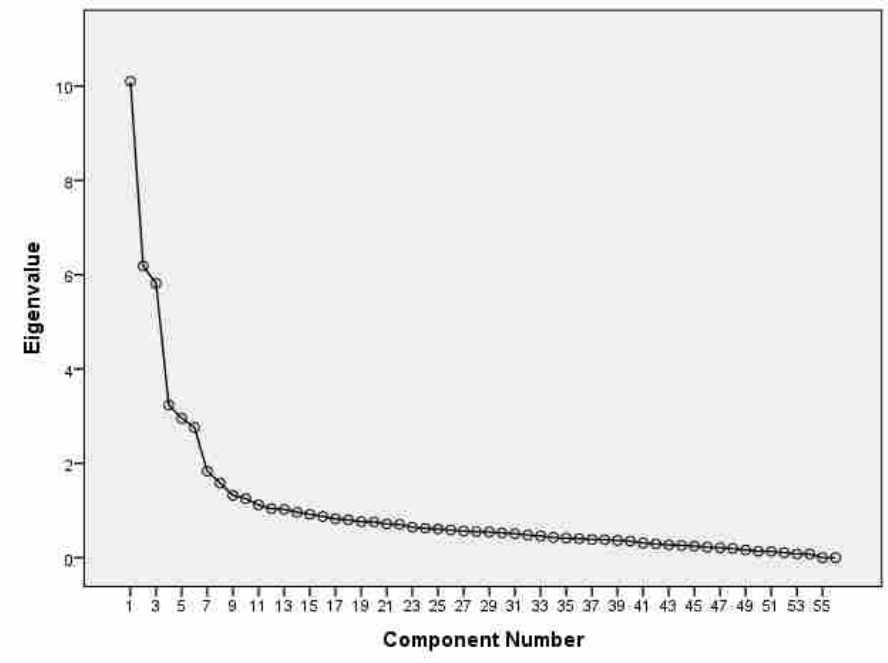


Figure 17: Scree Plot showing Factors to Retain

4.3.1 Total Variance Explained

Eigenvalues reflect the number of factors extracted for factor analysis. The result of selecting eigenvalues showed that 7 factors explain 55% of the variance and the remaining factors remain insignificant. In this case, the first factor accounts for 17.10% of the variance, the second 10.49%, the third 9.84%, the fourth 5.47%, the fifth 5% and sixth 4.67% of the total variance. Individual and cumulative factor variance is explained in Table 14 below.

Table 14: Total Variance Explained

Component	Initial Eigenvalues		
	Total	**% of Variance**	**Cumulative %**
1	10.10	17.10	17.10
2	6.18	10.49	27.57
3	5.81	9.84	37.42
4	3.23	5.47	42.89
5	2.95	5.00	47.90
6	2.76	4.67	52.57
7	2.00	3.90	**54.57**

After successfully completing the factor analyses, we were closer to understanding the respondents' characteristics and we then moved towards testing the hypotheses.

4.4 Respondents' Characteristics

4.4.1 Sector Representation

Data were collected from 467 respondents working in eight different government sectors namely, social and civic, culture and recreation, transport, economic affairs, health, education, public order and science and technology. The highest representation was from the social and civic department, which contributed 38.54% of all respondents. Those from the culture and recreation department form the second biggest category, with 14.1%. Of the eight departments in total, the respondents from the health department showed least representation, 5.14%. A complete breakdown of the respondents' profile with reference to their sector representation is given in Figure 18

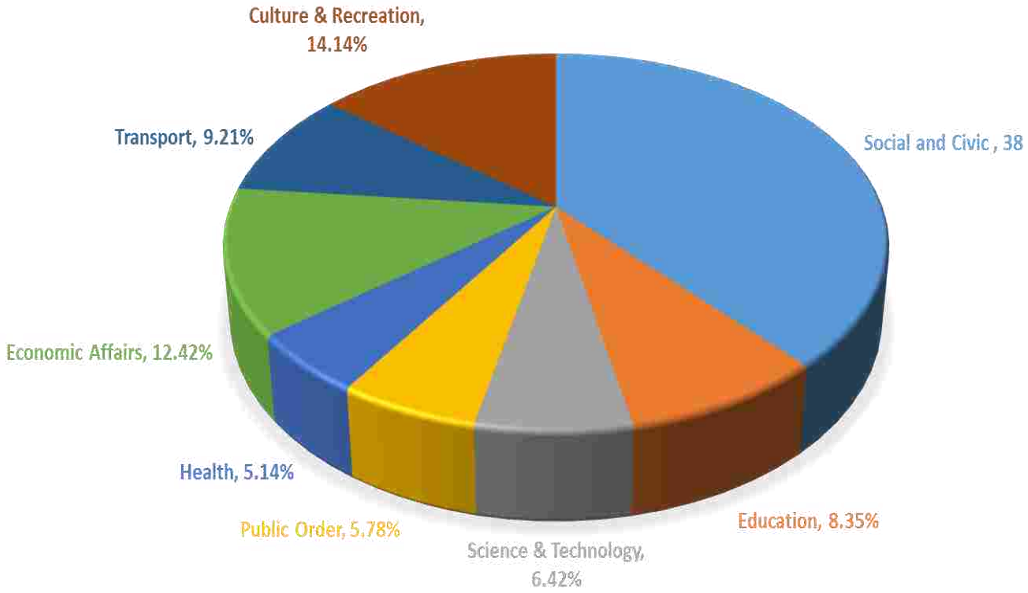


Figure 18: Sector-wise Distribution of Respondents Managerial Level

4.4.2 Respondents' Managerial Level

The respondents were categorized into five different levels, ranging from officer to consultant. The data show that 32.76% participants belonged to the executive or director level, the category that contributed most to the total. It shows that most of the respondents participating in the survey were at senior management level. A complete breakdown is given in Figure 19.

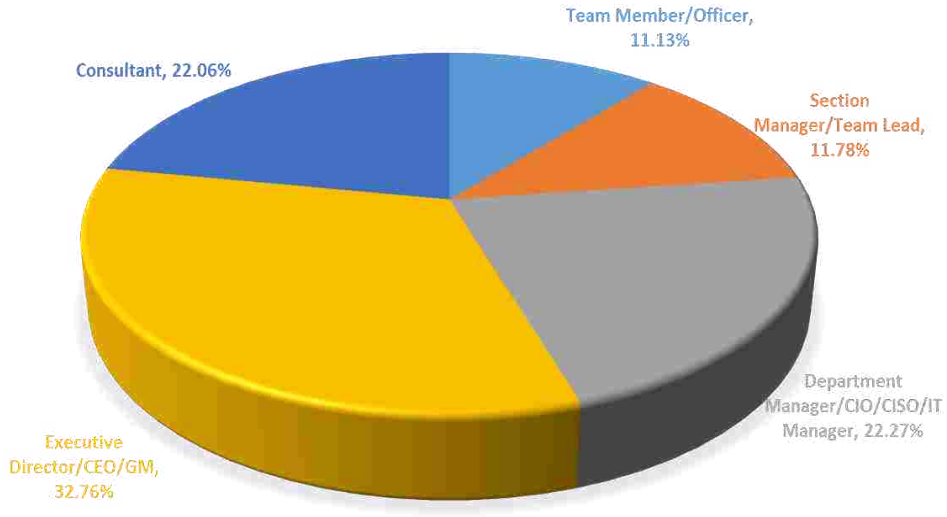


Figure 19: Managerial Level of Respondents

4.5 Group Comparisons of Demographic Variables

4.5.1 Respondents' Managerial Level and Education

Cross tabulation between respondents' education level and their managerial level is shown in Table 15. Cross tab analysis shows a direct relationship between education level and managerial level, that is; the higher the education level, the higher the managerial level. Respondents with high school education in officer or team lead level are mostly low in number and no one with this level of education attains the higher managerial levels, for instance director or consultant. Most of the senior level positions are filled by respondents with bachelors' and masters' degrees.

Table 15: Respondents' Managerial Level and Education

Variable	Category	Managerial Level										Total	
		Officer		Team Lead		CIO		Director		Consultant			
		Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%
Education Level	High School	11	21	14	26	7	7	-	-	-	-	32	7
	Diploma	9	17	6	11	11	11	6	4	-	-	32	7
	Higher Diploma	3	6	1	2	3	3	8	5	3	3	18	4
	Bachelors	25	48	30	55	73	70	100	65	52	51	280	60
	Masters	4	8	4	7	10	10	34	22	47	46	99	21
	Doctorate	0	-	-	-	-	-	5	3	1	1	6	1
Total		**52**	**52**	**100**	**55**	**100**	**104**	**100**	**153**	**100**	**103**	**100**	**467**

4.5.2 Respondents' Industrial Category and Size

The respondents' industry and their respective size in terms of number of employees are cross tabulated in Table 16. The overall representation is highest from the social and civic sector with 180 participants out of 467 and 66 came from the culture and recreational sector, the second highest group. It is noted that 135 respondents were from small organizations, i.e. those having fewer than 100 employees.

Table 16: Respondents' Representation by Sector and Size

Vars	Category	Size (No of Employees)											
		<100		100-200		201-500		501-999		>1000		Total	
		count	%	count	%	count	%	count	%	count	%	count	%
Industry	Social and Civic	65	48	38	50	21	28	32	43	24	23	180	39
	Culture and Recreation	33	24	7	9	7	9	10	14	9	9	66	14
	Transport	16	12	5	7	5	7	6	8	11	11	43	9
	Economic Affairs	9	7	6	8	23	30	5	7	15	14	58	13
	Health	2	2	6	8	6	8	2	3	8	8	24	5
	Education	2	2	6	8	4	5	11	15	16	15	39	8
	Public Order	5	4	6	8	5	7	3	4	8	8	27	6
	Science and Technology	3	2	2	3	5	7	5	7	13	13	30	6
Total		**135**	**100**	**76**	**100**	**76**	**100**	**74**	**100**	**104**	**100**	**467**	**100**

4.6 Reliability Analysis and Correlation Matrix

The mean, standard deviation, reliability and correlations of study variables are presented in Table 17. The results of the reliability analyses showed that all the study variables had an alpha value greater than 0.7, the minimum threshold for reliability. The correlation values show that all the independent variables cybersecurity knowledge/competence, support from top management, role of technology, training of staff, and awareness of users and presence of strategic plans were positively correlated with the dependent variable, cybersecurity effectiveness. These results initially support our hypotheses.

Table 17: Mean, Standard Deviation, Reliability and Correlations

Variables	Mean	SD	Alpha	CK	SM	RoT	CE	UT	SP	AU
1. CK	4.15	0.56	0.921	1						
2. SM	3.72	0.69	0.926	0.243**	1					
3. RoT	3.78	0.62	0.899	0.430**	0.243**	1				
4. CE	4.13	0.62	0.747	**0.397*** **	**0.245***	**0.367****	1			
5. UT	4.05	4.05	0.839	0.466**	0.122**	0.346**	**0.373****	1		
6.SP	3.95	3.95	0.815	0.406**	0.275**	0.375**	**0.337****	0.244**	1	
7. AU	4.01	0.601	0.712	0.139**	0.026*	0.133***	**0.301*** **	0.108**	0.074*	1

* P < 0.05, ** P < 0.01, ***P < 0.001

Note: CK = Cybersecurity knowledge/competence; SM = Support from Management, RoT = Role of Technology, CE = Cybersecurity effectiveness, TS = Training of staff, SP = Strategic Plans, AU = Awareness of users.

It is also noted that staff competence/cybersecurity knowledge and awareness of users were highly correlated with cybersecurity effectiveness (r = 0.397, r = 0.301) at p < 0.001 level and least correlated with support from management (r = 0.245) at p < 0.05 level. All the other variables showed good positive Pearson correlation value with the dependent variable of cybersecurity effectiveness. The role of technology, training of staff and support from management were significantly correlated (r = 0.367, r = 0.373, r = 0.337) with cybersecurity effectiveness at p < 0.01 level. After finding initial support for our study hypotheses, we further tested with regression analysis to accurately find the impact of the independent variables on the dependent variable.

4.7 Study Hypotheses

Hypotheses derived from the literature review state that both organizational and individual level factors contributed to an effective cybersecurity system. At the

organizational level, three factors, support from top management, role of technology and strategic plans were all positively related to cybersecurity effectiveness. We hypothesized that organizations with a higher score in these three factors have more effective cybersecurity systems. Similarly, at individual level, staff competency/cybersecurity knowledge, training of staff and awareness of users were found to be directly associated with cybersecurity effectiveness. Employee knowledge and awareness about cybersecurity systems is helpful in maintaining an effective cybersecurity system. Likewise, employees' training in cybersecurity also impacts positively such a system. We propose to test the following study hypotheses through linear and multiple regressions analysis methods to obtain answers to the study research questions;

H1: There is a positive relationship between the competence/knowledge of staff and cybersecurity effectiveness.

H2: There is a positive relationship between senior management support and cybersecurity effectiveness.

H3: There is a positive relationship between level of technology and cybersecurity effectiveness

H4: There is a positive relationship between cybersecurity training of staff and cybersecurity effectiveness.

H5: There is a positive relationship between the presence of cybersecurity strategic plans and cybersecurity effectiveness

H6: There is a positive relationship between awareness of users about cyber security and cybersecurity effectiveness.

4.8 Hypotheses Testing

This section discusses the results from hypothesis tests conducted for this study. The section below contains the general steps taken to arrive at the conclusions.

4.8.1 Competence/Knowledge of Staff and Cybersecurity Effectiveness

In order to tell the differences in the competency of staff in the eight different sectors, an ANOVA test was applied. An ANOVA test is used to compare the means of more than two groups on a continuous variable (Pallant et al., 2011). AN ANOVA test helps only by identifying whether or not the group means differ. It does not indicate the exact differences between groups. To find the significant differences between groups, post-hoc comparisons are performed.

The basic assumption for applying ANOVA test is to satisfy the condition of homogeneity of variance. If the p-value of Levene's statistics in the homogeneity of variance test is greater than 0.05, the condition of homogeneity of variance is satisfied and the ANOVA test can be applied. Therefore we conducted a test of homogeneity of variance and found that the p-value of Levene's statistics was greater than 0.05 (Table 18), so we proceeded further to do an ANOVA test.

Table 18: Test of Homogeneity of Variances (Staff competence)

Levene Statistic	**df1**	**df2**	**Sig.**
1.730	7	459	0.100

A one way analysis of variance between groups was performed to examine the effect of an employee's government sector on his/her competence/ cybersecurity

knowledge. Respondents were grouped into eight levels according to their relevant sectors or work departments (Group 1 = Social and Civic; Group 2 = Culture and Recreation; Group 3 = Transport; Group 4 = Economic Affairs; Group 5 = Health; Group 6 = Education; Group 7 = Public Order; Group 8 = Science and Technology). Table 19 presents the result of the ANOVA test. If the sig. (p-value) is less than or equal to 0.05, it indicates that at least two of the group means are different on a dependent variable, and the converse (Pallant et al., 2011). In our case, the sig. value was greater than 0.05 (p = 0.070) which explains that on the dependent variable of staff competence/cybersecurity knowledge there was no difference between the employees from the eight departments.

Table 19: ANOVA for staff competence (sector-wise)

	Sum of Squares	**Df**	**Mean Square**	**F**	**Sig.**
Between Groups	4.140	7	0.591	1.888	0.070
Within Groups	143.801	459	0.313		
Total	147.941	466			

We did not perform any post hoc analysis because the results of the ANOVA reported above supported no difference in staff competence between employees of different sectors.

4.8.1.1 Regression Analysis for study Hypothesis 1 (H1)

Linear regression analysis was conducted to test the study hypotheses. In order to find the impact of cybersecurity knowledge/staff competence on cybersecurity effectiveness, linear regression was conducted. The results of the ANOVA (see Table 20) show a significant p-value (p = 0.000), enabling us to say

that the cybersecurity knowledge/staff competence and cybersecurity effectiveness model is significant.

Table 20: ANOVA for H1

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	28.457	1	28.457	87.244	0.000[b]
	Residual	151.673	465	0.326		
	Total	180.131	466			

In order to analyze the variation in cybersecurity effectiveness due to cybersecurity knowledge/staff competence, we calculated the value of R^2, which was 0.158 (see Table 21). The value of R^2 shows that a 15.8% variation in cybersecurity effectiveness is explained by cybersecurity knowledge/staff competence.

Table 21: Model Summary for H1

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0.397[a]	0.158	0.156	0.57112

Moreover, the Beta value, 0.397 in Table 22 below shows that a one unit change in cybersecurity knowledge/staff competence can bring a 0.39 unit change in cybersecurity effectiveness, which is also significant. Hence Hypothesis 1 is supported by the results of the data analysis.

Table 22: Coefficients for H1

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.315	0.197		11.772	0.000
	Cybersecurity Knowledge	0.439	0.047	0.397	9.340	0.000

4.8.2 Support from Management and Cybersecurity Effectiveness

To analyze the difference between the staff from eight departments in terms of management support, a test of Homogeneity of Variances was conducted. The value of Levene's test is 0.239, greater than 0.05, (Table 23). It indicates that the assumption of homogeneity of variance is not violated and an ANOVA test can be applied.

Table 23: Test of Homogeneity of Variances (support from management)

Levene Statistic	df1	df2	Sig.
1.319	7	459	0.239

A one way ANOVA was conducted to gauge the influence of participants' working sector on support from top management (Table 24). The output of the ANOVA test shows a significant statistical difference at $p = 0.01$ in support for the management scores in the eight sectors: $F = 2.634$, $p = 0.01$.

Table 24: ANOVA for support from management (sector wise)

	Sum of Squares	**Df**	**Mean Square**	**F**	**Sig.**
Between Groups	8.704	7	1.243	2.634	0.011
Within Groups	216.688	459	0.472		
Total	225.392	466			

The multiple comparisons were conducted by performing post-hoc analysis, using Tukey's HSD test. The results of Tukey's HSD test reveal that the mean score for the Science and Technology (**M = 4.21**) group is statistically different from all the other groups (Social and Civic, Culture and Recreation, Transport, Economic Affairs, Education, Public Order) except the Health sector. The other groups do not differ from one another in terms of the same variable as seen in Table 25 and Table 26.

Table 25: Tuckey HSD

Employee Govt. Sector	**Subset for alpha = 0.05**	
	1	**2**
Culture and Recreation	3.61	
Public Order	3.64	
Transport	3.67	
Education	3.68	
Social and Civic	3.69	
Economic Affairs	3.71	
Health	3.81	3.81
Science and Technology		4.21
Sig.	0.880	0.165

Table 26: Multiple Comparisons for Support from Management

(I) Employ Govt Sector		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	Upper Bound
Social and Civic	Culture and Recreation	0.085	0.099	0.989	-0.216	0.386
	Transport	0.021	0.117	1.000	-0.334	0.376
	Economic Affairs	-0.042	0.134	1.000	-0.452	0.367
	Health	-0.106	0.152	0.992	-0.569	0.357
	Education	-0.170	0.170	1.000	-0.687	0.348
	Public Order	-0.233	0.188	1.000	-0.805	0.338
	Science and Technology	-0.297	0.205	0.004	-0.922	0.328
Culture and Recreation	Social and Civic	-0.361	0.223	0.989	-1.040	0.319
	Transport	-0.424	0.241	1.000	-1.158	0.309
	Economic Affairs	-0.488	0.259	0.991	-1.276	0.299
	Health	-0.552	0.276	.912	-1.393	0.290
	Education	-0.615	0.294	1.000	-1.511	0.280
	Public Order	-0.679	0.312	1.000	-1.629	0.271
	Science and Technology	-0.743	0.330	0.002	-1.747	0.261
Transport	Social and Civic	-0.807	0.347	1.000	-1.864	0.251
	Culture and Recreation	-0.870	0.365	1.000	-1.982	0.242
	Economic Affairs	-0.934	0.383	1.000	-2.100	0.232
	Health	-0.998	0.401	0.992	-2.218	0.223
	Education	-1.061	0.418	1.000	-2.335	0.213
	Public Order	-1.125	0.436	1.000	-2.453	0.203
	Science and Technology	-1.189	0.454	0.023	-2.571	0.194
Economic Affairs	Social and Civic	-1.252	0.472	1.000	-2.689	0.184
	Culture and Recreation	-1.316	0.489	0.991	-2.806	0.174
	Transport	-1.380	0.507	1.000	-2.924	0.165
	Health	-1.443	0.525	0.999	-3.042	0.155
	Education	-1.507	0.543	1.000	-3.160	0.146
	Public Order	-1.571	0.560	1.000	-3.277	0.136

Table 26: Multiple Comparisons for Support from Management (Continued)

(I) Employ Govt Sector		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	Upper Bound
Health	Science and Technology	-1.634	0.578	0.029	-3.395	0.126
	Social and Civic	-1.698	0.596	.992	-3.513	0.117
	Culture and Recreation	-1.762	0.614	.912	-3.631	0.107
	Transport	-1.825	0.631	.992	-3.748	0.097
	Economic Affairs	-1.889	0.649	.999	-3.866	0.088
	Education	-1.953	0.667	.995	-3.984	0.078
	Public Order	-2.017	0.685	.987	-4.102	0.069
	Science and Technology	-2.080	0.703	.415	-4.219	0.059
Education	Social and Civic	-2.144	0.720	1.000	-4.337	0.049
	Culture and Recreation	-2.208	0.738	1.000	-4.455	0.040
	Transport	-2.271	0.756	1.000	-4.573	0.030
	Economic Affairs	-2.335	0.774	1.000	-4.690	0.020
	Health	-2.399	0.791	0.995	-4.808	0.011
	Public Order	-2.462	0.809	1.000	-4.926	0.001
	Science and Technology	-2.526	0.827	0.034	-5.044	-0.008
Public Order	Social and Civic	-2.590	0.845	1.000	-5.161	-0.018
	Culture and Recreation	-2.653	0.862	1.000	-5.279	-0.028
	Transport	-2.717	0.880	1.000	-5.397	-0.037
	Economic Affairs	-2.781	0.898	1.000	-5.514	-0.047
	Health	-2.844	0.916	0.987	-5.632	-0.057
	Education	-2.908	0.933	1.000	-5.750	-0.066
	Science and Technology	-2.972	0.951	0.041	-5.868	-0.076
Science and Technology	Social and Civic	-3.035	0.969	0.004	-5.985	-0.085
	Culture and Recreation	-3.099	0.987	0.002	-6.103	-0.095
	Transport	-3.163	1.004	0.023	-6.221	-0.105
	Economic Affairs	-3.226	1.022	0.029	-6.339	-0.114
	Health	-3.290	1.040	0.415	-6.456	-0.124
	Education	-3.354	1.058	0.034	-6.574	-0.134
	Public Order	-3.418	1.075	0.041	-6.692	-0.143

4.8.2.1 Regression Analysis for Hypothesis 2 (H2)

In the regression analysis, the results highlighted the significance value of the F-test (0.000) in ANOVA as seen in Table 27 below. Results show that support from top management as compared to cybersecurity effectiveness model is significant.

