CRANFIELD UNIVERSITY

Sabri Al-Azazi

A multi-layer model for e-government information security assessment

SCHOOL OF APPLIED SCIENCES

PhD THESIS

CRANFIELD UNIVERSITY

SCHOOL OF APPLIED SCIENCES

PhD THESIS

Academic Year 2007-2008

SABRI AL-AZAZI

A multi-layer model for e-government information security assessment

Supervisor: **Dr. Ip-Shing Fan**

February 2008

This thesis is submitted in partial fulfilment of the requirements
for the Degree of Doctor of Philosophy

Abstract

The emphasis on the value of time from the knowledge workers and citizens has driven governments towards the transformation to the electronic method in offering government services to the public. This underpinned the need of launching e-governments worldwide. The inter-government integration, information sharing and collaboration is required to provide the citizens with well integrated services. The level of trust is one of the key factors for the integration and information sharing between the government departments. Information security contributes directly to the increased level of trust between the government departments by providing an assurance of confidentiality, integrity, and availability of sensitive governmental information.

The research reported in this thesis delivers a new model that can be used as a tool to assess the level of security readiness of government departments, a checklist for the required security measures, and as a common reference for the security in the government departments in Dubai. Based on extensive literature research a new model was developed using a qualitative approach to build the overall structure and the number of layers in it. A quantitative approach was adopted during the research study to confirm the importance of the model layers and sub layers. The applicability of the model was tested and the Dubai e-government authority was taken as a case study to validate the model and its layers.

The research contributes to the theoretical knowledge of the information security modelling concept in four ways. First the literature review of existing security model and their coverage of security aspects. Second, the analysis of the security threats related to the e-services. Third, the construction of a new security model based on the academic research on each layer. Fourth, the applicability of the model was in the validated case study selected.

Candidate biography

The author holds a Bachelor degree from Washington State University in Computer Engineering from the school of Electrical Engineering and Computer Science. During his academic study in Washington State the author has enrolled in Master and PhD level of classes in the digital microelectronics and semiconductors devices physics. The author was showing a strong interest in the field of security since his studies for the Bachelor degree in 1992. He got exposed to virus programming, UNIX and Linux security and early staging hacking techniques. He continued his research in the security field by following up Fred Cohen research on computer viruses. During his industrial experience, the industrial research in the security field was continued, reading many books and articles, and participating in many security conferences such as RSA, NetSec, Networkers, Metsec, etc. The contribution in the field of security was in enhancing the security systems and building security architectures for the military and Etisalat (A telecom service provider in UAE). In 2000, the author was appointed as senior manager of security for Dubai Internet City a new initiative which was announced in the country as a technology cluster. The author's career evolved to the Chief Operating Officer for a newly established business unit called Datafort offering security services to customers within and outside of the DIC free zone. In 2001, the highly-prized CISSP (Certified Information Security Systems Practitioner) professional certification was gained. In the year of 2002 he pursued his Executive MBA (EMBA) at the American University of Sharjah. During the programme the author focused on the E-commerce strategies and how security can contribute the spread of the Internet and e-commerce in the region. In 2005, the author was appointed as the CIO of Dubai Holding handling the IT and the security strategy for the largest conglomerate in the region.

The author's objective is to make the PhD degree as his beginning to contribute in the academic field of information security by continuing developing mathematical models for the information security, new programmes, architectures, and concepts which might come as part of his future publications. Currently, the author is co-authoring a book with

Professor Zeinab Shalhoub for the cybercrimes in the Middle East and their effect on the spread of the e-commerce and e-business in the region.

Acknowledgment

Pursing a PhD was always a dream of my parents and a long term challenge for me. This dream would have not been achieved without the support and the kind assistance of my advisor and friend Dr. Fan who noticed my passion of the information security field through my eyes and took my hands to step forward towards this dream. My gratitude goes to him and for his guidance, support, and continuous follow ups until I reached this point. I would like also to thank another man who stood by me, believed on my capabilities, and always acted as a great leader for me, a brother, and a mentor, Ahmad Bin Byat who I consider a school in leadership and a man of long term view and vision.

I would like also to thank a person who asked me not to mention her name but I wanted to at least thank her for the great support, her assistance in the analysis part, and her continuous motivation for me. Respect and nobility are her traits and her name shall be secret but can be revealed from her traits if the art of cryptography is applied. To her I owe a lot of respect.