Table 27: ANOVA for H2

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	10.792	1	10.792	29.634	0.000[b]
	Residual	169.339	465	0.364		
	Total	180.131	466			

Further, the results of the model summary (Table 28) showed an R^2 value of 0.060. This value of R^2 demonstrates that 6% of the variation in cybersecurity effectiveness (CSE) is due to support from top management.

Table 28: Model Summary for H2

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.245a	0.060	0.058	0.60346

Similarly the standardized beta value ($\beta = 0.245$) explains that a one unit change in support from management can bring a 0.24 unit change in cybersecurity effectiveness, which is also significant. The results presented in Table 29 provide full support for Hypothesis 2 (H2)

Table 29: Coefficients for H2

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.321	0.152		21.825	0.000
	Support from Management	0.219	0.040	0.245	5.444	0.000

4.8.3 Role of Technology and Cybersecurity Effectiveness

The homogeneity of variance for the role of technology in the eight different government sectors was calculated through Levene's statistics. The p-value of Levene's statistics (**p = 0.066**) shows that the assumption of homogeneity of variance is justified and an ANOVA test can be applied (Table 30).

Table 30: Test of Homogeneity of Variances (Role of Technology)

Levene Statistic	df1	df2	Sig.
2.171	7	459	0.066

The purpose of the one way analysis of variance between groups was to explore the impact of government sectors on the role of technology. We observed a significant difference at $p < 0.05$ level in the role of technology scores for the eight government sectors: $F = 2.261$, $p = 0.029$. The result specified that at least two of the government sectors were different from one another with respect to the technology deployed in these sectors (Table 31)**.**

Table 31: ANOVA for Role of Technology (sector-wise)

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	6.159	7	0.880	2.261	0.029
Within Groups	178.593	459	0.389		
Total	184.752	466			

The result of the multiple comparisons made using post-hoc analysis shows that only two sectors, i.e. health and education, were different from each other as well as from all the others: the p-value between the mean of these two sectors is somewhat significant (p = 0.057) i.e. slightly above 0.05 (Table 32).

Table 32: Multiple Comparisons for the Level of Technology

(I) Employ Govt Sector		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Social and Civic	Culture and Recreation	-0.067	0.090	1.000	-0.340	0.206
	Transport	-0.026	0.106	0.165	-0.349	0.296
	Economic Affairs	0.015	0.122	0.692	-0.357	0.386
	Health	0.056	0.138	0.251	-0.365	0.476
	Education	0.097	0.154	1.000	-0.373	0.566
	Public Order	0.137	0.170	1.000	-0.381	0.656
	Science and Technology	0.178	0.186	0.999	-0.389	0.746
Culture and Recreation	Social and Civic	0.219	0.203	1.000	-0.398	0.836
	Transport	0.260	0.219	0.529	-0.406	0.926
	Transport	1.447	0.686	0.346	-0.643	3.536
	Economic Affairs	1.487	0.702	0.818	-0.651	3.626
	Health	1.528	0.718	**0.057**	-0.659	3.716
	Public Order	1.569	0.734	0.999	-0.667	3.806
	Science and Technology	1.610	0.751	0.997	-0.675	3.896

Table 32: Multiple comparison for Level of Technology (Continued)

(I) Employ Govt Sector		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Public Order	Social and Civic	1.651	0.767	1.000	-0.684	3.986
	Culture and Recreation	1.692	0.783	1.000	-0.692	4.076
	Transport	1.733	0.799	0.867	-0.700	4.166
	Economic Affairs	1.774	0.815	0.998	-0.708	4.256
	Health	1.815	0.831	0.812	-0.716	4.346
	Education	1.856	0.847	0.999	-0.724	4.436
	Science and Technology	1.897	0.863	1.000	-0.733	4.526
Science and Technology	Social and Civic	1.937	0.880	0.999	-0.741	4.616
	Culture and Recreation	1.978	0.896	1.000	-0.749	4.706
	Transport	2.019	0.912	0.888	-0.757	4.796
	Economic Affairs	2.060	0.928	0.999	-0.765	4.886
	Health	2.101	0.944	0.835	-0.773	4.976
	Education	2.142	0.960	0.997	-0.782	5.066
	Public Order	2.183	0.976	1.000	-0.790	5.156

4.8.3.1 Regression Analysis for Hypothesis 3

The outcome of the F-test was statistically significant at $p < 0.001$ level, showing the significant impact of the regression model, meaning that the role of the technology and cybersecurity effectiveness model is significant (Table 33).

Table 33: ANOVA for H3

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	24.200	1	24.200	72.167	0.000
	Residual	155.931	465	0.335		
	Total	180.131	466			

The R^2 value indicates that a 13.4% variation in the dependent variable, cybersecurity effectiveness, is explained by the role of technology, as summarised in Table 34:

Table 34: Model Summary for H3

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.367	0.134	0.132	0.57908

Further, the beta value of 0.367 specifies that a one unit change in technology deployed by organizations may bring a 0.36 unit change in cybersecurity effectiveness, which is also significant. The results of regression analysis summarized in Table 35 highlight the fact that Hypothesis 3 of the study is fully supported.

Table 35: Coefficients for H3

Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	2.767	0.163		16.947	0.000
	Role of Technology	0.362	0.043	0.367	8.495	0.000

4.8.4 Training of staff and Cybersecurity Effectiveness

The homogeneity of variance test for the training of staff in the eight different government sectors was measured by Levene's statistics. The p-value of Levene's

statistics (p = 0.518) is greater than 0.05, satisfying the assumption of homogeneity of variance (Table 36). Therefore an ANOVA test was a useful technique to find the difference between different government sectors.

Table 36: Test of Homogeneity of Variances (Training of Staff)

Levene Statistic	df1	df2	Sig.
0.885	7	459	0.518

The output in Table 37 of a one way ANOVA test shows a significant p-value (p = 0.014) for between group analysis. It demonstrates that some of the government sectors are different from one another.

Table 37: ANOVA for Training of Staff (sector-wise)

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	6.986	7	0.998	2.551	0.014
Within Groups	179.576	459	0.391		
Total	186.562	466			

In order to know precisely which of the government sectors differ in the training of staff, a Tukey HSD test was conducted. The result shows that only three sectors are different from one another. From Table 38, it can be observed that there is a difference between the “culture and recreation” and “science and technology” sectors (P < 0.05). For further details please refer to Table 38 below.

Table 38: Multiple Comparisons for Training of Staff

(I) Employ Govt Sector		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Social and Civic	Culture and Recreation	0.193	0.090	0.392	-0.082	0.467
	Transport	-0.111	0.106	0.967	-0.434	0.212
	Economic Affairs	-0.140	0.094	0.818	-0.427	0.148
	Health	-0.140	0.136	0.970	-0.554	0.274
	Education	-0.098	0.110	0.987	-0.434	0.239
	Public Order	0.139	0.129	0.962	-0.255	0.532
	Science and Technology	-0.243	0.123	0.502	-0.619	0.132
Culture and Recreation	Social and Civic	-0.193	0.090	0.392	-0.467	0.082
	Transport	-0.304	0.123	0.208	-0.677	0.070
	Economic Affairs	-0.332	0.113	0.065	-0.675	0.011
	Health	-0.332	0.149	0.336	-0.786	0.122
	Education	-0.290	0.126	0.298	-0.675	0.095
	Public Order	-0.054	0.143	1.000	-0.489	0.381
	Science and Technology	-0.435	0.138	**0.035**	-0.855	-0.016
Transport	Social and Civic	0.111	0.106	0.967	-0.212	0.434
	Culture and Recreation	0.304	0.123	0.208	-0.070	0.677
	Economic Affairs	-0.029	0.126	1.000	-0.412	0.355
	Health	-0.029	0.159	1.000	-0.514	0.456
	Education	0.013	0.138	1.000	-0.408	0.435
	Public Order	0.250	0.154	0.735	-0.218	0.717
	Science and Technology	-0.132	0.149	0.987	-0.585	0.321

Table 38: Multiple Comparison for Training of Staff (Continued)

(I) Employ Govt Sector		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Economic Affairs	Social and Civic	0.140	0.094	0.818	-0.148	0.427
	Culture and Recreation	0.332	0.113	0.065	-0.011	0.675
	Transport	0.029	0.126	1.000	-0.355	0.412
	Health	0.000	0.152	1.000	-0.462	0.462
	Education	0.042	0.130	1.000	-0.352	0.437
	Public Order	0.278	0.146	0.545	-0.165	0.722
	Science and Technology	-0.103	0.141	0.996	-0.532	0.325
Health	Social and Civic	0.140	0.136	0.970	-0.274	0.554
	Culture and Recreation	0.332	0.149	0.336	-0.122	0.786
	Transport	0.029	0.159	1.000	-0.456	0.514
	Economic Affairs	0.000	0.152	1.000	-0.462	0.462
	Education	0.042	0.162	1.000	-0.452	0.536
	Public Order	0.278	0.175	0.758	-0.256	0.813
	Science and Technology	-0.103	0.171	0.999	-0.625	0.418
Education	Social and Civic	0.098	0.110	0.987	-0.239	0.434
	Culture and Recreation	0.290	0.126	0.298	-0.095	0.675
	Transport	-0.013	0.138	1.000	-0.435	0.408
	Economic Affairs	-0.042	0.130	1.000	-0.437	0.352
	Health	-0.042	0.162	1.000	-0.536	0.452
	Public Order	-0.236	0.157	0.803	-0.241	0.713
	Science and Technology	-0.146	0.152	0.980	-0.608	0.317
Public Order	Social and Civic	-0.139	0.129	0.962	-0.532	0.255
	Culture and Recreation	0.054	0.143	1.000	-0.381	0.489
	Transport	-0.250	0.154	0.735	-0.717	0.218
	Economic Affairs	-0.278	0.146	0.545	-0.722	0.165
	Health	-0.278	0.175	0.758	-0.813	0.256

Table 38: Multiple Comparison for Training of Staff (Continued)

(I) Employ Govt Sector		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Science and Technology	Education	-0.236	0.157	0.803	-0.713	0.241
	Science and Technology	-0.382	0.166	0.295	-0.887	0.124
	Social and Civic	0.243	0.123	0.502	-0.132	0.619
	Culture and Recreation	0.43568*	0.138	**0.035**	0.016	0.855
	Transport	-0.132	0.149	0.987	-0.321	0.585
	Economic Affairs	0.103	0.141	0.996	-0.325	0.532
	Health	0.103	0.171	0.999	-0.418	0.625
	Education	0.146	0.152	0.980	-0.317	0.608
	Public Order	0.382	0.166	0.295	-0.124	0.887

4.8.4.1. Regression Analysis for Hypothesis 4

The linear regression model is presented in Table 39. The significant value of the F-test shows a statistically significant regression model of training of staff and cybersecurity effectiveness.

Table 39: ANOVA for H4

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	25.078	1	25.078	75.209	0.000
	Residual	155.053	465	0.333		
	Total	180.131	466			

The R^2 value of 0.139 shows that 13.9% of the variation in cybersecurity effectiveness is due to the training of staff. These results are presented in Table 40 below.

Table 40: Model Summary for H4

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.373	0.139	0.137	0.57745

Moreover, the standardized beta value of 0.373 indicates that a one unit change in training of staff influenced a 0.37 unit change in cybersecurity effectiveness, which is also significant (Table 41). Therefore it supports our Hypothesis 4.

Table 41: Coefficients for H4

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.648	0.174		15.261	0.000
	Training of staff	0.367	0.042	0.373	8.672	0.000

4.8.5 Strategic Plan and Cybersecurity Effectiveness

The test of homogeneity of variance (see Table 42) showed the significant value ($p = 0.310$) to be greater than 0.05 and thus satisfied the condition of applying an ANOVA test of variance.

Table 42: Test of Homogeneity of Variances (Strategic Plan)

Levene Statistic	df1	df2	Sig.
1.185	7	459	0.310

The p-value of a one way ANOVA test was greater than 0.05 (i.e. p = 0.252), which confirmed that there was no difference between the eight government sectors on the basis of strategic plans (see Table 43 below). Since the ANOVA results were insignificant, no post hoc analysis was performed for this variable.

Table 43: ANOVA for Strategic Plan (sector-wise)

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	2.720	7	0.389	1.293	0.252
Within Groups	137.942	459	0.301		
Total	140.662	466			

4.8.5.1 Regression Analysis for Hypothesis 5

The significant value of the F-test in ANOVA in Table 44 showed that government sectors have strategic plans and that the cybersecurity effectiveness regression model was significant.

Table 44: ANOVA for H5

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	20.412	1	20.412	59.427	0.000
	Residual	159.719	465	0.343		
	Total	180.131	466			

The R^2 value of 0.113 in Table 45 showed an 11.3% variation in the dependent variable; cybersecurity effectiveness was explained by the independent variable, i.e., the strategic plan.

Table 45: Model Summary for H5

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.337	0.113	0.111	0.58607

The coefficients in the results in Table 46 showing a beta value of 0.337 indicates that a one unit change in strategic plans may affect staff cybersecurity effectiveness by 0.33 units and this impact is also significant, supporting our Hypothesis 5. The detailed results are presented in Table 46 below.

Table 46: Coefficients for H5

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.629	0.197		13.325	0.000
	SP_mean1	0.381	0.049	0.337	7.709	0.000

4.8.6 Awareness of Users and Cybersecurity Effectiveness

The significant value of Levene's test of homogeneity of variance (greater than 0.05) in Table 47 endorsed the assumption that an ANOVA test of variance could be applied.

Table 47: Test of Homogeneity of Variances (Awareness of Users)

Levene Statistic	df1	df2	Sig.
1.514	7	458	0.160

The p-value of a one way ANOVA test was greater than 0.05 (i.e. p = 0.101), which made it clear that there was no difference between the staff of the eight government sectors on the basis of awareness about cybersecurity issues (please see Table 48 below). Therefore, we did not apply a post hoc analysis.

Table 48: ANOVA for Awareness (sector-wise)

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	4.663	7	0.666	1.726	0.101
Within Groups	176.765	458	0.386		
Total	181.427	465			

4.8.6.1 Regression Analysis for Hypothesis 6

The impact of the awareness of users about cybersecurity on its effectiveness was calculated by using linear regression analysis. The regression model shows

significant value at a $p < 0.001$ level, indicating the significance of the regression model of awareness of users and cybersecurity effectiveness (Table 49).

Table 49: ANOVA for H6

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	16.260	1	20.412	46.427	0.000
	Residual	163.719	465	0.343		
	Total	180.131	466			

Although the F-test showed a significant regression model of independent and dependent variables, the smaller value of R^2 showed a smaller variation in cybersecurity effectiveness due to the awareness of users. There was a 9% change in the dependent variable due to awareness of users (see Table 50).

Table 50: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.301	0.090	0.088	0.59415

The coefficients table, Table 51, shows a beta value of 0.301 significant at $p < 0.001$. These results indicate that one unit change in the awareness of users may affect staff cybersecurity effectiveness by 0.30 units and this impact is also significant, supporting the study Hypothesis 6. The detailed results are presented below.

Table 51: Coefficients for H6

		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.929	0.179		16.325	0.000
	Awareness of users	0.299	0.049	0.301	6.709	0.000

4.9 Multiple Regression Analysis

In addition to the above discussions were impact of the six independent variables on dependent variable (CSE) has been evaluated separately, multiple regression analysis is also performed to know the combined effect of all independent variables on dependent variable. The results of multiple regression analysis presented in Table 52 shows a significant impact (F = 72.167, p = 0.000) of independent variables on dependent variable, cybersecurity effectiveness.

Table 52: ANNOVA for the Multiple Regression Test

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	24.200	1	24.200	72.167	0.000
	Residual	155.931	465	0.335		
	Total	180.131	466			

Furthermore, Table 53 shows the R-square value for the combined model which is 0.317. This values shows that 31% change in depending variable is

occurring due to the six (6) independent variables used in current study as seen below;

Table 53: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.563[a]	0.317	0.308	0.51768

Additionally, the individual independent variable effect on dependent variable is also shown in Table 54. Results suggested that all independent variables have significant impact on dependent variable. Awareness of users has highest impact ($\beta = 0.230$, $p = 0.000$) on cybersecurity effectiveness followed by training of staff ($\beta = 0.192$, $p = 0.000$). Complete detail is given in Table 55 below.

Table 54: Multiple Regression Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0.348	0.265		1.315	0.189
Competence/knowledge of staff	0.150	0.053	0.136	2.818	0.005
Level of Technology	0.130	0.045	0.132	2.921	0.004
Support from Mgt	0.100	0.037	0.112	2.747	0.006
Training of Staff	0.188	0.044	0.192	4.314	0.000
Strategic Plans	0.156	0.050	0.138	3.119	0.002
Awareness of Users	0.229	0.039	0.230	5.885	0.000

4.10 Summary of Hypotheses Testing

A. Research Hypothesis H1: There is a positive relationship between the Competence/knowledge of staff of information security and cybersecurity effectiveness.

In addition to demographic statistical results presented previously, linear regression analysis was conducted to evaluate the relationship between Competence/knowledge of staff of information security and cybersecurity effectiveness of their organisations. The significant p-value of F-test shows the association between competence/knowledge of staff of information security and cybersecurity effectiveness. Further, the R^2 value (0.158) shows a direct positive impact of competence/knowledge of staff of information security on cybersecurity effectiveness.

In order to generalize our results, the impact of staff competency/knowledge on cybersecurity effectiveness was compared among eight different departments. The p-value (0.070) of ANOVA results show that there is no difference among employees of eight sectors on the basis of their competency/knowledge about cyber information.

B. Research Hypothesis H2: There is a positive relationship between senior management support and cybersecurity effectiveness.

Impact of support from top management on employees' performance is a widely studied topic in field of management. Support from top management brings several positive results on employees' behaviour, their well-being and their performance which in turn helps organizations to achieve their goals. The empirical

support for our hypothesis reveal the importance of management support in generating effective cybersecurity framework. These results were in line with theoretical deliberations discussed in literature where authors emphasized that; "cybersecurity is a management issue" which requires management intervention through establishment of appropriate cyber and information security strategies, policies and frameworks;

(Asante, 2011; NIST, 2014, Symantec, 2013; and Dutton and Duncan, 1987) among others. Our results offer interesting findings that establishment of an effective cybersecurity system does not only require user competency but also demands for management cooperation.

The comparative ANOVA test is applied on eight different government entities to analyse if there any difference among the support provided by top management team. The results of ANOVA test show no difference among all departments with respect to management support for effective cybersecurity system. It means employees from all departments need equal support from management for effective functioning of their information security.

C. Research Hypothesis H3: There is a relationship between role of technology and cybersecurity effectiveness

New security challenges place significant demands for highly secure software and hardware platforms to maintain appropriate level of confidentiality, integrity and access to critical data (Conklin, 2006). In analyzing the factors of developing effective cybersecurity framework, the most critical factor is the role of technology. Impact of technology in managing cyber-threats is widely acknowledged among practitioners and academicians. The application of regression test in current study

show statistically significant p-value ($p < 0.001$) of F-test. We can infer from these results that role of technology has a direct positive impact on cybersecurity effectiveness model. It includes all sort of measures i.e. use of antivirus, firewalls etc.

Unlike other factors, the impact of role of technology on cybersecurity system shows difference among some departments. The significant p-value of ANOVA test indicates that at least two of the departments are differ with respect to their use of technology. The post-hoc analysis further discloses that two of the departments, health and education are different with each other on role of technology. It might be the difference in types of technology two departments deployed.

D. Research Hypothesis H4: There is a positive relationship between cybersecurity training of staff and cybersecurity effectiveness.

Training of staff enriches end user security knowledge which in turn help them to manage cyber-threats effectively. Scholars agree that training of staff enhances their capacity to handle cyberattacks. The significant value of F-test shows a statistically significant regression model of training of staff and cybersecurity effectiveness. This significance level supports the study hypothesis H4. From the study results, it eminent that management in Abu Dhabi government entities needs to establish and maintain appropriate cybersecurity training program for all employees to enable acquisition of cybersecurity knowledge especially for the less experienced workers with little or no knowledge of cyber and information security skills.

E. Research Hypothesis H5. There is a positive relationship between the presence of cybersecurity strategic plans and cybersecurity effectiveness

Impact of strategic plans on cybersecurity effectiveness is not clearly known. Past studies on this issue presented a mixed view. The results of linear regression shows a significant positive relationship between cybersecurity strategic plans and cybersecurity effectiveness. Moreover, the data collected from eight different departments also show similar findings with regard to the relationship between cybersecurity strategic plans and cybersecurity effectiveness. These regression results were in support of the study hypothesis H5 which confirms that when developing strategic plans, all Abu Dhabi government entities need to consider cybersecurity as part of the planning process to ensure effectiveness of the established cyber and information security defences. In the next section we discuss the recommendations of this study on cybersecurity effectiveness in Abu Dhabi government entities.

F. Research Hypothesis H6. There is a positive relationship between awareness of users about cybersecurity and cybersecurity effectiveness

Users' awareness about cybersecurity can be helpful in managing cyber-threats and maintaining effective cybersecurity system. The impact of awareness of users about cybersecurity on its effectiveness was calculated by using linear regression analysis. The regression model shows significant value at $p < 0.001$ level indicating the significant regression model of awareness of users and cybersecurity effectiveness. Although the F-test shows a significant regression model of independent and dependent variable, the smaller value of R^2 shows a smaller variation in cybersecurity effectiveness due to awareness of users. There is 9%

change in dependent variable due to awareness of awareness of users.

4.10.1 Comparison of Departments based on Cybersecurity Effectiveness

A departmental comparison based on the performance of the different government entities in terms of cybersecurity effectiveness is shown in Table 55 below. For this study, the data were collected from eight different public sector departments of the Abu Dhabi government. It is interesting to investigate whether or not these departments are different in terms of effectiveness with regard to their cybersecurity system. We divide cybersecurity effectiveness into three categories (low, medium and high. The departments with cybersecurity mean ranges from 1 to 3 are classified as low while departments with a cybersecurity mean value greater than 3 but less than 4 are classified as medium. Finally, the departments with a cybersecurity mean value greater than 4 are considered highly effective in terms of their cybersecurity system. It is worth noting that all public sector departments are highly effective as regards their cybersecurity system except the public order department, which is in the medium category of cybersecurity effectiveness. The comparison also reveals that no department shows low effectiveness in this regards. Full details of the departmental cybersecurity comparison are given below.

Table 55: Department Wise Effectivity of Cybersecurity System

Department	N	CE Mean	Std. Deviation	High/Medium/ Low
Social and Civic	180	4.09	0.65	High
Culture and Recreation	66	4.07	0.55	High
Transport	43	4.24	0.43	High
Economic Affairs	58	4.25	0.59	High
Health	24	4.21	0.44	High
Education	39	4.08	0.75	High
Public Order	27	3.83	0.76	Medium
Science and Technology	30	4.37	0.50	High
Total	467	4.13	0.62	High

Note: CE Mean 1-3 = Low effectiveness, CE Mean > 3 but < 4 = Medium effectiveness, CE Mean > 4 = High effectiveness

Table 55 above and Figure 20 below present that, while all departments show high performance, four departments in particular stand out when it comes to Cybersecurity Effectiveness. The departmental results show that Science and Technology (M = 4.37), Economic Affairs (M = 4.25), Transport (M = 4.24) and Health (M = 4.21) performed better in terms of cybersecurity effectiveness than did the Social and Civic, Culture and Recreation, Education and Public Order departments. This is attributed to the strong cybersecurity systems established in these departments and the highly qualified staff employed there.

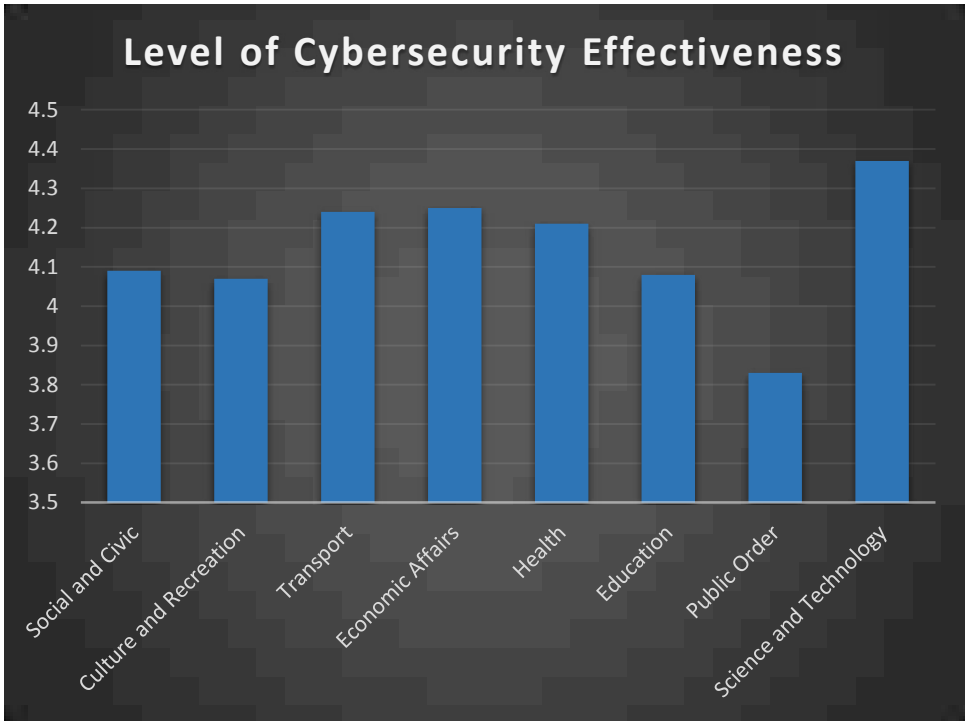


Figure 20: Departmental Cybersecurity Effectiveness comparison

4.11 Summary of the Results

The detailed analyses were performed using IBM SPSS 21. All the hypotheses were tested using linear regression. Table 56 below provides a summary of the hypotheses testing, which shows that all the proposed hypotheses were supported by the empirical data. This exhibits the important role of the predictors proposed in our model in developing cybersecurity effectiveness.

Table 56: Summary of Results

Hypothesis	Variables	Beta Value	Significance	Accepted /Rejected
H1	Competence →CSE	0.397	0.000	Accepted
H2	Support from mgt. →CSE	0.245	0.000	Accepted
H3	Role of tech. →CSE	0.367	0.000	Accepted
H4	Training of staff →CSE	0.373	0.000	Accepted
H5	Strategic plan →CSE	0.337	0.000	Accepted
H6	Awareness of users →CSE	0.301	0.000	Accepted

4.12 Conclusion

The empirical evidence showed that all the six factors (staff competency/knowledge, support from top management, role of technology, training of staff, strategic plans and awareness of users) play a significant role in developing effective cybersecurity systems. The support for the proposed hypotheses reveals that for an effective cybersecurity system all six factors are equally important for the eight sectors. This study has several important implications for both practitioners and academics. These are discussed in detail in Chapter five below.

Chapter 5: Discussions and Implications of the Study

5.1 Introduction

The previous chapter presented results of data analysis process through descriptive and inferential statistics. Several statistical tests have been conducted including post-hoc analysis, One Way ANOVA, linear regression and multiple regressions to assess the statistical significance of the casual relationships between different study constructs with the goal of testing the different study hypotheses and answering of the research questions.

In this chapter, the researcher presents a discussion and summary of findings from the survey results presented in the previous chapter in comparison with the key research hypotheses as well as study objectives and deduces the overall contribution and implication of the study compared to the theoretical and practical frameworks and strategies critically reviewed in literature. Further, the chapter highlights the contributions of the study and provides recommendations to managers and future directions to the researchers bearing in mind limitations of the study. Finally, a summary of chapters and conclusion is provided at the end. The design of the chapter is presented Figure 21 below:

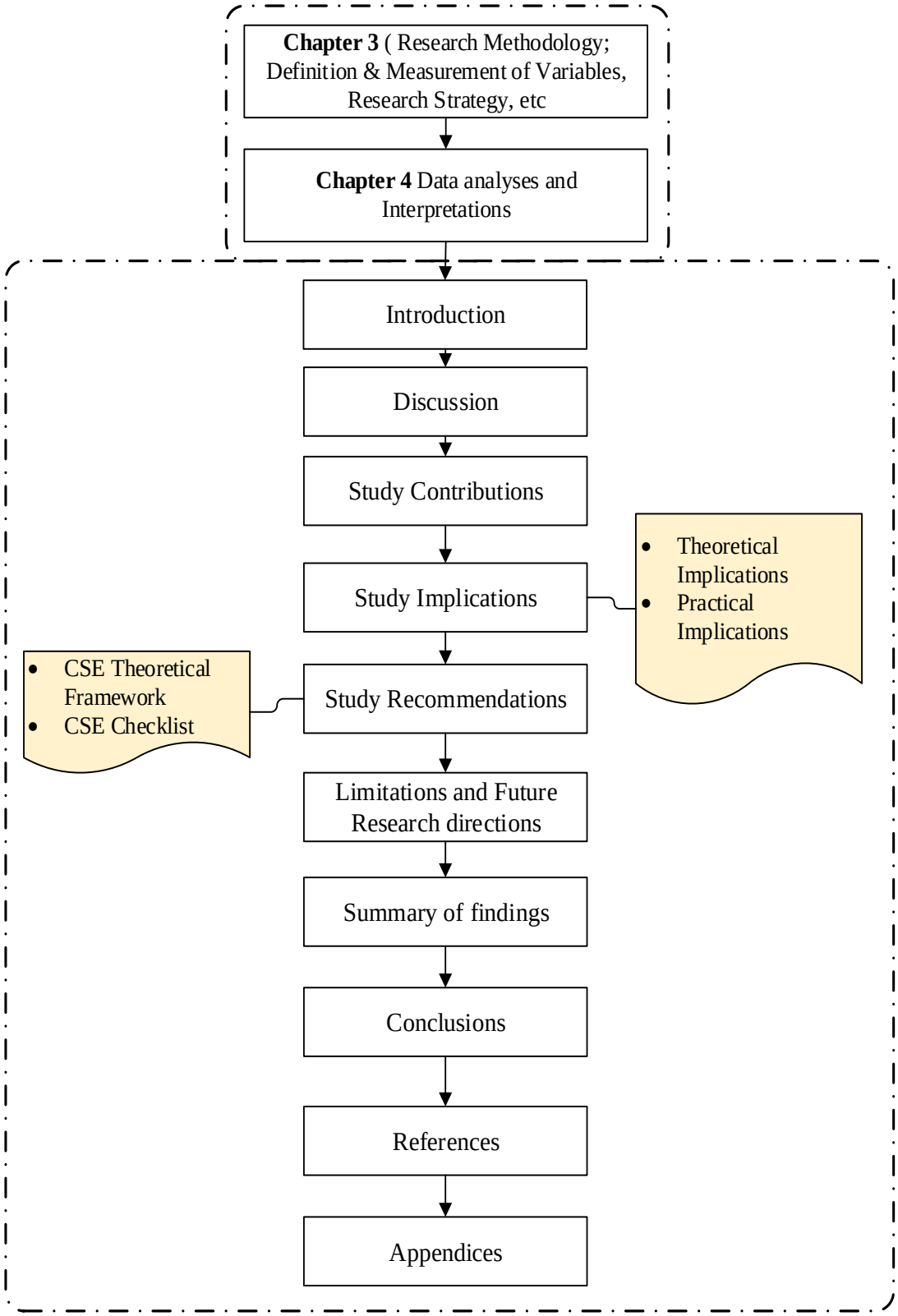


Figure 21: Design of Chapter Five

5.2 Discussion

Safe and secure management of the cyberspace system is critically important for information centered organizations. Although most of these organizations have equipped themselves with the latest technologies for prevention of cyberattacks and other vulnerabilities, incidences of cyber intrusions are still evident globally and the UAE in particular. Therefore, this study has focused on identifying additional human and organizational factors responsible for evaluating the effectiveness of a cybersecurity system in an organization. More specifically, areas of end-user security competency and senior management support provided to the system have attained higher attention in various organizations. In a cybersecurity framework, observing end-user security competence is very much challenging due to the divergent views and preferences.

In this dissertation, the researcher developed and tested a theoretical framework with a checklist for enhancing cybersecurity effectiveness in government organizations (the case study of Abu Dhabi government entities). Impact of end-user capacity building factors were examined to enrich readers' understanding of employee compliance to cybersecurity policies. Based on the data collected and analyzed from the eight different entity types, the model was tested empirically. Study findings advocate that security behaviors can be predisposed through extrinsic as well as intrinsic motivators. Similarly, the staff competency to handle cybersecurity issues is also controlled by their individual as well as organizational factors. Further, implications of the study results are discussed for theory and practice.

The major goal of this study was to develop a framework for the evaluation

of cybersecurity effectiveness in Abu Dhabi government entities. Specifically, the study was intended to identify the factors that contribute to cybersecurity effectiveness of an organization more especially determining the role of management in the prevention of cyberattacks, the role of training and awareness in resisting cyberattacks, the role of technology level in building defences against cyberattacks, and examining the relationship between the competence/ knowledge of employees and cybersecurity effectiveness as well as the role cybersecurity strategic planning in ensuring an effective cybersecurity system.

Moreover, this study validates the critical role of some human and organizational factors that help in augmenting the effectiveness of cybersecurity defence system. Acknowledging the idiosyncratic features of UAE public organizations, the researcher, based on the findings of the study in consultation with 10 experts in the practice and 2 academic professors, proposed a set of factors responsible for improving cybersecurity effectiveness. The research postulated that competence/knowledge of staff, support from senior management, level of technology, training of staff, cybersecurity strategic planning and awareness of users about cybersecurity have significant bearing on bringing effectiveness to the cybersecurity defence system of an organization.

The survey, conducted in eight different public sector organizations of the Abu Dhabi government, revealed some important findings; first, when establishing an effective cybersecurity framework, both human as well as organizational level variables are important. At individual level, employees need to have sufficient knowledge and awareness about cybersecurity issues to tackle cyberattacks. Further, the research also found out that cybersecurity training to employees especially the

information security staff provides an imperative element in developing effective cybersecurity defense. In addition to individual level factors, this study highlighted some important organizational level factors contributing towards operative cybersecurity system. The researcher found that support from senior management and organization's strategic plans about cybersecurity help employees in effective implementation of cybersecurity plans and policies. Finally, this research supports the previous study, (Rowe et al., 2011) that different technological tools (firewalls, data encryption, anti-malware, anti-spyware and anti-virus scanners) are indispensable in generating effective cybersecurity model. Findings of other authors have also lent support for the above finding observed in this research study (Rees, 2011; NIST, 2014; and Hiller and Russell, 2015) among others.

A second significant upshot that emerges from this research is the generalizability of all antecedents to the eight different sectors. The data was collected from eight different public sector entities including social and civic, culture and recreation, transport, economic affairs, health, education, public order and science and technology. The results from ANOVA, linear and multiple regression tests show that all six factors are equally important in the eight different entities in framing an effective cybersecurity system.

5.3 Contributions

Despite the high rate of cybersecurity problems, systems administrators and information security professionals continue to take few effective precautions. During interviews and discussions with the experts as well as organizations functionaries it was observed that this lack of precaution was partly because of the lack a meaningful

tool or framework as well as checklist to assess the effectiveness of cybersecurity system within the different government entities. In order to gain an effective security position, organizations must overcome this drawback with effective measures. This study therefore, contributes to literature by providing a useful framework and checklist for evaluation of cybersecurity effectiveness in Abu Dhabi government entities. A gap was revealed in literature concerning existing cybersecurity frameworks that majorly focus on technological mechanisms for identification, detection, prevention and analysis of associated risks, while others were found inadequate with a focus on the European or American standards which may not fully address cyber and information security issues in cultural setup of the region. Additionally these frameworks were found complex especially when it comes to interpretation and implementation. Therefore, the researcher proposed additional strategies to strengthen the existing technological strategies including the introduction of culturally sensitive cybersecurity training and awareness programmes, ensuring strong legal framework, strong management support, and attracting and retaining experienced information technology professionals in government entities and incorporation of cybersecurity strategic planning in the organization wide planning.

An important contribution of this study is the comparison of effective cybersecurity measures in eight different public entities in Abu Dhabi government out of which Science and Technology, Economic affairs, Transport and Health showed better performance and readiness in terms cybersecurity counter measures in place. The results from multiple regressions conducted on all the six study factors combined in a single model showed that all six factors make a significant difference

to firms' cybersecurity system with the R-square value of 0.317 for the combined model signifying that 32% change in an organization's cybersecurity effectiveness (CSE) is occurring due to the six independent variables in the study combined with standardised coefficients showing awareness of users ($\beta = 0.230$, $p = 0.000$) and training of staff ($\beta = 0.192$, $p = 0.000$) contributing the highest impact to an organization's cybersecurity system. All eight entities have different culture, values and cybersecurity issues which enhances the generalizability and reliability of study results by confirming that six factors are critical in developing effective cybersecurity defence mechanism in line with several scholars previously reviewed in literature, (Nambiro et al., 2014; Abawajy, 2014; Ahn et al., 2013; Aloul, 2010 and Asante et al., 2011) among others.

The current research focuses on recommending new ways of approaching cybersecurity risks. A major goal of the research was to analyse if employee development and organizational support systems are effective in improving cybersecurity system. Application of different factors to the eight different entities highlighted that both employee effectiveness and organizational effectiveness are essential in managing cybersecurity issues.

Although the sensitivity of information security is well acknowledged among IT professionals, managers and government entities, information is often protected without considering its form or location or the competencies of the people involved in protection. Cybersecurity deals not only with the protection of information but also with security and development of the person using it (Von Solms and Van, 2013).

5.4 Study Implications

5.4.1 Theoretical Implications

In this study, a framework for evaluating the effectiveness of the existing cybersecurity defences in Abu Dhabi government entities has been proposed. The framework is based on six major factors; *1*: Competency/ Knowledge of information security staff, *2:* Senior management support, *3:* Level of technology deployed *4*: Training of staff, *5:* Presence of cybersecurity strategic plans and *6:* Awareness of users in addition to the existing Laws and regulations that support and protect cybersecurity.

The present study has several theoretical implications in cybersecurity regulations literature. It is among the few endeavours to investigate the antecedents of effective cybersecurity system. Past researches mainly emphasized technology as the major variable in cybersecurity with little or no focus on human and organizational factors. This research adds to this body of knowledge by proposing that, in addition to technological sophistication, organizations should focus on human factors as well including; (competency/knowledge of staff, awareness of users about cybersecurity, regulations and the training of staff) for examining effectiveness of cybersecurity issues. Therefore, this research opens new dimensions for future scholars to view cybersecurity issue from a different angle.

The necessity for a behaviourally-rooted cybersecurity framework is addressed in this research. Drawing on intrinsic motivation theory, the researcher endeavours to analyse cybersecurity related employee and organizational competencies in organizations. The findings of the study confirms that there exists a

real necessity for effective enhancement of employee's capacity to manage cybercrimes, in the organizations under study. Kshetri (2005) explains that employees' behaviour for doing a task is affected by two motivation factors: (1) intrinsic and (2) extrinsic. In cybersecurity context, results of this study confirm the role of intrinsic as well as extrinsic motivating factors in strengthening security behaviours of firms.

5.5 Proposed Framework

The cybercrime threats force policymakers to suggest new regulations in order to prevent from cyberattacks. The framework proposed in this study consists of strategies beneficial to such stakeholders. The government policy makers can utilize the findings of our study for defining crucial policies on cybersecurity regulations. Our research guides lawmakers to consider some factors more critically than others while formulating cybersecurity regulations.

The framework proposed in this study is worthwhile for organizational managers, leaders and executives. These people are supposed to implement cybersecurity policies in their organizations. For that reason, this study leads them in implementing cybersecurity strategies while considering different individual and organizational level factors. The management of organization must know that in order to implement cybersecurity strategies effectively, their employees must be competent enough and have sufficient training and should be well aware of cybersecurity issues. Further, the study findings helps managers in supporting their team while efficiently applying cybersecurity regulations. Finally, the research outcomes are equally important for information security consultants and trainers.

Trainers can use this research for making a broad checklist of competencies that need to be developed by IT personnel. IT personnel equipped with capabilities like cybersecurity knowledge, awareness and training can handle cybersecurity issues better.

Below, we present the proposed theoretical framework for evaluating the effectiveness of cybersecurity systems that could be used by authorities in Abu Dhabi government entities. The framework has been based on the six factors, as summarised in Figure 22 below after which the factors are related to the proposed checklist to enable evaluation in terms of CSE as discussed in section 5.5.1.