My special thanks to Hossam Kaddoura who assisted me to edit and format this document and chased me to complete the final version on time. I also would like to thank those who participated in filling the survey and spared a valuable time to assist me getting the data collection phase completed.

To all the people who have lived with me over this tough era of my life and endured my frustration and struggle of this long journey, I owe you my respect and my love.

Finally my sincere thanks go my parents who supported me and showed me their love and their great empathy. Without their understanding, this dream would have not been achieved, family, the staff of the CIO office in Dubai Holding and those who stood by me during this tough journey.

Table of Contents:

List of figures

List of tables

Glossary of terms

Term	Definition
e-government	Refers to the use of Information and Communication Technology (ICT) to change the structures and processes of government organisations (Beynon, D. P., 2005).
e-services	An online service which has its processes automated and can be accessed through the web
e-government Authority	A government body responsible for the e-government initiative, projects, and services. The authority is also responsible for the coordination between the other government departments in order to create a synergy and strong alignment
DEG	Dubai E-government Authority
GITEX	Gulf IT Exhibition
Multilevel Secure (MLS)	"A class of system that has system resources (particularly stored information) at more than one security level and that permits concurrent access by users who differ in security clearance and need to know, but is able to prevent each user from accessing resources for which the user lacks authorization" (Stallings, W. and Brown, L., 2008)
COBIT	Control Objectives for Information Technology
ICDL	International Computer Driving License
CISSP	Certified Information Security System Professional
NRL Pump	Naval Research Laboratory Pump
CWM	Clark and Wilson

Chapter one: Introduction

1.1 Introduction:

Dubai has been marked in the past decade as the fastest growing city in the knowledge economy in the Middle East. The government of Dubai plays a major role in the economic development in the United Arab Emirates and was the first to launch the e-government in the country and encourage its citizens to use the government e-services in order to enhance the efficiency and the standards of life in the city. The city of Dubai was transformed to be a modern city providing state of the art city infrastructure, buildings, and all the necessary facilities which assist the government to embrace knowledge workers as part of the strategic objectives. The e-government initiative was an embodiment of the strategic goals and objectives which gave Dubai a head start and valuable experience. This chapter aims to give the reader a background on Dubai and provide chronological facts of the launch of the e-government. It also addresses the research challenge being conducted in a real world scenario. The research objectives, processes, data collection tools, and the structure of the document are addressed through the following sections of this chapter.

1.2 Dubai e-government development

"The land of globalization and modern life in the Middle East", a description that you will hear a lot from many well known public speakers and business leaders describing Dubai as a fast growing and a role model city in the region. Dubai as one of the seven emirates "States" of United Arab Emirates has become a brand of quality, modernization, and high standards of life in the region. "Dubai has achieved a lot in the past 40 years or so. Its location has helped and the emirate is ideally located to serve the growing markets in the Middle East, India, Pakistan, Iran and East Africa", (Sampler, J. and Eigner, S., 2003)**.** The growth of the GDP of the city is strong economic evidence reflecting the success of the city which has been achieved through the past decade. As illustrated in **Table 1** the staging development of the GDP from 1996 to 2005 (from 7.0 to 13.4) is considered phenomenal as the growth in the non-oil GDP continued to rise from 10.9 in 1996 to 15.1 in 2005.

Table 1: The GDP growth of Dubai

	1996	1997*	1998*	1999*	2000*	2005**
GDP	7.0	5.5	5.3	8.2	7.5	13.4
Non-Oil GDP	10.9	12.1	5.3	9.2	8.9	15.1

*: Adjusted

-: Preliminary

** Source: www.dubai.ae)

(From: Sampler, J. and Eigner, S., 2003)

In 1990s, many governments have launched electronic government projects with a common objective; providing electronic information and services to citizens and businesses (Torres, L., Pina, V. and Acerete, B., 2005). Based on the foresight of the Dubai government for the need of having world class services and efficient life style for its citizens, the Dubai e-government initiative was announced in 2000. It was the start of a new era of virtual government in the country and the region (Sampler, J. and Eigner, S., 2003). "The notion of Government has to be re-invented if we want Dubai to become a leading business hub in the new economy", H.H Shaikh Mohamed Bin Rashid.