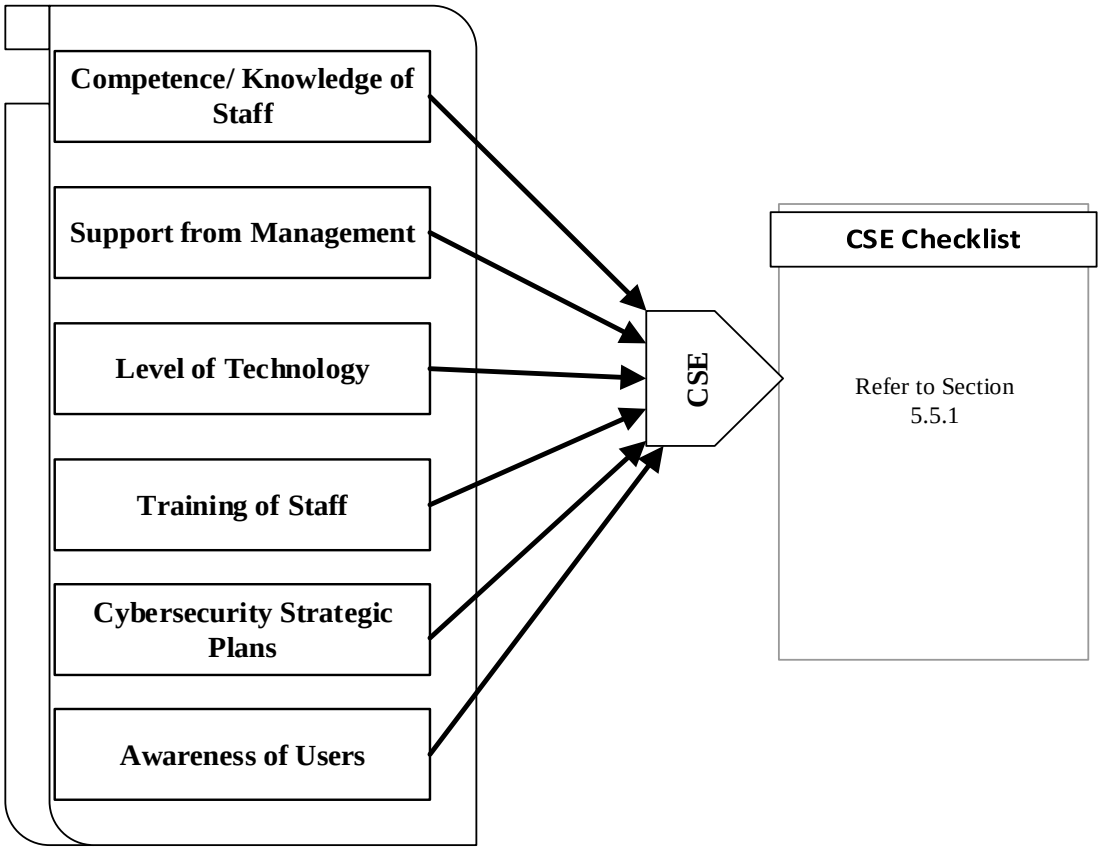


Figure 22: Proposed Theoretical Framework

Furthermore, Figure 23 below shows the proposed research framework from which the entire study has been grounded.

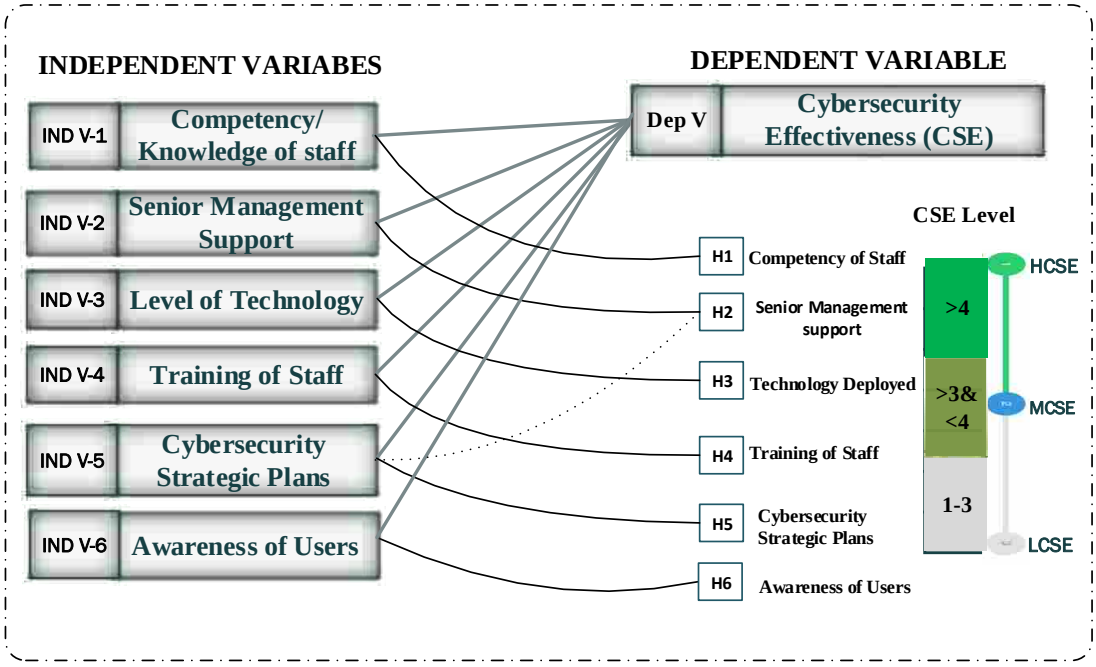


Figure 23: Proposed Research Framework

In the next section, we discuss the proposed CSE checklist with respect to the proposed pillars in details.

5.5.1 Cybersecurity Checklist

The checklist proposed in tables 57- 60 for this study was developed in consultation with 10 experts in the subject area within the Abu Dhabi Government, guidelines from 2 academic Professors, the researcher's vast experience of 17 years in region's cyber and information security domain, empirical evidence revealed from international standards on cyber and information security such as the ADSIC II Information Security Guidelines, 2013, ISO / IEC 27001; 2013; ISMS standard, ISO/ IEC 27032; 2012; Cybersecurity Standard, ISO / IEC 27035, International Standard

for incident management and the NIST (2014) risk based framework for information security implementation and process improvement to enable Abu Dhabi government entities assess the status of their existing cybersecurity defences, the severity of potential security breaches and analyse the potential cyber and information security risks associated with their entities to ensure appropriate resource allocation and overall improvement of their entity's cybersecurity systems. The checklist was formulated basing on the six (6) pillars (factors) for evaluation of cybersecurity effectiveness in Abu Dhabi government entities as cited in the proposed cybersecurity theoretical framework.

Furthermore, to establish an appropriate CSE evaluation scale, the researcher modified the Capability Maturity Model Integration (CMMI) software process evaluation scaling technique explained earlier in the literature to come up with a measurement scale that government entities can use to verify their level of cybersecurity effectiveness (CSE). According to this modified scale for the study checklist, a Level of 1 indicates that the organization has taken initial steps towards implementing measures that contribute towards CSE; Level of 2 indicates that these measures are repeatable and show evidence of improvement; Level 3 indicates that these CSE measures are defined and can be referenced and evidenced in the organization's process assets. Meanwhile, Level 4 shows that the organization has well managed CSE operations and the highest level of CSE evaluation in an organization is Level 5, which shows that the all the six factors in addition to a strong technology foundation are optimized and understood by all users in the organization.

In addition, as previously presented in Chapter 4, departmental cybersecurity effectiveness is considered low if the scores are 1 – 3; medium if they are greater

than 3 but less than 4 and high wherever they are greater than 4 with a score of 5 being maximum to scale. It is the researcher's hope that assessors of cybersecurity preparedness in Abu Dhabi government entities can apply or modify this scale to evaluate their cybersecurity effectiveness levels. The checklist has been organized according to the pertinent factors to ease implementation and allow focus by different departmental groups to different areas of concern. For instance, to complete and evaluate the competency/knowledge of information security staff pillar, the assessor enters a score of 1 – 5 on the last column for each sub-factor then calculates the average for the factor. At the end of the evaluation process, the level of Competency/knowledge of Information Security will have a cybersecurity effectiveness level of between 1 and 5 as indicated in the Table 57.

Meanwhile, for Support from Management factor on the checklist, the assessor enters a score of 1 – 5 on the last column for each sub-factor then calculates the average for the factor. At the end of the evaluation process, Support from Management factor on the scale will have a cybersecurity effectiveness level between 1 and 5 representing the performance level of the organization to scale in terms of CSE as seen in Table 58.

Below, the researcher presents the CSE evaluation checklist proposed for the study based on the six pillars; 1) Competence/ Knowledge of staff, 2) Support from Management, 3) Level of Technology, 4) Training of Staff, 5) Strategic Plans and 6) Awareness of Users as described in the study theoretical framework in Figure 22.

Table 57: Competence/Knowledge of Staff Checklist

CSE Evaluation Pillars		Proposed Abu Dhabi Government Department CSE-Checklist based on 6 - Pillars	Check Options *I=Initial; M=Managed; D=Defined; QM=Quantitatively Managed; O=Optimized*				
		**Pillar 1: Competence/Knowledge of Staff**	I	M	D	QM	O
	i.	Organization has well qualified and experienced staff assigned to cybersecurity functions.					
	ii.	Most Cybersecurity staff have relevant industry certifications academic credentials on Cyber and information security.					
	iii.	Cybersecurity staff maintain up to date industry knowledge in their domain of expertise.					
	iv.	Cybersecurity staff have membership in international professional organizations.					
	v	Experienced staff are retained in the organization					
	vi	The organization has subscribed and can access up to date Libraries on cyber and Information security.					
		Average for Competence/ Knowledge of Staff					

Table 58: Support from Management Checklist

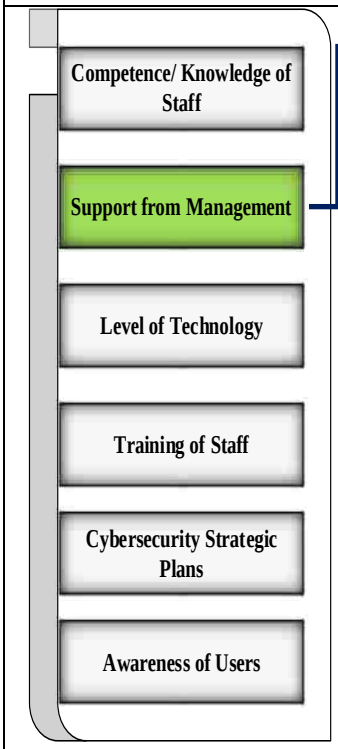
CSE Evaluation Pillars	Proposed Abu Dhabi Government Department CSE-Checklist based on 6 - Pillars		Check Options *I= Initial; M= Managed; D=Defined; QM=Quantitatively Managed; O=Optimized*				
			I	M	D	QM	O
	**Pillar 2: Support from Management**						
	A	Development and Communication of Cybersecurity Security Policies					
	i.	Organization has developed cybersecurity policies.					
	ii.	Cybersecurity policies are approved by the Chief Executive Officer or equivalent					
	iii.	The policies are published within the organization in places where they are easily seen.					
	iv.	The policies are communicated to all employees when they are first hired and on a regular basis thereafter					
	v.	The policies are shared with all relevant external parties.					
	B	Review and updating of Cybersecurity Policies					
	i.	Cybersecurity policies are revised at least once a year and whenever need arises					
	ii.	Changes to policies are approved by senior management and communicated to all the staff					

Table 58: Support from Management Checklist (Continued)

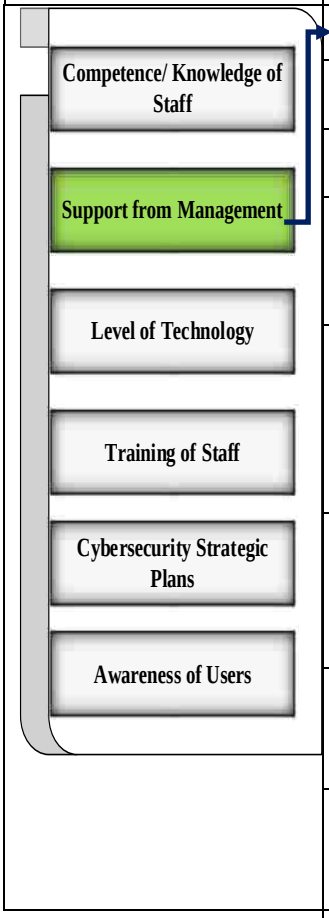
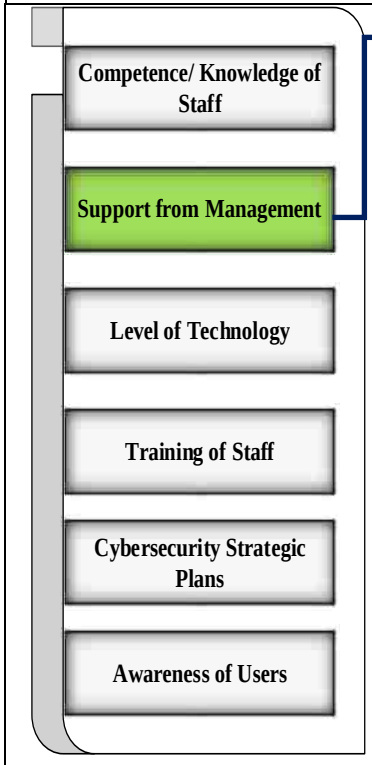
CSE Evaluation Pillars	Proposed Abu Dhabi Government Department CSE-Checklist based on 6 - Pillars			Check Options *I=Initial; M=Managed; D=Defined; QM=Quantitatively Managed; O=Optimized*				
				I	M	D	QM	O
	**Pillar 2: Support from Management**							
	C		Cyber Security Roles and Responsibilities					
		i	Chief Information Security Officer (CISO) roles are well defined.					
		ii	There is clear segregation between CISO and IT roles and responsibilities in the organization.					
		iii	The cybersecurity department in the organization maintains contact and engagement with relevant UAE organizations such as NESA, AE-Cert and ADSIC.					
		iv	The CISO in the organization reports directly to the Chief Executive Officer (CEO) or equivalent.					
		v	The Information Security department maintains contacts with relevant external organizations.					
		vi	Information Security requirements are integrated into project management functions.					
	D		Budget					
		i.	The organization has an annual line item on cybersecurity activities.					
		ii.	Budgets for IT Cybersecurity equipment is separated from other general budget and allocated appropriately to purchase the latest Cyber Intrusion hardware.					

Table 58: Support from Management Checklist (Continued)

CSE Evaluation Pillars	Proposed Abu Dhabi Government Department CSE-Checklist based on 6 - Pillars		Check Options *I=Initial; M=Managed; D=Defined; QM=Quantitatively Managed; O=Optimized*				
			I	M	D	QM	O
	**Pillar 2: Support from Management**						
	E.	Planning					
	i.	Organization has established strategic plans.					
	ii.	Cybersecurity measures and efforts are explicitly stated in the strategic plans.					
	iii.	Cybersecurity plans are documented and distributed within the organization.					
	iv.	Cybersecurity plans are reviewed and updated annually.					
	F.	Cyber Security Key Performance Indicators					
	i.	Organization has metrics that measures performance of cyber security activities					
	ii.	Organization has established overall monitoring tools for cyber-security performance.					
	Average for Support of Management						

For the Level of Technology factor on the checklist, the assessor enters a score of 1 – 5 on the last column for each sub-factor then calculates the average for the factor. At the end of the evaluation process, the level of Technology will have a cybersecurity effectiveness level assessed between 1 and 5 as indicated in Table 59 below.

Table 59: Level of Technology Deployed Checklist

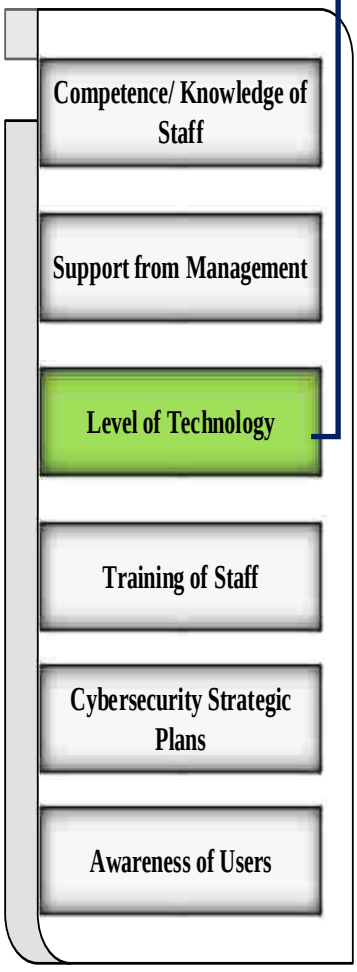
CSE Evaluation Pillars	Proposed Abu Dhabi Government Department CSE-Checklist based on 6 - Pillars			Check Options *I=Initial; M=Managed; D=Defined; QM=Quantitatively Managed; O=Optimized*				
	Pillar 3: Level of Technology			I	M	D	QM	O
	**A.**	Operations Management						
		i.	Organization has annual budget for information security technology					
		ii.	Organization has implemented technology for detection of cyber breaches					
		iii.	Technology has been implemented to prevent cybersecurity breaches from happening in the organization					
		iv.	Our organization has effective backup policies, procedures and technology.					
		v.	Our organization has established technology to test and evaluate cybersecurity breaches.					
		vi.	Network or system access by all users are logged, regularly reviewed and monitored for cybersecurity breaches.					
		vii	Our organization has implemented processes for change management					
	B.	Vulnerability Management						
		i.	Reports generated from the penetration tests are presented and discussed and senior management meetings.					

Table 59: Level of Technology Deployed Checklist (Continued)

CSE Evaluation Pillars	Proposed Abu Dhabi Government Department CSE-Checklist based on 6 - Pillars			Check Options *I=Initial; M=Managed; D=Defined; QM=Quantitatively Managed; O=Optimized*				
	Pillar 3: Level of Technology			I	M	D	QM	O
		ii.	Organization has policies and procedures for connection of personal devices to the corporate network.					
		iii.	Actions taken to mitigate information security vulnerabilities are planned, documented and monitored for effectiveness.					
		iv.	Organization has policies and procedures that govern user installation of software.					
		v.	Our organization uses third parties to conduct penetration testing of its information systems environment.					
	C	Incident Management						
		i.	Organization has designated roles for cybersecurity incident management.					
		ii.	Organization has established plans, policies and procedures for handling cyber security incidents.					
	D.	Business Continuity						
		i.	Organization has established a framework for business continuity in the case of cyberattacks.					
		ii.	There is a redundant site for recovery in case of major cyber-attack.					

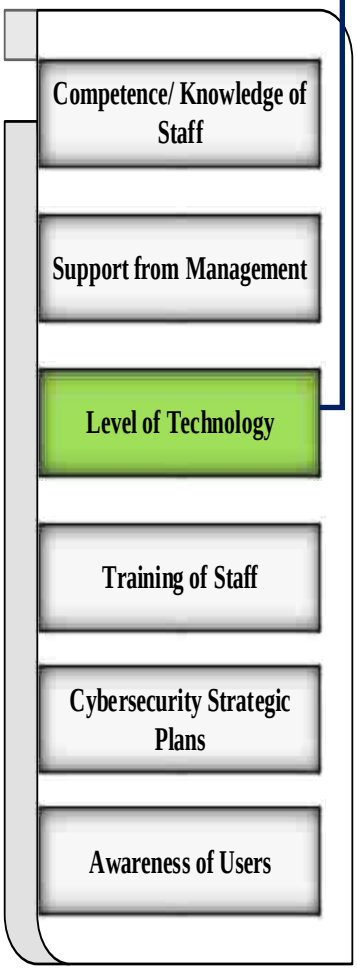


Table 60: Training of Staff and CSE Checklist

CSE Evaluation Pillars		Proposed Abu Dhabi Government Department CSE-Checklist based on 6 - Pillars	Check Options *I=Initial; M=Managed; D=Defined; QM=Quantitatively Managed; O=Optimized*				
		Pillar 4: Training of Staff	**I**	**M**	**D**	**QM**	**O**
Competence/ Knowledge of Staff	i.	The organization has implemented a regular user training program on cyber security for all its employees.					
Support from Management	ii.	User training programs implemented takes into consideration the cultural diversity of the workforce.					
Level of Technology	iii.	Monitoring and measurement tools are in place to evaluate the effectiveness of staff training programs.					
Training of Staff	iv.	All staff cybersecurity training programmes are reviewed at least once a year or whenever the security need arises					
Cybersecurity Strategic Plans	v	Our induction training programmes include culturally sensitive session on cyber and information security					
Awareness of Users							
		Average for training of staff					

For the Training of Staff factor, to use the checklist in Table 60 above, the assessor enters a score of 1 – 5 on the last column and then calculates the average for the factor. At the end of the evaluation process, the contribution of Training of Staff to cybersecurity effectiveness will be evaluated between 1 to 5.

Finally the strategic planning pillar checklist is further presented on Table 61 below and the assessor enters a score of 1 – 5 on the last column for each sub-factor then calculates the average for the factor after which an average value will be computed to attain the final CSE level for the factor.

Table 61: Checklist for Strategic Planning Pillar

CSE Evaluation Pillars		Proposed Abu Dhabi Government Department CSE-Checklist based on 6 - Pillars	Check Options *I=Initial; M=Managed; D=Defined; QM=Quantitatively Managed; O=Optimized*				
		Pillar 5: Strategic Planning	**I**	**M**	**D**	**QM**	**O**
Competence/ Knowledge of Staff	i.	A cybersecurity budget has been incorporated into our organization's strategic plan					
Support from Management	ii.	Information and cybersecurity policies are reviewed at least once in a year and whenever need arises to ensure effectiveness					
Level of Technology	iii.	All employees can access the organization's strategic plans					
Training of Staff	iv.	Strategic plans guide our organization to implement cybersecurity measures					
Cybersecurity Strategic Plans							
Awareness of Users							
		Average for Cybersecurity Strategic Planning					

Next, for the Awareness of Users factor the relationship with the checklist is indicated in Table 62. At the end of the evaluation process, the level of User Awareness will have a cybersecurity effectiveness (CSE) level of between 1 and 5.

Table 62: Awareness of Staff and CSE Checklist

CSE Evaluation Pillars			Proposed Abu Dhabi Government Department CSE-Checklist based on 6 - Pillars	Check Options *I=Initial; M=Managed; D=Defined; QM=Quantitatively Managed; O=Optimized*				
			Pillar 6: Awareness of Staff	**I**	**M**	**D**	**QM**	**O**
Competence/ Knowledge of Staff		i.	All employees are made aware of information security policies upon joining.					
Support from Management		ii.	Organization's policies on information awareness are strictly enforced.					
Level of Technology		iii.	The organization has a formal and documented disciplinary policy for information security breaches adhered to by all staff.					
Training of Staff		iv.	The organization consistently applies the disciplinary measures on cybersecurity breaches.					
Cybersecurity Strategic Plans		v.	Periodic campaigns are held by the organization to communicate, emphasize and reinforce cyber security readiness within the organization.					
Awareness of Users								
			Average for Awareness of Staff					

5.6 Limitations and Future Research Directions

In this study, a framework for examining the effectiveness of cybersecurity defences in Abu Dhabi government entities has been proposed. In future, the researcher intends to examine applicability of the proposed framework to private sector organizations, the Abu Dhabi government and globally. This study covers the cybersecurity aspects of only UAE public organizations. Comparing cybersecurity regulations, cybersecurity attack patterns and way of tackling these threats in other countries of the world would offer more insights to the issue at hand. This comparison study would also provide more detailed knowledge about cybersecurity regulations and methods of prevention from data breach.

The study findings are based on cross sectional data. Future studies may bring more comprehensive findings about patterns of cybersecurity issues by adopting longitudinal data collection at two different points of time. Similarly, use of experimental design by incorporating experiment and control group can give more robust picture about the influential factors responsible for effective cybersecurity system. Such studies will help in concluding causal relationship among different factors of cybersecurity effectiveness.

The current study focused both human and organizational level factors that contribute towards cybersecurity effectiveness. Future research, however, should include factors that are beyond human and organizational control; for example government support, government policies regarding use of information technology, external political influence among others.

The system of cybersecurity effectiveness is analysed in the light of several practicable factors. In this study, all these factors are supposed to have a positive

effect in enhancing the effectiveness of cybersecurity system. Further research is required to examine those factors that can deteriorate the potential capacity of cybersecurity system. These may be poor working conditions, lack of employee engagement among others. Such type of research will guide managers and policy makers to avoid those factors that can be a hindrance to effective management of cybersecurity systems.

5.7 Summary of the Study

The major goal of this study was to propose a framework for evaluation of cybersecurity defences in Abu Dhabi government entities. A cybersecurity framework consisting of key factors for evaluation of cybersecurity defences has been proposed by this study. This framework has been developed basing on the six key factors proposed for evaluating cybersecurity effectiveness in Abu Dhabi government entities. These factors are; 1) Competence/ Knowledge of Information security staff 2) Support from senior management 3) Level of technology deployed 4) training of staff 5) cybersecurity strategic plans and 6) Awareness of users. The proposed framework provides systematic guidelines to executive level management in different departments for preparation, protection and prevention of their departments from any form of cyber and information security attacks. A chapter wise overview of the study is summarized below:

In chapter one, the researcher introduced the study on cybersecurity globally and the United Arab Emirates (UAE) in particular. Several research glitches, research objectives, the research questions were formulated grounded on the fact that the UAE has become a target for a multitude of cyberattacks recently.

In chapter two, the researcher reviewed literature from several existing studies, journals, and published conference papers, among others, concerning the subject matter, which enabled identification of the research gap and the six study hypotheses for further analysis.

Chapter three presented the methodological approach undertaken to address the research questions and study hypotheses. A detailed discussion of the research strategy, tools and the research design was presented in detail. The chapter further presented various tests conducted to validate and ensure reliability of the research instrument and to test the hypotheses of the study.

In chapter four, the researcher presented the data analysis and study results including the method of analysis, reliability and validity checks, demographic statistical results and correlation results linear and multiple regression. In the same chapter the results were presented to provide answers to the different research questions identified in chapter one.

Finally, chapter five discussed the research contributions and presented a framework with checklist for cybersecurity assessment with the aid of key check points to evaluate effectiveness and readiness of a department’s cybersecurity programme as well as study recommendations and areas of future research.

References

Abawajy J. (2014). User Preference of Cybersecurity Awareness Delivery methods, Journal of Behaviour and Information Technology, volume 33, issue 3, pp. 236- 247, Taylor and Francis Inc. Bristol, PA, USA.

Abraham S. and Nair S. (2015). A predictive Framework for Cybersecurity Analytics using attack graphs, International Journal of Computer Networks and Communications (IJCNC), Volume 7, pp. 712-740, DOI: 10.5121/ijcnc.2015.7101.

Ahn Y.S., Dutt V. and Gonzalez C. (2013). Cyber situation awareness, modelling detection of cyberattacks with instance based leasing theory. The journal of Human Factors and Ergonomics Society, volume 55, issue 3, pp. 605 – 618.

Al Bawaba (2012). Cybercrime laws in the UAE are dangerously vague. Retrieved from:https://www.albawaba.com/mena_voices/uae-cybercrime-law-450814, Accessed 13th, December, 2015.

Alqatawna J. (2014). The Challenge of Implementing Information Security Standards in Small and Medium e-Business Enterprises. Journal of Software Engineering and Applications, volume 7, pp. 883-890. http://dx.doi.org/10.4236/jsea.2014.710079.

Al-Khouri M. (2012). E-Government Strategies. The Case of the United Arab Emirates, European journal of e-practice, ISSN: 1988-625X, volume 17, pp. 133-141.

Al-Khouri M., Malik A. and Bachalaghen M. (2011). Towards Federated e- identity Management across GCC, A solution's Framework, Global Journal of Strategies and Governance, volume 4, issue, 1, pp. 30-49.

Aloul A., Al-Dalky R., Al-Mardini M. and El-Hajj W. (2012). Smart Grid Security: Threats, Vulnerabilities and Solutions, International Journal of Smart Grid and Clean Energy, Department of Computer Science American University of Sharjah, UAE, volume 1, issue 1, pp. 1-6, Electronic ISBN: 978-0-9564263-6-9.

Aloul A. (2010). Information security awareness in UAE: A survey paper, International Conference for Internet Technology and Secured Transactions, IEEE Xplore, pp. 1-6.

Andrew L. J. (2014). Center of Strategic and International Studies (CSIS), Middle East Programme Report. Accessed on November 1st, 2015 from https://www.csis.org/people/james-andrew-lewis.

Andrew L. J. and Gotz N. (2013). United Nations Institute for Disarmament Research (UNIDIR) Report, The cyber index, International Security Trends and Realities, Center for strategic and International Studies, https://www.unidir.org, accessed on 4th, June, 2016.

Assante M. J. and Tobey D. H. (2011). Enhancing Cybersecurity workforce, IEEE Computer Society, volume 13, issue 1, pp. 12-15.

Bass T. (2000). Intrusion Detection System and Multi-Sensor Data Fusion, Communications of the ACM, volume 43, issue 4, pp. 99 - 105.

Birtwhistle R.V., Delva M. D., Kirby J. R. and Knapper C. K. (2002). Postal survey of approaches to learning among Ontario physicians; Implications for continuing medical education, British Medical Journal, volume 325, pp. 1218-1222.

Brews P. and Purohit D. (2007). Strategic Planning in Unstable Environments, Journal, Long Range Planning, volume.40, pp. 64-83.

Bronk C. and Eneken T. (2013). Hack or Attack? Shamoon and the Evolution of Cyber Conflict, Survival, Global Politics and Strategy volume 55, issue 2, pp. 81-96.

Burgers R., Baars H., Adriaensen M. and Raja A. (2013). Middle East needs cybersecurity from within Utilities face energy threat. DNV KEMA Energy and Sustainability.

CGI Group Report (2014). Cybersecurity in Modern Critical Infrastructure Environments, pp. 5, https://www.cgi.com, accessed on September, 18th, 2014.

Choo K. R., Smith R. G. and McCusker, R. (2007). The future of technology-enabled crime in Australia, Australian Institute of Criminology, ISBN 978 1 921185 48 9, pp. 341.

Choo K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, volume 30, issue 8, pp. 719-731.

Choo K. R. (2010). Cloud computing: challenges and future directions, Trends and Issues in Crime and Criminal justice, volume 400, pp. 1-6.

Cisco Systems Report (2017). Mid-year cybersecurity Report, retrieved from https://engage2demand.cisco.com/cisco_2017_midyear_cybersecurity_report September 10, 2017.

Comrey A.L and Lee H. B. (1973). A first course in factor analysis. New York: Academic Press, volume 14, issue 3, pp. 301-321.

Conklin A. (2006). Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course, Proceedings of the 39th Hawaii International Conference on System Sciences, IEEE.

Cressey R. and Hayfer M. (2012). Cyber capability in the Middle East, Seizing opportunity while managing Risk in Digital age, Booz Allen Hamilton.

Creswell J. W. and Miller D. L. (2000). Determining validity in qualitative inquiry. Theory into Practice, volume 39, issue 3, pp. 124-130.

Craigen D., Diakun-Thibault N. and Purse R. (2014). Defining Cybersecurity, Technology Innovation Management review, volume 4, issue 10, pp. 196-207, https:// www.timreview.ca.

Da Veiga A. and Eloff J. H. P. (2010). A framework and assessment instrument for information security culture. Journal of Computers and Security, volume 29 no.2, Elsevier Advanced Technology Publications Oxford, UK, volume 29, issue 2 pp. 196-207.

DeVellis R. F. (2003). Scale development: Theory and applications (2nd Edition). Thousand Oaks, CA: Sage Publications, Inc.

Dong-Young K. and Gerald G. (2010). E-government maturity model using the capability maturity model integration, Journal of Systems and Information Technology, volume 12, issue 3, pp. 230-244, https://doi org.ezproxy4.lib.le.ac.uk/10.1108/13287261011070858.

Dutton J. E. and Duncan R. (1987). The Influence of the Strategic Planning Process on Strategic Change, Strategic Management Journal, John Wiley and Sons, volume 8, pp. 103 - 116.

Elbanna S. (2010). Strategic Planning in the United Arab Emirates. International Journal of Commerce and Management, Emerald Group Publishing Limited, volume 20, issue 1, pp. 26-40, ISSN: 1056-9219, https://doi.org/10.1108/10569211011025934.

Enders C. K. (2001). The relative performance of full information maximum likelihood estimation for missing data in structural equation models. Structural Equation Modeling, volume 8, issue 3, pp. 430.

Emerging Cyber Threats Report (2015). Georgia Tech Cyber Security Summit 2014, pp. 1-3, https://www.cc.gatech.edu/sites/default/files/images/2015emergingcyberthreats report.pdf, accessed on 5th, July, 2017.

ENISA (2012). National Cybersecurity Strategies, Setting the course for national efforts to strengthen security in cyberspace, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cybersecurity-strategies-ncsss.

Efthymiopoulos M. P. and Christopher W. J. (2014). Implementation of safety techniques in a Cyber-Domain. University of Glasgow, ACM 978-1-4503.

Evangelopoulou M., Christopher W. and Johnson C.W. (2014). Implementation of safety techniques in a Cyber-Domain. University of Glasgow, ACM 978-1-4503.

Finland's Cybersecurity Strategy Report (2013). Government Resolution 24.1.2013, ISBN: 978-951-25-2438-9,https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, accessed on April, 20th, 2015.

Gallagher R., Tonette S. B., Linda A. S., Perez-Prado A. (2003). Information Technology, Learning, and Performance Journal; Morehead volume 21, issue 1, pp. 19-28.

Gilbert T.F. (1978). Human Competence. Engineering Worthy Performance. New York: McGraw-Hill, volume 17, issue 9, pp. 19-26.

Ginsberg A. (1997). New Age Strategic Planning: Bridging Theory and Practice, Long Range Planning, volume 30, issue 1, pp. 125-128.

Glaister K. W. and Falshaw J. R. (1999). Strategic Planning: Still Going Strong Long Range Planning, volume 32, issue 1, pp. 107-116.

Grant R. M. (2003). Strategic Planning in A Turbulent Environment: Evidence from the Oil Majors, Strategic Management Journal, volume 24, pp. 491-517.

Greitzer F., Moore A., Cappelli D., Andrews D., and Carroll L.(2008). Combating the Insider Cyber Threat, IEEE Security & Privacy, volume 6, pp. 61-64.

Greitzer F., Kuchar O.A. and Huston K., (2007). Cognitive science implications for enhancing training effectiveness in a serious gaming context. ACM Journal of Educational Resources in Computing, volume 7, issue 3, pp. 10, DOI=10.1145/1281320.1281322, http://doi.acm.org/10.1145/1281320.1281322

Gercke M. (2014). Understanding cybercrime: Phenomena, challenges and legal response, ITU Publication, pp. 2- 3, http:// www.itu.int/ITU-D/cyb/cyber security/legislation.html.

Hakmer J. (2017). Cybercrime and the Digital Economy in the GCC Countries, International Security Department. The Royal Institute of International Affairs, 2 June 30th, ISBN 978 1 78413 235 4.

Hair J.F., Black W.C., Babin B.J. and Anderson R.E. (2009). Multivariate data Analysis (7th ed.). Upper Saddle River, NJ; Person.

Herath T. and Rao H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, volume 47, pp. 154-165, doi: 10.1016/j.dss.2009.02.005.

Hight S. D. (2005). The importance of a Security, Education, Training and awareness programme. Raleigh, NC 27601.

Hiller J. S. and Russell R.S. (2015). Modalities for Cybersecurity and Privacy Resilience: The NIST Approach, Virginia Tech, Proceedings of the ISCRAM 2015 Conference – Kristiansand.

Hippel P. T. (2004). Biases in SPSS 12 .0 missing value analysis. The American Statistician, volume 58, issue 2, pp. 160-164.

Hunter G. S. (2013). Fresh calls for tighter UAE banking regulations in wake of $45m cyber heist. Retrieved Jan 15, 2014, from

http://www.thenational.ae/business/industry-insights/finance/fresh-calls-for-tighter-uae-banking-regulations-in-wake-of-45m-cyber-heist#ixzz2qRl09jRz

Humaidi N. and Balakrishnan V. (2013). Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security. J Health Med Inform, volume 4, issue 2, pp. 2-9, doi: 10.4172/2157-7420.1000123.

International Telecommunication Union Report (2012). Arab Summit, Connecting the unconnected by 2015, ICT Progress and adoption in the Arab region. pp. 141.

ISACA and RSA conference (2016). State of Cybersecurity implications for 2016, an ISACA and RSA conference survey, CSX cybersecurity Nexus, pp. 1-18, https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf.

Katz F. H. (2005). The Effect of A University Information Security Survey on Instruction Methods In Information Security. Proceedings of the second annual conference on information security curriculum development, pp. 43-48.

Kalberg J. and Bhavani T. (2012). Towards Cyber operations, The New Role of Academic Cyber security Research and Education, Intelligence and Security Informatics (ISI), 2012 IEEE International Conference, Arlington, VA, USA, **ISBN:** 978-1-4673-2104-4, pp. 132-134.

Knapp K. J. 2009. Information security policy: An organizational-level process model. In Computers & Security, volume 28, issue 7, pp. 493–508. Available at: http://www.sciencedirect.com/science/article/B6V8G-4WSHK032/2/65673d7d064cc45cd182b82622c6acda.

Kwangjo K. and Kaist D. (2012). Challenges of Cyber Security for Nuclear Power Plants, Khalifa University of Science, Technology and Research, Abu Dhabi, UAE, The 18th Pacific Basin Nuclear Conference (PBNC 2012), BEXCO, Busan, Korea.

Kritzinger E. and Von Solms S. H. (2010). Cybersecurity for home users: A new way of protection through awareness enforcement. Journal of Computers and Security, volume 29, issue 8, pp. 840-847.

Kritzinger, E. and Smith E. (2008). Information security management: An information security retrieval and awareness model for industry. Computers and Security, volume 27, issue 5, pp. 224-231.

Kruger H. A., Flowerday L., Drevin L. and Steyn T. (2011). An assessment of the role of cultural factors in Information Security awareness, pp. 1-7, www.researchgate.net, ISSA, IEEE Xplore Digital Library.

Kshetri N. (2005). Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, volume 11, issue 4, pp. 541-562.

KPMG Report (2017). Building Cybersecurity & Resilience in a Digital Africa, pp. 5, https://www.kpmg.com/ng, accessed on 15th, August, 2017.

Leach J. (2003). Improving user security behavior. Computers and Security, volume 22, issue 8, pp. 685-692.

Liedtka (2000). Strategic Planning as a Contributor to Strategic Change: A Generative Model. European Management Journal, volume 18, issue 2, pp. 195 - 206.

Lydon B. (2013). Cyber security strategy and actions, International Society of Automation, https://insurancenewsnet.com/oarticle/Cybersecurity-strategy-and-actions-%5BInTech%5D-a-410613#.WkGh5lWWbcc, accessed on 16th, June, 2016.

McCrohan K. (2010). Influence of Awareness and Training on Cybersecurity. Journal of Internet Commerce, method approaches, London: Sage Media, Inc., Hingham, MA, volume 9, pp. 3-23.

McAfee (2014). https://www.insight.com/content/dam/insight-web/en_US/article-images/whitepapers/partner-whitepapers/mcafee-labs-threats-report.pdf, accessed, July 20th, 2016.

Miller C. C. and Cardinal I. B. (1994). Strategic Planning and firm performance: a synthesis of more than two decades of research, Academy of management journal volume 37, issue 6, pp. 1649-1665.

National Institute of Standards and Technology (NIST) Report, Framework for Improving Critical Infrastructure 40 Cybersecurity, Feb, 2014.

Nambiro A., Wechuli G. M. and Nahason M. (2014). Cybersecurity Assessment Framework: Case of Government Ministries in Kenya, International Journal of Technology in Computer Science & Engineering, volume 1, pp. 2349-1582, 2014, http://www.ijtcse.com.

Neuneck G. and Weizmann N. (2013). The Role of CBMs in assuring Cyber Stability, United Nations Institute for Disarmament Research (UNIDIR) Geneva, Switzerland report.

Nigel M. and Rice J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. Computers and Security, volume 30, issue 8, pp. 803-814.

Obama B. (2009). Remarks by the President on Securing Our Nation's Cyber Infrastructure. Retrieved November 18, 2012, http: //www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.Pacific Basin Nuclear Conference (PBNC 2012), BEXCO, Busan, Korea.

Ola S. (2015). Every Small Business Should Use the NIST Cybersecurity Framework, e-management, https://www.eminc.com, accessed on December, 12th, 2016.

Pallant J. F. (2013). SPSS survival manual.5th ed. Buckingham: Open University Press.

Pallant J. F., Helen H., Annika K. and Ingegerd H. (2011). Cross-cultural comparison of levels of childbirth-related fear in an Australian and Swedish sample, Midwifery journal, volume 27, issue 4, pp. 560-567.

Pepitone J. (2011). Group claims fresh hack of 1 million Sony accounts. Retrieved July 15, 2014, from CNN Money: http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/.

Pfleeger S. and Caputo D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. Computers and Security, volume 31, issue 4, pp. 597-611, https://doi.org/10.1016/j.cose.2011.12.010.

Preston C. S. (2014). Incentives to encourage adoption of the NIST Cybersecurity framework, Mississippi State University, USA.

Price W. C. (2015). Information Security Breaches Survey, Available at: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf.

Price W. C. (2014). Information Security Breaches Survey, Available at: https://www.pwc.co.uk/assets/pdf/cyber-security-2014-technicalreport.pdf.

Rees L. P. (2011). Decision support for Cybersecurity risk planning. Decision Support Systems, volume 51, issue 3, pp. 493-505.

Rezgui Y. and Marks A. (2008). Information security awareness in higher education: An exploratory study. Computers and Security, volume 27, issue 8, pp. 241-253.

Rohmeyer P. (2006). An evaluation of information security management effectiveness. Ann Arbor, Ph.D. thesis, Stevens Institute of Technology, Hoboken, USA, pp. 258-258.

Rotvold G. (2008). How to create a security culture in your organization. Information Management Journal, volume 42, pp. 32-38.

Rovai A. P., Baker J. D. and Ponton M. K (2014). Social science research design and statistics: A practioners guide to research methods and IBM SPSS analysis, (2nd ed., Kindle). Chesapeake, VA: Water tree Press, LLC.

Rowe D., Lunt B. and Ekstron J. (2011). The role of Cybersecurity in information Technology Education, ACM, Proceedings of the 2011 conference on Information technology education, pp. 113-122.

Rudd J. M. (2008). Strategic planning and performance: Extending the debate. Journal of Business Research, volume 61, issue 2, pp. 99-108.

Saeed B S., Hani A. and Qudaih J. I. (2014). An Overview on Cybersecurity Awareness in Muslim Countries, International Journal of Information and Communication Technology Research, volume 4, issue 1, pp. 1-3, ISSN 2223 – 4985.

Sage O. (2015). Every Small Business Should Use the NIST Cybersecurity Framework, e-management, accessed at http:// www.eminc.com, 15-04-2017.

Seibert P.S. (2002) A checklist to facilitate cultural awareness and sensitivity, Journal of Medical Ethics, volume 28, pp. 143-146, doi:10.1136/jme.28.3.143.

Schultz E. (2005). The human factor in security, Computers & Security, volume 24, pp. 425-426.

Shackelford S. J., Proia A.A., Markell B. and Craig N. (2014). Towards a Global Cybersecurity standard of care, exploring the implications of the NIST 2014 cybersecurity framework on shaping reasonable National and International practices, Texas International Law Journal, volume 50, issue 2, pp. 305- 312.

Shackelford S. J., Russell S. and Jeffrey H. (2015). A Comparison of Voluntary Cybersecurity Frameworks, UC Davis Business Law Journal, Forthcoming; Kelley School of Business Research, volume 1, pp. 16-2. Available at SSRN: https://ssrn.com/abstract=2702039.

Schein E. H. (2004). Organizational Culture and Leadership, Jossey-Bass; 3 edition, pp. 39-63 ISBN-13: 978-0787968458.

Shen L. (2014). The NIST Cybersecurity Framework, Overview and Potential impacts, Journal of Internet Law, Aspen Publishers Inc, volume 10, issue 4, pp. 16-19.

Siponen M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management and Computer Security, volume 8, no.1, issue 1, pp. 31-41.

Siponen M. T. (2001). Five Dimensions of Information Security Awareness. Computers and Society, volume 31, issue 2, pp. 24-29.

Siponen M. T., Adam M. and Pahnila S. (2014). Employees' adherence to information security policies: An exploratory field study. Information and Management, volume 5, issue 2, pp. 217–224.

Smith E., Kritzinger E., Oosthuizen H. J. and Von Solms S. H. (2004). Information Security Education, in Proceedings of the WISE 4 Conference, Moscow, Russia.

Symantec (2013). Internet Security Threat Report, Retrieved October 2014 from http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v18_2012_21291018.en-us.pdf.

Symantec (2016).Internet Security Threat Report, volume 21, pp.1-3, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, accessed on December, 26th, 2016.

Tabachnick B. G. and Fidell L. S. (2007). Using multivariate statistics (5th edition). Boston, MA: Allyn and Bacon/Pearson Education.

Ting W.W. and Comings D. R. (2010). Information assurance metric for assessing NIST's monitoring step in the risk management framework, Institute of Strategic Risk Management, ISSN 1939 – 3555.

Teodoro N., Goncalves L. and Serrawo C. (2015). NIST Cybersecurity Framework. The European Network and Information Security Agency (ENISA) Report, (2012). National Cybersecurity Strategies, setting the course for National efforts to strengthen security in cyberspace www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cybersecurity strategies-ncsss.

Tubey R. J., Rotich J. K and Bengat J.K. (2015). Research Paradigms; Theory and practice: Research on Humanities and Social Sciences, volume 5, Issue 5, pp. 224-228.

UAE Computer Emergency Response Team Website (aeCERT), http://www.aecert.ae/index-en.php.

UAE Telecommunication Regulatory Authority web portal, http://www.tra.gov.ae/national-emergency-plan.php.

UAE Federal Law No.3 (2012), http://ejustice.gov.ae/downloads/latest_laws/federal_decree_law_3_2012_en.pdf, accessed on July, 3rd, 2014.

UAE Federal Law No.5 (2012), http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf, accessed on February, 14th, 2014.

UAE Federal Law No.2 (2006), http://www.qcert.org/sites/default/files/public/documents/uae-ecrime-the_prevention_of_information_technology_crimes-eng-2006.pdf, accessed on February, 16th, 2015.

Uchenna P., Daniel A., Hongmei M. and Ashutosh T. (2016). Human Capability Evaluation Approach for cybersecurity in critical industrial infrastructure, Springer International Journal Publishing Switzerland, Proceedings of the AHFE 2016 International Conference on Human factors in Cybersecurity, July

27-31, Walt Disney world, Florida, USA, Part III, , pp. 169-182, DOI: 10.1007/978-3-319-41932-9-14.

United Nations Development Programme (UNDP) E-government Survey (2012). E-government for the people, retrieved 30th/07/2014, from http://www.unpan.org/egovkb/global_report.html.

United States Congress (2017). Report of the US-China Economic and Security Review Commission, 2010. Retrieved from https://www.uscc.gov/Washington DC, May 17, 2016.

Vacca J.R. (2002). Computer Forensics: Computer Crime Scene Investigation, Charles River Media, Inc., Hingham, MA.

Von Solms R. and Van N. J. (2013). From information security to cyber security, Journal of computers & security, Elsevier Advanced Technology, volume 38, pp. 97-102.

Vroom C. and Von Solms R. (2004). Towards information security behavioural compliance, Computers and Security, volume 23, issue 3, pp. 191-198.

Vroom C. and Von Solms R. (2003) Information Security: Auditing the Behaviour of the Employee, Security and Privacy in the Age of Uncertainty. SEC 2003. IFIP -The International Federation for Information Processing, Springer, Boston, MA, volume 122, pp.401-404, Online ISBN 978-0-387-35691-4.

Whitmer M. G. (2007). IT Security Awareness and Training, Changing the culture of state government, NASCIO: Chief Information Officers of the States.

Wilson M. and Hash J. (2003). Building an Information Technology Security Awareness and Training Program. National Institute of Standards and Technology Report.

Wunderle W. D. (2006). Through the Lens of Cultural Awareness: A Primer for US Armed Forces Deploying to Arab and Middle Eastern Countries, Combat Studies Institute Press Fort Leavenworth, KS 66027.

World Internet Statistics (2016). http://www.internetlivestats.com/internet-users/united-arab-emirates/, accessed on August, 20th, 2017.

Zhao J. J. (2010). Opportunities and threats: A security assessment of state e-government websites. Government Information Quarterly, volume 27, issue 1, pp. 49-56.

Zikmund W. G., Babin B. J., Carr J. C. and Griffin M. (2010). Business research methods (9th edition). Mason, OH: South-Western.

Appendix 1: Survey Questionnaire

A Framework for the Evaluation of Cybersecurity Effectiveness **إطار لتقييم فاعلية أمن المعلومات**

Introduction: **مقدمة**

I am currently enrolled into the DBA program at the UAE University. As part of my studies I am conducting research on cybersecurity in Abu Dhabi government agencies. The purpose of this questionnaire is to collect data for this research. The names of the participants or the agencies they work for will not be identified anywhere in this survey or the dissertation to follow. This survey will not take more than 15 minutes. Thank you for participating.

أنا ملتحق حاليا في برنامج الدكتوراه في إدارة الأعمال بجامعة الإمارات العربية المتحدة، و اطروحتي تتناول مجال أمن المعلومات الإلكتروني في المؤسسات الحكومية في إمارة أبوظبي، الغرض من هذا الاستبيان هو جمع معلومات لإعداد هذه الدراسة، و لن تُذكر أسماء المشاركين أو المؤسسات التي يعملون فيها في أي مكان من الدراسة أو من الأطروحة التي سيتم إعدادها لاحقا، لن يستغرق هذا الاستقصاء أكثر من 15 دقيقة، شكرا لكم على مشاركتكم.

General information:

المعلومات العامة:

1. What is your age?

1. ماهو عمرك؟

O	Less than 25 years	أقل من 25 سنة.	O
O	25 - 30 years	بين 25 و30 سنة	O
O	30 - 40 years	بين 30 و40 سنة	O
O	More than 40 year	أكثر من 40 سنة	O

2. What is your educational background? [Indicate major course work where applicable]

2. ما هو مستواك التعليمي؟ (مع ذكر التخصص إن وجد)

O	High School	ثانوية عامة	O
O	Diploma	دبلوم	O

O	Higher Diploma	دبلوم عالي	O
O	Bachelors	بكالوريوس	O
O	Masters	ماجستير	O
O	Doctorate	دكتوراه	O

3. What is your major?

3. ما هو تخصصك؟

O	No Major	دون تخصص	O
O	Computer or IT related	مرتبط بمجال الكمبيوتر أو تقنية المعلومات	O
O	Engineering related	مرتبط بمجال الهندسة	O
O	Business relater	مرتبط بمجال الإدارة و الأعمال	O
O	Others (……)	آخر (.....)	O

4. How many years have you worked in the government sector?

4. كم سنة عملت في القطاع الحكومي؟

O	0 – 5 years	من 0 إلى 5 سنوات	O
O	5 - 10 years	من 5 إلى 10 سنوات	O
O	More than 10 years	أكثر من 10 سنوات	O

5. What is your managerial level?

5. ماهو مستواك الإداري؟

O	Team Member/ Officer	عضو فريق/ موظف	O
O	Section Manager/ Team Lead	مدير قسم/ مدير فريق	O
O	Department Manager/ CIO/ CISO/ IT manager	مدير إدارة	O
O	Executive Director/CEO/GM	مدير تنفيذي/ مدير عام	O
O	Consultant	مستشار	O

6. How many employees does your organization have?

6. كم عدد الموظفين الذين يعملون في المؤسسة؟

Less than 100	100 – 200	201 – 500	500 - 999	Greater than 1000
اقل من 100	من 100 إلى 200	من 201 إلى 500	من 500 إلى 999	أكثر من 1000
O	O	O	O	O

7. How would you rate your understanding of cybersecurity?

7. كيف تصنف فهمك لأمن المعلومات الإلكتروني (الأمن السيبراني)؟

O	None	لا يوجد	O
O	Poor	ضعيف	O
O	Good	جيد	O
O	Excellent	ممتاز	O

8. A cyberattack is a perceived threat to network security.

8. القرصنة (الإختراق الإلكتروني) تشكل تهديدا لأمن الشبكات.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

9. Our employees do not know when their computers have been attacked by a virus.

9. موظفونا لا يعلمون متى تعرضت أجهزة الكمبيوتر الخاصة بهم لفيروس إليكتروني.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

10. A cyberattack can be perceived as a threat to data and information

10. القرصنة (الإختراق الإلكتروني) تشكل تهديدا للبيانات والمعلومات الإلكترونية.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

11. A Virus attack is a type of a cyber-attack.
11. الهجوم الفيروسي نوع من أنواع الهجمات الإلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

12. Untrustworthy employees or disgruntled IT insiders can initiate a cyberattack against the organization.
12. يمكن أن يشن الموظفون غير الموثوق بهم أو مختصو تقنية المعلومات المخولين و غير الراضيين عن العمل، هجمات الإلكترونية (قرصنة) ضد المؤسسة .

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

13. Website defacing is a type of a cyber-attack
13. تخريب مواقع الإنترنت نوع من أنواع الهجوم الإلكتروني أو (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

14. I completely understand what email client vulnerability is.
14. أدرك تماما تواجد الثغرات لدى موفري خدمات البريد الإلكتروني (مثل Gmail, Yahoo, Hotmail إلخ.).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

15. I understand the importance of choosing a strong password
15. أدرك أهمية اختيار كلمة السر المنيعة و صعبة التخمين.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

16. The vulnerability of an organization can be decreased by implementing appropriate security countermeasures

16. يمكن الحد من ضعف المؤسسة الأمني من خلال تطبيق الإجراءات الأمنية و التنظيمية الملائمة.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

17. Our organization understands the risk of cyberattacks and the importance of implementing safeguarding techniques.

17. تدرك مؤسستنا خطورة الهجمات الإلكترونية (القرصنة) ومدى أهمية تطبيق تقنيات لحمايتها.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

18. Cyberattacks may disrupt organizational activities.

18. يمكن للهجمات الإلكترونية (القرصنة) أن تعرقل نشاط المؤسسة.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

19. Legal consequences against attackers may deter cyberattacks.

19. المساءلة القانونية لمرتكبي الهجمات قد تردع عمليات القرصنة (الهجمات الإلكترونية).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

20. Cyber-attackers focus on targets such as networks, servers and routers.

20. يركز مرتكبي الهجمات الإلكترونية (القرصنة) على أهداف مثل الشبكات والخوادم و نقاط التوجيه.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

21. Please check below what type of attack your organization has experienced over the last 1 – 3 years?

21. أي نوع من الهجمات الإلكترونية (القرصنة) تعرضت له مؤسستكم؟

□	Denial of Service (DOS)	الحرمان من الخدمات	□
□	Virus Attack	الهجوم الفيروسي	□
□	Worm Attack	هجوم بواسطة دودة الكمبيوتر	□
□	Industrial Sabotage	تخريب صناعي	□
□	Insider Attack	الهجمات الداخلية	□
□	Denial of access to your email or computer systems	الحرمان من الوصول لخدمات البريد الإليكتروني أو خدمات الأنظمة	□
□	Website defacing	تخريب الموقع الإلكتروني	□
Others: (Please specify) _____ _____		أخرى (يرجى التحديد) _____ _____	

22. When was this information about the attack disclosed to the public/customers? (In days, weeks etc.)

22. . متى تم الإعلان عن هذه المعلومة عن الهجمة الإلكترونية (القرصنة) للجمهور / العملاء (بالأيام/ الأسابيع/... إلخ).

O	On the same day	في نفس اليوم	O
O	Within a week	خلال اسبوع	O
O	Within a month	خلال شهر	O
O	Never been disclosed	لم يتم الإعلان عنها	O

23. To what degree did the attacks reduce the availability of your network?

23. إلى أي درجة تسببت الهجمات الإلكترونية (القرصنة) في فقدان نظام الشبكة الخاصة بكم؟

I Don't know	No Effect	Some Effect	Considerable Effect	Catastrophic Effect
لا أعلم	بدون تأثير	بعض التأثير	تأثير بالغ	تأثير مأساوي
O	O	O	O	O

24. To what degree did the attacks reduce the availability of your data/information?

24. إلى أي درجة تسببت الهجمات الإلكترونية (القرصنة) في تقليل توافر البيانات/المعلومات الإلكترونية؟

I Don't know	No Effect	Some Effect	Considerable Effect	Catastrophic Effect
لا أعلم	بدون تأثير	بعض التأثير	تأثير بالغ	تأثير مأساوي
O	O	O	O	O

25. To what degree did the attacks reduce your ability to collaborate by email?
25. إلى أي درجة تسببت الهجمات الإلكترونية (القرصنة) في تقليل قدرتكم على التواصل بواسطة البريد الإلكتروني؟

I Don't know	No Effect	Some Effect	Considerable Effect	Catastrophic Effect
لا أعلم	بدون تأثير	بعض التأثير	تأثير بالغ	تأثير مأساوي
O	O	O	O	O

26. To what degree did the attacks reduce the overall operations of your organization?
26. إلى أي درجة تسببت الهجمات الإلكترونية (القرصنة) في تعطيل نشاط مؤسستكم؟

I Don't know	No Effect	Some Effect	Considerable Effect	Catastrophic Effect
لا أعلم	بدون تأثير	بعض التأثير	تأثير بالغ	تأثير مأساوي
O	O	O	O	O

27. To what degree did the attacks reduce employee productivity in your organization?
27. إلى أي درجة تسببت الهجمات الإلكترونية (القرصنة) في تقليل إنتاجية موظفي مؤسستكم؟

I Don't know	No Effect	Some Effect	Considerable Effect	Catastrophic Effect
لا أعلم	بدون تأثير	بعض التأثير	تأثير بالغ	تأثير مأساوي
O	O	O	O	O

28. Disclosing to the public that an organization has experienced a cyberattack may negatively impact its reputation.
28. الإعلان بأن المؤسسة قد تعرضت لهجمات إلكترونية (عمليات القرصنة) قد يؤثر سلبا على سمعتها؟

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

29. All Abu Dhabi government organization should have a budget allocated to strengthen cybersecurity measures.
29. جميع مؤسسات حكومة أبوظبي، يجب أن تخصص ميزانية لتعزيز الإجراءات الأمنية الإلكترونية (الأمن السيبراني).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

30. Our organization has invested adequate funds to promote countermeasures against cyberattacks.

30. استثمرت مؤسستنا أموالا كافية لترقية تدابير مضادة ضد الهجمات الإلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

31. Our organization has invested adequate funds towards increasing employee education as a protection from cyberattacks.

31. استثمرت مؤسستنا أموالا كافية في تعليم موظفيها كوسيلة لحمايتها من الهجمات الإلكترونية (القرصنة)

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

32. Disaster recovery is not considered as a protection from cyberattacks, but rather a pre-determined plan in case of a cyberattack.

32. "خطط التعافي من الكارثة" لا تعتبر حماية من الهجمات الإلكترونية (القرصنة)، بل خطة إحتياطية مسبقة في حالة حدوث أي هجمة إلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

33. In our organization, government practices and guidelines has helped us in safeguarding against cyberattacks.

33. في مؤسستنا، ساعدتنا الممارسات و الإجراءات الحكومية في مجال الأمن الإلكتروني (الأمن السيبراني) لحمايتها من الهجمات إلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

34. It is important to have cybersecurity incorporated in organizations Strategic plans.

34. من المهم دمج و تضمين مسألة الأمن الإلكتروني (الأمن السيبراني) ضمن مخططات المؤسسة الاستراتيجية.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

35. All employees in our organization are aware of the strategic plan implemented to protect against cyberattacks

35. كل العاملين في مؤسستنا على إدراك بالخطة الإستراتيجية للحد من الهجمات الإلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

36. Senior management has an important role in developing information security policies for our organization.

36. للإدارة العليا في مؤسستنا دور مهم في تطوير سياسات أمن المعلومات الإليكترونية (الأمن السيبراني).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

37 . The Head of Information Security of our organization reports directly to the highest official in our organization

37. رئيس أمن المعلومات في مؤسستنا على اتصال مباشر بأعلى سلطة في المؤسسة.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

38. It is important that information security policies are reviewed on a regular basis to ensure their effectiveness in our organization.

38. من المهم مراجعة سياسات و إجراءات أمن المعلومات الإلكتروني (الأمن السيبراني) بصفة منتظمة لضمان فعاليتها في مؤسستنا.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

39. Strategic plans guide our organization to implement cybersecurity measures

39. الخطة الإستراتيجية توجه مؤسستنا نحو تطبيق تدابير الأمن الإلكتروني (الأمن السيبراني).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

40. Cybersecurity generally should be the responsibility of the IT department.

40. ينبغي أن يكون أمن المعلومات الإلكتروني (الأمن السيبراني) عموما من اختصاص إدارة تقنية المعلومات.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

41. It is important to separate the roles of IT management and Information Security management in our organization.

41. من المهم الفصل بين دور إدارة تقنية المعلومات ودور إدارة أمن المعلومات الإلكترونية (الأمن السيبراني) في مؤسستنا.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

42. Budget al.,location is not important when it comes to cybersecurity strategies for our organization.

42.عندما يتعلق الأمر باستراتيجيات أمن المعلومات بالنسبة لمؤسستنا فليس من المهم تخصيص ميزانية.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

43. Our organization has implemented software solutions to protect against cyberattacks.

43. تعمل مؤسستنا على تطبيق حلول برمجية للحماية من الهجمات الإلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

44. Our organization has implemented an effective anti-virus software program to safeguard against cyberattacks.

44. تعمل مؤسستنا على تطبيق عملية منهجية و فعالة (برنامج مكافحة الفيروسات) للحماية من الهجمات الإلكترونية (القرصنة)

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

45. Our organization has implemented an effective up-to-date software patching procedure to safeguard against cyberattacks.

45. تعمل مؤسستنا على تطبيق إجراءات منهجية و فعالة (تحديث برامج مكافحة الفيروسات) للحماية من الهجمات الإلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

46. Our organization has installed the following items as safeguards against cyberattacks. (Check all that apply)

46. تعتمد مؤسستنا العناصر التالية للحماية من الهجمات الإلكترونية (القرصنة) (يرجى اختيار ما هو مطبق).

□	Anti-Virus software's	برامج مكافحة الفيروسات	□
□	Firewalls	الجدران النارية	□
□	Proxy Servers	خوادم البروكسي	□
□	Intrusion Detection Systems (IDS)	انظمة كشف التسلل	□
□	Intrusion Protection Systems (IPS)	أنظمة الحماية من التسلل	□
□	Data Encryption	تشفير البيانات	□
□	Digital Signature Certificates	التوقيعات الرقمية / الشهادات الرقمية	□

□	Password Policies	سياسات كلمة المرور	□
□	I don't know	لا أعرف	□

47. Within our organization, we have implemented Employee Awareness programs/strategies in order to minimize some vulnerabilities that facilitate cyberattacks.

47. في مؤسستنا، قمنا بتنفيذ برامج / استراتيجيات توعوية للموظفين بغرض الحد من بعض نقاط الضعف التي تسهل الهجمات الإلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

48. Within our organization, we have implemented a strong Organizational Security Policies on employee awareness programs in cybersecurity.

48. في مؤسستنا، قمنا بتطبيق سياسات أمن المعلومات (الأمن السيبراني) ضمن برامج توعوية للموظفين في مجال الأمن الإلكتروني (الأمن السيبراني).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

49. Within our organization, an increase in Employee Awareness has minimized some vulnerabilities that facilitate cyberattacks.

49. في مؤسستنا، ساهمت زيادة وعي الموظفين في الحد من بعض نقاط الضعف التي تسهل الهجمات الإلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

50. Our employees know what to do and whom to contact in case of a cybersecurity breach in our Organization
50. موظفينا يعلمون ما الذي يجب القيام به والجهة التي يجب الاتصال بها في حال حدوث خرق أمني إلكتروني (القرصنة) في المؤسسة

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

51. All employees who join our organization must go through a cybersecurity awareness training.
51. كل الموظفين الذين يلتحقون بمؤسستنا يجب عليهم الالتحاق بدورة تدريبية و توعوية حول الأمن الإلكتروني (الأمن السيبراني).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

52. Most employees generally understand the different types of cyberattacks.
52. معظم الموظفين على دراية بمختلف أنواع الهجمات الإلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

53. Weak passwords by employees is not a threat to network systems.
53. كلمات المرور الضعيفة و السهلة التي يستخدمها الموظفون لا تشكل تهديدا لنظم الشبكة.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

54. Employees in our organization understand their responsibility in preventing against cyberattacks
54. يُدرك الموظفون في مؤسستنا مسؤوليتهم في منع الهجمات الإلكترونية (القرصنة).

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

55. Our employees are able to tell when their computers have been infected by viruses.
55. موظفونا قادرون على تحديد متى تعرضت أجهزة الكمبيوتر الخاصة بهم لإصابة بفيروسات.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

56. Our employees know the importance of keeping their passwords secret.
56. يُدرك موظفونا أهمية الحفاظ على سرية كلمات المرور الخاصة بهم.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

57. Our employees understand the importance of not connecting their personal devices (smartphones etc.) on corporate network systems.
57. يُدرك موظفونا أهمية عدم توصيل أجهزتهم الشخصية (مثل الهواتف الذكية، و الأجهزة اللوحية،...إلخ) بنظم شبكة المؤسسة الإلكترونية.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
O	O	O	O	O

Thank you for participating!
نشكركم على مشاركتكم،،،

Appendix 2: Ethics Application

UAEU Division of Research & Graduate Studies

جامعة الإمارات العربية المتحدة
United Arab Emirates University

Social Sciences Research Ethics Committee
-Research Ethics Review Form

A. Title of Study

A Framework for the Evaluation of Cyber-Security Effectiveness of Abu Dhabi Government Entities

B. Principle investigator (and co-investigator(s))

1. Name of PI: Abdulla Al Nuaimi
   Program: DBA Program: DBA
   Mobile: 050 616 1881
   Email: 200350510@uaeu.ac.ae

2. Name(s) of co-investigator(s):* N/A
   Department(s) (if within UAE University):
   Organization(s)/Department(s)/Unit(s) (*if other than within UAE University*):
   Phone:
   Email:

**Copy and paste (2) as needed.*

C. Abstract

(Give a brief abstract of the proposed research (not more than one page)

Cyberspace has become the new frontier for countries to demonstrate power. Nations that have developed defensive mechanisms or those that can successfully launch attacks against adversaries will become the

Appendix 3: Letter of Introduction

UAEU Faculty of Business & Economics

United Arab Emirates University

22 March,2015

TO WHOM IT MAY CONCERN

RE: FIELD RESEARCH BY MR. ABDULLA RASHID AL NEAIMI – STUDENT

The above named student, Mr. Abdulla Rashid Al Neaimi is currently undertaking a Doctoral study in Business Administration (DBA) program at the UAE University (UAEU). For his dissertation, he has chosen the title: *"A Framework for the Evaluation of Cyber-Security Effectiveness of Abu Dhabi Government Entities"*. In order to complete his study, he needs to conduct a survey of key government of Abu Dhabi Agencies that include senior management as well as key personnel responsible for IT and Cybersecurity.

As his supervisor, I am aware of the methodology and approach of this study and so understand the importance of conducting this survey. The UAE University and all of its students are bound by ethical considerations when conducting research. Therefore you are assured, among other things of the following:

1. Your consent must be obtained before the survey is given to you.
2. Should you agree to participate, your name or the name of the government agency you work in will not be used or mentioned anywhere on the survey questionnaire.
3. You (government officer) are not obligated to answer any or all the questions given.
4. All information given by you will only be used for the purpose of this study.

I fully support this effort and is available, through email, to answer any questions or provide additional clarifications.

Yours Sincerely,

Dr. James Thomas Kamparath,
Supervising Professor

Faculty of Business & Economics
United Arab Emirates University

Appendix 4: Consent Form

Social Sciences Research Ethics Committee
- Consent to Participate in a Research Study-

Please read carefully before signing the Consent Form!

A Framework for the Evaluation of Cyber-Security Effectiveness of Abu Dhabi Government Entities

You will be asked to provide or deny consent after reading this form.

Topic of the research, the researcher(s) and the location

You have been invited to take part in a study to **investigate Cybersecurity Effectiveness of Abu Dhabi Government Entities**

This study will be conducted by **Mr. Abdulla Al Neaimi] in DBA Program of UAEU**.

The study will take place via survey monkey. Participants will receive email inviting them to this study if they choose. The questionnaire will take approximately 15 minutes to complete.

Benefit of the research

It is hoped that the results of this study will be beneficial in two main ways:

1. Provide a uniform way of evaluating cybersecurity effectiveness in government entities.
2. Provide a basis which cybersecurity can be enhanced in government departments.

Procedure/setting

The online survey can be done by using any device that has internet connection (phone, ipad, computer etc).

Confidentiality and Privacy Information

No names of participants or the agencies they work for will be collected or used in this study.

Right to Withdraw

Participants are free to withdraw from this study at any time.

Informed Consent

1. I confirm that I have read and understood the above information sheet and have had the opportunity to ask questions.
2. I understand that my participation is voluntary and that I am free to withdraw.
3. I understand that my data will be kept confidential and if published, the data will not be identifiable as mine.

I agree to take part in this study:

(Name and signature of participant)	(Date)
(Name and signature of person taking consent)	(Date)
(Name and signature of witness (if participant unable to read/write)	(Date)
(Name and signature of parent/guardian/next of kin (when participant unable to give consent due to age or incapacity)	(Date)

Appendix 5: Statistical Tables and Analysis

Table 63: Descriptive Statistics-Education Background Vs Managerial Level

What is your Education Background * Your Managerial Level Crosstabulation

Count

		Your Managerial Level					Total
		1 Officer	2 Station manager/ Team Leader	3 CIO/CISO	4 Exec-Director	5 Consultant	
What is your Education Background	1 High School	1	19	12	0	0	32
	2 Diploma	9	0	13	10	0	32
	3 Higher Diploma	3	0	0	12	3	18
	4 Bachelors	189	81	0	0	10	280
	5 Masters	56	43	0	0	0	99
	6 Doctorate or PHD	0	6	0	0	0	6
Total		258	149	25	22	13	467

Table 64: Descriptive Statistics- Gov't Sector Vs. Number of Employees

Employ Govt Sector * Number of Employees Crosstabulation

Count

		Number of Employees					Total
		1 <100	2 100 - 200	3 201 - 500	4 501 – 999	5 >1000	
Employ Govt Sector	1 Social and Civic	65	38	21	32	24	180
	2 Culture and Recreation	33	7	7	10	9	66
	3 Transport	16	5	5	6	11	43
	4 Economic Affairs	9	6	23	5	15	58
	5 Health	2	6	6	2	8	24
	6 Education	2	6	4	11	16	39
	7 Public Order	5	6	5	3	8	27
	8 Science and Technology	3	4	5	5	13	30
Total		135	78	76	74	104	467

Table 65: Descriptive Statistics-Education Background vs Managerial Level

What is your Education Background * Your Managerial Level Crosstabulation

Count

		Your Managerial Level					Total
		1 Officer	2 Station manager/ Team Leader	3 CIO/CISO	4 Exec-Director	5 Consultant	
What is your Education Background	1 High School	11	14	7	0	0	32
	2 Diploma	9	6	11	6	0	32
	3 Higher Diploma	3	1	3	8	3	18
	4 Bachelors	25	30	73	100	52	280
	5 Masters	4	4	10	34	47	99
	6 Doctorate or PHD	0	0	0	5	1	6
Total		52	55	104	153	103	467

Table 66: Descriptive Statistics-Gov't Experience Vs Managerial Level

Your Govt Experience * Your Managerial Level Crosstabulation

Count

		Your Managerial Level					Total
		1 Officer	2 Station manager/Team Leader	3 CIO/CISO	4 Exec-Director	5 Consultant	
Your Govt Experience	1 0 -5 years	30	22	44	31	2	129
	2 5 - 10 years	19	4	37	96	25	181
	3 >10 Years	3	29	23	26	76	157
Total		52	55	104	153	103	467

Table 67: Descriptive Statistics- Study Population by Education Background

What is your Education Background

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 High School	32	5.3	6.9	6.9
	2 Diploma	32	5.3	6.9	13.7
	3 Higher Diploma	18	3.0	3.9	17.6
	4 Bachelors	280	46.7	60.0	77.5
	5 Masters	99	16.5	21.2	98.7
	6 Doctorate or PHD	6	1.0	1.3	100.0
	Total	467	77.8	100.0	
Missing	System	133	22.2		
	Total	600	100.0		

Table 68: Descriptive Statistics- Study Population by Major

What is your major					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 No Major	13	2.2	2.8	2.8
	2 Computer or IT related	145	24.2	31.0	33.8
	3 Engineering Related	70	11.7	15.0	48.8
	4 Business Related	158	26.3	33.8	82.7
	5 Others	81	13.5	17.3	100.0
	Total	467	77.8	100.0	
Missing	System	133	22.2		
Total		600	100.0		

Table 69: Descriptive Statistics- Study Population by Education by Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 0 -5 years	129	21.5	27.6	27.6
	2 5 - 10 years	181	30.2	38.8	66.4
	3 >10 Years	157	26.2	33.6	100.0
	Total	467	77.8	100.0	
Missing	System	133	22.2		
Total		600	100.0		

Table 70: Descriptive Stats - Correlation Results

Correlations

		CE_mean1	CK_mean1	RoT_mean1	SM_mean1	UT_mean	SP_mean1	UA_mean
CE_mean1	Pearson Correlation	1	.397**	.367**	.245**	.373**	.337**	.301**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000
	N	467	467	467	467	467	467	466
CK_mean1	Pearson Correlation	.397**	1	.430**	.243**	.466**	.406**	.139**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.003
	N	467	467	467	467	467	467	466
RoT_mean1	Pearson Correlation	.367**	.430**	1	.243**	.346**	.375**	.133**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.004
	N	467	467	467	467	467	467	466
SM_mean1	Pearson Correlation	.245**	.243**	.243**	1	.122**	.275**	.026
	Sig. (2-tailed)	.000	.000	.000		.008	.000	.573
	N	467	467	467	467	467	467	466
UT_mean	Pearson Correlation	.373**	.466**	.346**	.122**	1	.244**	.108*
	Sig. (2-tailed)	.000	.000	.000	.008		.000	.019
	N	467	467	467	467	467	467	466
SP_mean1	Pearson Correlation	.337**	.406**	.375**	.275**	.244**	1	.074
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.113
	N	467	467	467	467	467	467	466
UA_mean	Pearson Correlation	.301**	.139**	.133**	.026	.108*	.074	1
	Sig. (2-tailed)	.000	.003	.004	.573	.019	.113	
	N	466	466	466	466	466	466	466

**. Correlation is significant at the 0.01 level (2-tailed).

Table 71: Descriptive - Stats (Mean and Standard Deviation)

Descriptive Statistics

	Mean	Std. Deviation	N
CE_mean1	4.1352	.62173	467
CK_mean1	4.1501	.56344	467
RoT_mean1	3.7804	.62965	467
SM_mean1	3.7212	.69547	467
UT_mean	4.0557	.63273	467
SP_mean1	3.9543	.54941	467
UA_mean	4.0012	.62463	466

Table 72: Reliability Statistical results: Cronbach Alpha and PCA
Cronbach alpha-Rotated Component Matrix

Component Matrix[a]

	Component						
	1	2	3	4	5	6	7
SM9	.720	.321					
SM1	.714	.303					
SM8	.706	.334					
SM7	.704	.325					
SM2	.697	.357					
SM3	.666	.320					
SM4	.662	.349					
SM6	.621						
SM10	.580						
SM5	.491						
CK1	-.390	.642	.327				
CK2	-.423	.616	.301				
CK5	-.400	.566	.308				
CK4	-.415	.559	.347				
CK8	-.418	.556					
CK6	-.410	.544					
CK10	-.425	.539					
CK7	-.412	.520					
CK9	-.322	.507					
CK3	-.342	.504	.327				
RoT11		-.409	.686				
RoT6		-.412	.680				
RoT7		-.352	.673				
RoT3		-.421	.652				
RoT10		-.421	.628				
RoT8		-.330	.614				
RoT12		-.330	.614				
RoT4		-.367	.612				
RoT5		-.348	.593				
RoT1		-.322	.520				
RoT2			.473				
RoT9			.338				
UTA5				.739			-.304
UTA11				.709			-.305
UTA4				.693			
UTA7				.691			
UTA8				.647			
UTA10				.643			.311
UTA6				.627			

Table 72: Reliability Statistical results: Cronbach Alpha and PCA
Cronbach alpha-Rotated Component Matrix (Continued)

UTA3			.529			.412
CE3				.684		
CE4	-.316			.671		
CE7	-.336			.606		
CE6				.604		
CE5				.599		
CE2				.533		
UTA1				.341		
SP3					.656	
SP1		-.302			.623	
SP2		-.327			.575	
SP4		-.323			.565	
UTA9			.442			.599
UTA2			.394			.534

Extraction Method: Principal Component Analysis.
a. 7 components extracted.

Table 73: Component Transformation Matrix-Varimax Rotation

Component Transformation Matrix

Component	1	2	3	4	5	6	7
1	.804	-.489	-.033	-.097	-.250	.181	-.091
2	.381	.705	-.489	-.190	-.145	-.230	-.094
3	.273	.381	.865	-.007	-.091	-.153	-.003
4	.201	.108	-.103	.871	-.033	.014	.421
5	.298	.067	.000	-.071	.937	.141	.057
6	-.064	.306	.028	.126	-.103	.872	-.338
7	-.016	.093	.008	-.418	-.134	.332	.829

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

Table 74: Reliability Statistics-Rotated component Matrix-Cumulative Variance

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.791	12.814	12.814	6.791	12.814	12.814	6.174	11.648	11.648
2	6.344	11.971	24.784	6.344	11.971	24.784	5.899	11.130	22.778
3	5.767	10.881	35.665	5.767	10.881	35.665	5.886	11.106	33.884
4	4.183	7.893	43.558	4.183	7.893	43.558	3.822	7.210	41.094
5	2.843	5.363	48.922	2.843	5.363	48.922	3.163	5.969	47.063
6	2.206	4.163	53.084	2.206	4.163	53.084	2.621	4.944	52.007
7	1.748	3.298	56.383	1.748	3.298	56.383	2.319	4.375	56.383
8	1.616	3.049	59.432						
9	1.224	2.310	61.742						
10	1.134	2.140	63.882						
11	1.046	1.974	65.857						
12	1.037	1.957	67.814						
13	.928	1.750	69.564						
14	.873	1.647	71.211						
15	.862	1.626	72.837						
16	.827	1.561	74.398						
17	.770	1.453	75.851						
18	.680	1.282	77.134						
19	.664	1.254	78.387						
20	.653	1.231	79.619						
21	.643	1.212	80.831						
22	.610	1.150	81.981						
23	.590	1.113	83.094						
24	.563	1.063	84.156						
25	.530	1.001	85.157						
26	.512	.967	86.124						
27	.498	.940	87.064						

Table 74: Reliability Statistics-Rotated Component Matrix-Cumulative Variance (Continued)

28	.452	.853	87.917						
29	.446	.841	88.758						
30	.428	.808	89.566						
31	.424	.801	90.367						
32	.421	.794	91.161						
33	.384	.724	91.885						
34	.368	.695	92.580						
35	.353	.665	93.245						
36	.350	.661	93.906						
37	.341	.643	94.549						
38	.333	.628	95.177						
39	.299	.565	95.742						
40	.270	.509	96.251						
41	.257	.484	96.735						
42	.247	.466	97.201						
43	.224	.422	97.623						
44	.218	.410	98.033						
45	.203	.383	98.416						
46	.194	.366	98.782						
47	.171	.322	99.104						
48	.150	.282	99.386						
49	.120	.226	99.612						
50	.104	.196	99.808						
51	.102	.192	100.000						
52	.000	.000	100.000						
53	.000	.000	100.000						
Extraction Method: Principal Component Analysis.									

Table 75: ANOVA Group Comparison Results for Competence of Staff (CK)

CK_mean1

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.140	7	.591	1.888	.070
Within Groups	143.801	459	.313		
Total	147.941	466			

Table 76: Regression analysis Results for Competence of Staff – CK

Descriptives

CK_mean1

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Social and Civic	180	4.0848	.59740	.04453	3.9970	4.1727	2.00	5.00
Culture and Recreation	66	4.1182	.59223	.07290	3.9726	4.2638	2.00	5.00
Transport	43	4.3302	.44909	.06849	4.1920	4.4684	3.40	5.00
Economic Affairs	58	4.2279	.51687	.06787	4.0920	4.3638	2.00	5.00
Health	24	4.3750	.35047	.07154	4.2270	4.5230	3.60	5.00
Education	39	4.0564	.68664	.10995	3.8338	4.2790	2.00	5.00
Public Order	27	4.1407	.45341	.08726	3.9614	4.3201	3.20	5.00
Science and Technology	30	4.1533	.50291	.09182	3.9655	4.3411	3.20	5.00
Total	467	4.1501	.56344	.02607	4.0988	4.2013	2.00	5.00

CK_mean1

Levene Statistic	df1	df2	Sig.
1.730	7	459	.100

Table 77: Post Hoc Test Results for Competence of Staff- CK

Multiple Comparisons						
Dependent Variable: CK_mean1						
LSD						
(I) Employ Govt Sector	(J) Employ Govt Sector	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Social and Civic	Culture and Recreation	-.03336	.08054	.679	-.1916	.1249
	Transport	-.24541*	.09501	.010	-.4321	-.0587
	Economic Affairs	-.14308	.08451	.091	-.3092	.0230
	Health	-.29018*	.12163	.017	-.5292	-.0512
	Education	.02841	.09886	.774	-.1659	.2227
	Public Order	-.05592	.11552	.629	-.2829	.1711
	Science and Technology	-.06851	.11038	.535	-.2854	.1484
Culture and Recreation	Social and Civic	.03336	.08054	.679	-.1249	.1916
	Transport	-.21205	.10969	.054	-.4276	.0035
	Economic Affairs	-.10972	.10074	.277	-.3077	.0883
	Health	-.25682	.13342	.055	-.5190	.0054
	Education	.06177	.11305	.585	-.1604	.2839
	Public Order	-.02256	.12787	.860	-.2738	.2287
	Science and Technology	-.03515	.12325	.776	-.2774	.2070
Transport	Social and Civic	.24541*	.09501	.010	.0587	.4321
	Culture and Recreation	.21205	.10969	.054	-.0035	.4276
	Economic Affairs	.10233	.11264	.364	-.1190	.3237
	Health	-.04477	.14262	.754	-.3250	.2355
	Education	.27382*	.12377	.027	.0306	.5170
	Public Order	.18949	.13744	.169	-.0806	.4596
	Science and Technology	.17690	.13315	.185	-.0848	.4386
Economic Affairs	Social and Civic	.14308	.08451	.091	-.0230	.3092
	Culture and Recreation	.10972	.10074	.277	-.0883	.3077
	Transport	-.10233	.11264	.364	-.3237	.1190
	Health	-.14710	.13585	.279	-.4141	.1199
	Education	.17149	.11591	.140	-.0563	.3993
	Public Order	.08716	.13040	.504	-.1691	.3434
	Science and Technology	.07457	.12588	.554	-.1728	.3219
Health	Social and Civic	.29018*	.12163	.017	.0512	.5292
	Culture and Recreation	.25682	.13342	.055	-.0054	.5190
	Transport	.04477	.14262	.754	-.2355	.3250
	Economic Affairs	.14710	.13585	.279	-.1199	.4141
	Education	.31859*	.14521	.029	.0332	.6040

Table 77: Post hoc Test Results for Competence of Staff (CK-Continued)

	Public Order	.23426	.15703	.136	-.0743	.5428
	Science and Technology	.22167	.15329	.149	-.0796	.5229
Education	Social and Civic	-.02841	.09886	.774	-.2227	.1659
	Culture and Recreation	-.06177	.11305	.585	-.2839	.1604
	Transport	-.27382*	.12377	.027	-.5170	-.0306
	Economic Affairs	-.17149	.11591	.140	-.3993	.0563
	Health	-.31859*	.14521	.029	-.6040	-.0332
	Public Order	-.08433	.14013	.548	-.3597	.1910
	Science and Technology	-.09692	.13593	.476	-.3640	.1702
Public Order	Social and Civic	.05592	.11552	.629	-.1711	.2829
	Culture and Recreation	.02256	.12787	.860	-.2287	.2738
	Transport	-.18949	.13744	.169	-.4596	.0806
	Economic Affairs	-.08716	.13040	.504	-.3434	.1691
	Health	-.23426	.15703	.136	-.5428	.0743
	Education	.08433	.14013	.548	-.1910	.3597
	Science and Technology	-.01259	.14848	.932	-.3044	.2792
Science and Technology	Social and Civic	.06851	.11038	.535	-.1484	.2854
	Culture and Recreation	.03515	.12325	.776	-.2070	.2774
	Transport	-.17690	.13315	.185	-.4386	.0848
	Economic Affairs	-.07457	.12588	.554	-.3219	.1728
	Health	-.22167	.15329	.149	-.5229	.0796
	Education	.09692	.13593	.476	-.1702	.3640
	Public Order	.01259	.14848	.932	-.2792	.3044
*. The mean difference is significant at the 0.05 level.						

Table 78: ANOVA and Regression Results for Level of Technology (RoT)

Descriptives

RoT_mean1

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Social and Civic	180	3.6989	.66538	.04959	3.6010	3.7967	1.17	5.00
Culture and Recreation	66	3.7660	.50284	.06190	3.6423	3.8896	2.50	5.00
Transport	43	3.7250	.73832	.11259	3.4978	3.9523	1.83	5.00
Economic Affairs	58	3.8957	.42203	.05542	3.7847	4.0066	2.67	4.83
Health	24	4.1655	.50166	.10240	3.9536	4.3773	3.00	5.00
Education	39	3.7735	.70034	.11214	3.5465	4.0005	1.50	5.00
Public Order	27	3.7346	.74716	.14379	3.4390	4.0301	1.17	5.00
Science and Technology	30	3.9000	.61370	.11205	3.6708	4.1292	2.83	5.00
Total	467	3.7804	.62965	.02914	3.7231	3.8377	1.17	5.00

ANOVA

RoT_mean1

	Sum of Squares	Df	Mean Square	F	Sig.	
Between Groups	6.159	7	.880	2.261	.029	
Within Groups	178.593	459	.389			
Total	184.752	466				

Table 79: Multiple Comparisons with Post hoc Test for Level of Technology (RoT)

	Education	-.07463	.11017	.498	-.2911	.1419
	Public Order	-.03570	.12873	.782	-.2887	.2173
	Science and Technology	-.20113	.12301	.103	-.4429	.0406
Culture and Recreation	Social and Civic	.06708	.08976	.455	-.1093	.2435
	Transport	.04091	.12225	.738	-.1993	.2811
	Economic Affairs	-.12970	.11227	.249	-.3503	.0909
	Health	-.39952*	.14869	.007	-.6917	-.1073
	Education	-.00755	.12598	.952	-.2551	.2400
	Public Order	.03138	.14250	.826	-.2486	.3114
	Science and Technology	-.13405	.13735	.330	-.4040	.1359
Transport	Social and Civic	.02617	.10588	.805	-.1819	.2342
	Culture and Recreation	-.04091	.12225	.738	-.2811	.1993
	Economic Affairs	-.17061	.12553	.175	-.4173	.0761
	Health	-.44043*	.15894	.006	-.7528	-.1281
	Education	-.04846	.13793	.725	-.3195	.2226
	Public Order	-.00953	.15316	.950	-.3105	.2915
	Science and Technology	-.17496	.14839	.239	-.4666	.1166
Economic Affairs	Social and Civic	.19678*	.09418	.037	.0117	.3819
	Culture and Recreation	.12970	.11227	.249	-.0909	.3503
	Transport	.17061	.12553	.175	-.0761	.4173
	Health	-.26981	.15140	.075	-.5673	.0277
	Education	.12215	.12917	.345	-.1317	.3760
	Public Order	.16109	.14532	.268	-.1245	.4467
	Science and Technology	-.00435	.14028	.975	-.2800	.2713
Health	Social and Civic	.46659*	.13555	.001	.2002	.7330
	Culture and Recreation	.39952*	.14869	.007	.1073	.6917
	Transport	.44043*	.15894	.006	.1281	.7528
	Economic Affairs	.26981	.15140	.075	-.0277	.5673
	Education	.39196*	.16183	.016	.0739	.7100
	Public Order	.43090*	.17499	.014	.0870	.7748

Table 79: Multiple Comparisons with Post hoc test for Level of Technology (RoT) (Continued)

Education	Social and Civic	.07463	.11017	.498	-.1419	.2911
	Culture and Recreation	.00755	.12598	.952	-.2400	.2551
	Transport	.04846	.13793	.725	-.2226	.3195
	Economic Affairs	-.12215	.12917	.345	-.3760	.1317
	Health	-.39196*	.16183	.016	-.7100	-.0739
	Public Order	.03894	.15616	.803	-.2680	.3458
	Science and Technology	-.12650	.15148	.404	-.4242	.1712
Public Order	Social and Civic	.03570	.12873	.782	-.2173	.2887
	Culture and Recreation	-.03138	.14250	.826	-.3114	.2486
	Transport	.00953	.15316	.950	-.2915	.3105
	Economic Affairs	-.16109	.14532	.268	-.4467	.1245
	Health	-.43090*	.17499	.014	-.7748	-.0870
	Education	-.03894	.15616	.803	-.3458	.2680
	Science and Technology	-.16543	.16547	.318	-.4906	.1597
Science and Technology	Social and Civic	.20113	.12301	.103	-.0406	.4429
	Culture and Recreation	.13405	.13735	.330	-.1359	.4040
	Transport	.17496	.14839	.239	-.1166	.4666
	Economic Affairs	.00435	.14028	.975	-.2713	.2800
	Health	-.26547	.17083	.121	-.6012	.0702
	Education	.12650	.15148	.404	-.1712	.4242
	Public Order	.16543	.16547	.318	-.1597	.4906

*. The mean difference is significant at the 0.05 level.

Table 80: Regression and ANOVA Test Results for Awareness of Users (UA)

Model Summary Table

Model	R	R Square	Adjusted R Square		Std. Error of the Estimate
1	.013[a]	.000	-.002		.75323

a. Predictors: (Constant), UA_mean

b. Dependent Variable: CE_mean

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2.7701	2.8164	2.8005	.00982	466
Residual	-1.81175	1.79904	.00000	.75242	466
Std. Predicted Value	-3.094	1.612	.000	1.000	466
Std. Residual	-2.405	2.388	.000	.999	466

a. Dependent Variable: CE_mean

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	.021	1	.021	.037	.847[b]
	Residual	263.276	464	.567		
	Total	263.297	465			

Dependent Variable: CE_mean

Table 81: Multiple Comparisons-Tukeys HSD Results for CSE

Multiple Comparisons

Dependent Variable: CE_mean1

LSD

(I) Employ Govt Sector	(J) Employ Govt Sector	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Social and Civic	Culture and Recreation	.08503	.09887	.390	-.1093	.2793
	Transport	.02134	.11663	.855	-.2078	.2505
	Economic Affairs	-.01878	.10374	.856	-.2226	.1851
	Health	-.12158	.14931	.416	-.4150	.1718
	Education	.01237	.12136	.919	-.2261	.2509
	Public Order	.05040	.14180	.722	-.2283	.3291
	Science and Technology	-.51718*	.13550	.000	-.7834	-.2509
Culture and Recreation	Social and Civic	-.08503	.09887	.390	-.2793	.1093
	Transport	-.06368	.13465	.636	-.3283	.2009

Table 81: Multiple Comparisons-Tukeys HSD Results for CSE (Continued)

Transport	Social and Civic	-.02134	.11663	.855	-.2505	.2078
	Culture and Recreation	.06368	.13465	.636	-.2009	.3283
	Economic Affairs	-.04012	.13827	.772	-.3118	.2316
	Health	-.14293	.17507	.415	-.4870	.2011
	Education	-.00898	.15193	.953	-.3075	.2896
	Public Order	.02906	.16871	.863	-.3025	.3606
	Science and Technology	-.53852*	.16345	.001	-.8597	-.2173
Economic Affairs	Social and Civic	.01878	.10374	.856	-.1851	.2226
	Culture and Recreation	.10381	.12366	.402	-.1392	.3468
	Transport	.04012	.13827	.772	-.2316	.3118
	Health	-.10280	.16676	.538	-.4305	.2249
	Education	.03115	.14228	.827	-.2485	.3108
	Public Order	.06918	.16008	.666	-.2454	.3837
	Science and Technology	-.49840*	.15452	.001	-.8020	-.1947
Health	Social and Civic	.12158	.14931	.416	-.1718	.4150
	Culture and Recreation	.20661	.16378	.208	-.1152	.5285
	Transport	.14293	.17507	.415	-.2011	.4870
	Economic Affairs	.10280	.16676	.538	-.2249	.4305
	Education	.13395	.17826	.453	-.2163	.4842
	Public Order	.17198	.19276	.373	-.2068	.5508
	Science and Technology	-.39559*	.18817	.036	-.7654	-.0258
Education	Social and Civic	-.01237	.12136	.919	-.2509	.2261
	Culture and Recreation	.07266	.13877	.601	-.2000	.3454
	Transport	.00898	.15193	.953	-.2896	.3075
	Economic Affairs	-.03115	.14228	.827	-.3108	.2485
	Health	-.13395	.17826	.453	-.4842	.2163
	Public Order	.03803	.17202	.825	-.3000	.3761
	Science and Technology	-.52954*	.16686	.002	-.8574	-.2016

Table 81: Multiple Comparisons-Tukeys HSD Results for CSE (Continued)

Public Order	Social and Civic	-.05040	.14180	.722	-.3291	.2283
	Culture and Recreation	.03463	.15696	.825	-.2738	.3431
	Transport	-.02906	.16871	.863	-.3606	.3025
	Economic Affairs	-.06918	.16008	.666	-.3837	.2454
	Health	-.17198	.19276	.373	-.5508	.2068
	Education	-.03803	.17202	.825	-.3761	.3000
	Science and Technology	-.56757*	.18227	.002	-.9258	-.2094
Science and Technology	Social and Civic	.51718*	.13550	.000	.2509	.7834
	Culture and Recreation	.60220*	.15129	.000	.3049	.8995
	Transport	.53852*	.16345	.001	.2173	.8597
	Economic Affairs	.49840*	.15452	.001	.1947	.8020
	Health	.39559*	.18817	.036	.0258	.7654
	Education	.52954*	.16686	.002	.2016	.8574
	Public Order	.56757*	.18227	.002	.2094	.9258

*. The mean difference is significant at the 0.05 level.

Table 82: ANOVA and Regression Results for Training of Staff

Descriptives

UT_mean

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Social and Civic	180	4.0324	.66254	.04938	3.9349	4.1298	1.00	5.00
Culture and Recreation	66	3.8399	.61062	.07516	3.6898	3.9900	2.00	5.00
Transport	43	4.1434	.53702	.08189	3.9781	4.3087	2.83	5.00
Economic Affairs	58	4.1721	.54649	.07176	4.0284	4.3158	2.40	5.00
Health	24	4.1722	.55696	.11369	3.9370	4.4074	3.00	5.00
Education	39	4.1299	.71781	.11494	3.8972	4.3626	2.00	5.00
Public Order	27	3.8938	.74627	.14362	3.5986	4.1890	2.00	5.00
Science and Technology	30	4.2756	.47107	.08601	4.0997	4.4515	3.17	5.00
Total	467	4.0557	.63273	.02928	3.9982	4.1132	1.00	5.00

UT_mean

Levene Statistic	df1	df2	Sig.
.885	7	459	.518

Table 83: Multiple Comparisons using Tukeys HSD for Training of Staff

Multiple Comparisons						
Dependent Variable: UT_mean						
LSD						
(I) Employ Govt Sector	(J) Employ Govt Sector	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Social and Civic	Culture and Recreation	.19251*	.09001	.033	.0156	.3694
	Transport	-.11103	.10617	.296	-.3197	.0976
	Economic Affairs	-.13968	.09444	.140	-.3253	.0459
	Health	-.13984	.13592	.304	-.4069	.1273
	Education	-.09753	.11048	.378	-.3146	.1196
	Public Order	.13856	.12909	.284	-.1151	.3922
	Science and Technology	-.24317*	.12335	.049	-.4856	-.0008
Culture and Recreation	Social and Civic	-.19251*	.09001	.033	-.3694	-.0156
	Transport	-.30353*	.12258	.014	-.5444	-.0626
	Economic Affairs	-.33218*	.11258	.003	-.5534	-.1110
	Health	-.33235*	.14909	.026	-.6253	-.0394
	Education	-.29004*	.12633	.022	-.5383	-.0418

Table 83: Multiple Comparisons using Tukeys HSD for Training of Staff (Continued)

	Public Order	-.05395	.14289	.706	-.3348	.2269
	Science and Technology	-.43568*	.13773	.002	-.7063	-.1650
Transport	Social and Civic	.11103	.10617	.296	-.0976	.3197
	Culture and Recreation	.30353*	.12258	.014	.0626	.5444
	Economic Affairs	-.02865	.12587	.820	-.2760	.2187
	Health	-.02881	.15937	.857	-.3420	.2844
	Education	.01350	.13831	.922	-.2583	.2853
	Public Order	.24958	.15359	.105	-.0522	.5514
	Science and Technology	-.13214	.14879	.375	-.4245	.1603
Economic Affairs	Social and Civic	.13968	.09444	.140	-.0459	.3253
	Culture and Recreation	.33218*	.11258	.003	.1110	.5534
	Transport	.02865	.12587	.820	-.2187	.2760
	Health	-.00016	.15181	.999	-.2985	.2982
	Education	.04215	.12953	.745	-.2124	.2967
	Public Order	.27823	.14572	.057	-.0081	.5646
	Science and Technology	-.10349	.14066	.462	-.3799	.1729
Health	Social and Civic	.13984	.13592	.304	-.1273	.4069
	Culture and Recreation	.33235*	.14909	.026	.0394	.6253
	Transport	.02881	.15937	.857	-.2844	.3420
	Economic Affairs	.00016	.15181	.999	-.2982	.2985
	Education	.04231	.16227	.794	-.2766	.3612
	Public Order	.27840	.17547	.113	-.0664	.6232
	Science and Technology	-.10333	.17130	.547	-.4400	.2333
Education	Social and Civic	.09753	.11048	.378	-.1196	.3146
	Culture and Recreation	.29004*	.12633	.022	.0418	.5383
	Transport	-.01350	.13831	.922	-.2853	.2583
	Economic Affairs	-.04215	.12953	.745	-.2967	.2124
	Health	-.04231	.16227	.794	-.3612	.2766
	Public Order	.23609	.15659	.132	-.0716	.5438

Table 83: Multiple Comparisons using Tukeys HSD for Training of Staff (Continued).

	Science and Technology	-.14564	.15190	.338	-.4441	.1529
Public Order	Social and Civic	-.13856	.12909	.284	-.3922	.1151
	Culture and Recreation	.05395	.14289	.706	-.2269	.3348
	Transport	-.24958	.15359	.105	-.5514	.0522
	Economic Affairs	-.27823	.14572	.057	-.5646	.0081
	Health	-.27840	.17547	.113	-.6232	.0664
	Education	-.23609	.15659	.132	-.5438	.0716
	Science and Technology	-.38173*	.16593	.022	-.7078	-.0557
Science and Technology	Social and Civic	.24317*	.12335	.049	.0008	.4856
	Culture and Recreation	.43568*	.13773	.002	.1650	.7063
	Transport	.13214	.14879	.375	-.1603	.4245
	Economic Affairs	.10349	.14066	.462	-.1729	.3799
	Health	.10333	.17130	.547	-.2333	.4400
	Education	.14564	.15190	.338	-.1529	.4441
	Public Order	.38173*	.16593	.022	.0557	.7078

*. The mean difference is significant at the 0.05 level.

Table 84: ANOVA and Regression Results for Support from Management

Descriptives

SP_mean1

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Social and Civic	180	3.9062	.54478	.04061	3.8261	3.9863	2.00	5.00
Culture and Recreation	66	3.8811	.55958	.06888	3.7435	4.0187	2.60	5.00
Transport	43	3.9831	.58383	.08903	3.8035	4.1628	2.75	5.00
Economic Affairs	58	4.0985	.50790	.06669	3.9649	4.2320	2.63	5.00
Health	24	4.0813	.48808	.09963	3.8752	4.2873	3.13	5.00
Education	39	3.9936	.52796	.08454	3.8224	4.1647	2.63	5.00
Public Order	27	3.8722	.44199	.08506	3.6974	4.0471	3.13	5.00
Science and Technology	30	4.0057	.70206	.12818	3.7435	4.2678	2.38	5.00
Total	467	3.9543	.54941	.02542	3.9044	4.0043	2.00	5.00

Table 85: Test of Homogeneity of Variances for Support from Management

SP_mean1

Levene Statistic	df1	df2	Sig.
1.185	7	459	.310

Table 86: Multiple Comparisons for Support from Management

	Culture and Recreation	.21739*	.09867	.028	.0235	.4113
	Transport	.11534	.11032	.296	-.1015	.3321
	Health	.01723	.13305	.897	-.2442	.2787
	Education	.10489	.11352	.356	-.1182	.3280
	Public Order	.22626	.12772	.077	-.0247	.4772
	Science and Technology	.09280	.12328	.452	-.1495	.3351
Health	Social and Civic	.17507	.11913	.142	-.0590	.4092
	Culture and Recreation	.20016	.13067	.126	-.0566	.4570
	Transport	.09811	.13968	.483	-.1764	.3726
	Economic Affairs	-.01723	.13305	.897	-.2787	.2442
	Education	.08766	.14222	.538	-.1918	.3672
	Public Order	.20903	.15379	.175	-.0932	.5113
	Science and Technology	.07557	.15013	.615	-.2195	.3706
Education	Social and Civic	.08741	.09683	.367	-.1029	.2777
	Culture and Recreation	.11250	.11072	.310	-.1051	.3301
	Transport	.01045	.12122	.931	-.2278	.2487
	Economic Affairs	-.10489	.11352	.356	-.3280	.1182
	Health	-.08766	.14222	.538	-.3672	.1918
	Public Order	.12137	.13725	.377	-.1483	.3911
	Science and Technology	-.01209	.13313	.928	-.2737	.2495
Public Order	Social and Civic	-.03396	.11314	.764	-.2563	.1884
	Culture and Recreation	-.00887	.12524	.944	-.2550	.2372
	Transport	-.11092	.13461	.410	-.3754	.1536
	Economic Affairs	-.22626	.12772	.077	-.4772	.0247
	Health	-.20903	.15379	.175	-.5113	.0932
	Education	-.12137	.13725	.377	-.3911	.1483
	Science and Technology	-.13346	.14542	.359	-.4192	.1523
Science and Technology	Social and Civic	.09951	.10811	.358	-.1129	.3120
	Culture and Recreation	.12460	.12071	.303	-.1126	.3618
	Transport	.02254	.13041	.863	-.2337	.2788
	Economic Affairs	-.09280	.12328	.452	-.3351	.1495
	Health	-.07557	.15013	.615	-.3706	.2195
	Education	.01209	.13313	.928	-.2495	.2737
	Public Order	.13346	.14542	.359	-.1523	.4192

Table 87: Test of Homogeneity of Variances for User Awareness

UA_mean

Levene Statistic	df1	df2	Sig.
1.514	7	458	.160

Table 88: Test of Homogeneity of Variances for Cybersecurity Effectiveness Variable

CE_mean1

Levene Statistic	df1	df2	Sig.
1.894	7	459	.069

CE_mean1

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	6.286	7	.898	2.371	.022
Within Groups	173.844	459	.379		
Total	180.131	466			

Table 89: Multiple Comparisons using Tukeys HSD for Cybersecurity Effectiveness (CSE)

Multiple Comparisons

Dependent Variable: CSE_mean1

(I) Employ Govt Sector	(J) Employ Govt Sector	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Social and Civic	Culture and Recreation	.02374	.08856	.789	-.1503	.1978
	Transport	-.15005	.10446	.152	-.3553	.0552
	Economic Affairs	-.16158	.09292	.083	-.3442	.0210
	Health	-.12020	.13374	.369	-.3830	.1426
	Education	.00928	.10870	.932	-.2043	.2229
	Public Order	.25943*	.12701	.042	.0098	.5090
	Science and Technology	-.27687*	.12136	.023	-.5154	-.0384
Culture and Recreation	Social and Civic	-.02374	.08856	.789	-.1978	.1503
	Transport	-.17378	.12061	.150	-.4108	.0632
	Economic Affairs	-.18531	.11076	.095	-.4030	.0324
	Health	-.14394	.14670	.327	-.4322	.1443
	Education	-.01445	.12430	.907	-.2587	.2298
	Public Order	.23569	.14059	.094	-.0406	.5120
	Science and Technology	-.30061*	.13551	.027	-.5669	-.0343

Table 89: Multiple Comparisons using Tukeys HSD for Cybersecurity Effectiveness (CSE)- (Continued)

Transport	Social and Civic	.15005	.10446	.152	-.0552	.3553
	Culture and Recreation	.17378	.12061	.150	-.0632	.4108
	Economic Affairs	-.01153	.12385	.926	-.2549	.2318
	Health	.02984	.15681	.849	-.2783	.3380
	Education	.15933	.13609	.242	-.1081	.4268
	Public Order	.40947*	.15111	.007	.1125	.7064
	Science and Technology	-.12682	.14640	.387	-.4145	.1609
Economic Affairs	Social and Civic	.16158	.09292	.083	-.0210	.3442
	Culture and Recreation	.18531	.11076	.095	-.0324	.4030
	Transport	.01153	.12385	.926	-.2318	.2549
	Health	.04137	.14937	.782	-.2522	.3349
	Education	.17086	.12744	.181	-.0796	.4213
	Public Order	.42100*	.14338	.003	.1392	.7028
	Science and Technology	-.11529	.13840	.405	-.3873	.1567
Health	Social and Civic	.12020	.13374	.369	-.1426	.3830
	Culture and Recreation	.14394	.14670	.327	-.1443	.4322
	Transport	-.02984	.15681	.849	-.3380	.2783
	Economic Affairs	-.04137	.14937	.782	-.3349	.2522
	Education	.12949	.15966	.418	-.1843	.4432
	Public Order	.37963*	.17265	.028	.0403	.7189
	Science and Technology	-.15667	.16854	.353	-.4879	.1745
Education	Social and Civic	-.00928	.10870	.932	-.2229	.2043
	Culture and Recreation	.01445	.12430	.907	-.2298	.2587
	Transport	-.15933	.13609	.242	-.4268	.1081
	Economic Affairs	-.17086	.12744	.181	-.4213	.0796
	Health	-.12949	.15966	.418	-.4432	.1843
	Public Order	.25014	.15407	.105	-.0526	.5529
	Science and Technology	-.28615	.14945	.056	-.5799	.0075
Public Order	Social and Civic	-.25943*	.12701	.042	-.5090	-.0098
	Culture and Recreation	-.23569	.14059	.094	-.5120	.0406
	Transport	-.40947*	.15111	.007	-.7064	-.1125
	Economic Affairs	-.42100*	.14338	.003	-.7028	-.1392
	Health	-.37963*	.17265	.028	-.7189	-.0403
	Education	-.25014	.15407	.105	-.5529	.0526
	Science and Technology	-.53630*	.16326	.001	-.8571	-.2155
Science and Technology	Social and Civic	.27687*	.12136	.023	.0384	.5154
	Culture and Recreation	.30061*	.13551	.027	.0343	.5669
	Transport	.12682	.14640	.387	-.1609	.4145
	Economic Affairs	.11529	.13840	.405	-.1567	.3873
	Health	.15667	.16854	.353	-.1745	.4879
	Education	.28615	.14945	.056	-.0075	.5799
	Public Order	.53630*	.16326	.001	.2155	.8571

*. The mean difference is significant at the 0.05 level.