The objectives of the initiative were set from the beginning by the leadership of Dubai; the vision was clear from day one. Dubai e-government (DEG) authority's mission was to achieve a digital or virtual government through the provisioning of e-services to the citizens and visitors of Dubai. This shall simplify the process of government citizen interaction and enhance the efficiency of the government departments.

Looking back to the year of 2000, many visionary leaders of government departments had doubt about the success of this new initiative. It was a key transformational point for the government of Dubai. The target of completing the launch of the government portal in 18 months was considered aggressive but Dubai was always known as achieving things rapidly, racing the time, and performing the quantum leaps while managing the change effectively. In 2002, the Dubai leader has announced the launch of the e-government portal and the success of completing the project within the planned dead line. Dubai has given a

strong example to other cities in the gulf and the region and achieving strategic objectives with speed and accuracy has become the known trait and brand of Dubai.

Dubai e-government (DEG) authority kept encouraging other government departments to participate in the e-government initiative and to automate the government processes and make them publicly accessible by the citizens as e-services. In 2003 and during one of the most prestigious IT exhibition in the region known as "GITEX", DEG authority was able to encourage 21 government departments to exhibit their e-services to all visitors and government delegates. Dubai government departments were able to demonstrate different e-services offered through the unified government portal (www.dubai.ae). The DEG authority continued to sell the concept of e-government to other government departments and assist them in the launch of their first e-service. In the following year, 26 government departments participated in GITEX demonstrating new e-services and training citizens on how to use them. The immediate participations of the large government departments in Dubai was an evidence that the e-government initiative has received good support from the government departments which continued in competing for the launch of new, effective, and market demanded e-services to the public and private sectors. The 26 government departments are illustrated in **Table 2**.

Table 2: Government departments offering e-Services

1	Dubai Police	10	Al-Awqaf Department	19	Dubai Municipality
2	Dubai Development Board	11	Dubai Naturalization and Residency Department	20	e-TQM College
3	Land Department	12	Dubai Transport	21	Dubai Real Estate Department
4	Dubai Civil Aviation	13	Dubai Chamber of Commerce and Industry	22	Ministry of Labour
5	Department of Economic Development	14	Tanmia	23	Dubai Civil Defence
6	Dubai Justice Department	15	Dubai Government Workshop	24	Department of Health and Medical Services (DOHMS)
7	Department of Tourism and Commerce Marketing (DTCM)	16	Dubai Electricity and Water Authority (DEWA)	25	Department of Information
8	Jebel Ali Free Zone Authority	17	Dubai Ports and Customs Free Zone Corporation	26	Dubai Airport and Free Zone Authority
9	Dubai Quality Group	18	Mohamed Bin Rashid Al Maktoum Charitable and Humanitarian Foundation		

The DEG authority acted as an active member of the e-government initiative and launched some key e-services which can be accessed by citizens and other government departments. DEG authority called these services as synergetic e-services. The portfolio of the synergetic e-services was including ePay, AskDubai, mDubai, eJob, eEmployee, eLearn and eLibrary e-services. The ePay e-service allows registered users to pay for public services through eDirham card or credit cards. It is widely used and considered the key transactional e-service for all the government departments. The author believes that ePay is the spine of the government e-services due to its integration with many government e-services offered by different departments. As a facility, the DEG authority has provided the government departments an e-service called mDubai which will enable them to send short text messages to all the residents of Dubai through the residents database stored in DEG authority's IT infrastructure. mDubai is considered one of the push e-services used as a strong tool for propagating mass information in the city.

The eEmployee service is developed based on the concept of the European Computer Driving License Foundation, a recognized standard for computer literacy in over 120 countries and is endorsed by UNESCO for all Arabic speaking countries. eEmployee is a double certification programme that combines ICDL-Start certification with three additional courses of instruction selected by e-government to meet the specific needs of Dubai Government. This e-service contributes in building of the computer knowledge in the government sector. The contribution of the DEG authority in developing knowledge workers was reflected in the launch of the eLearn service, a service which provides online training services to departments, residents and businesses.

The launching of different e-services was not bound to any restriction as long as it serves the objective of the e-government initiative. The DEG authority has also launched a limited interactive service through the call centre entitled as "ASK Dubai".

It was observed by the author that the interactive e-services of DEG and its affiliates are not real time processes. They are mainly as one way interaction and the rest of the processes are performed in the backend offices of the government departments. Due to this

disconnection between the interfaced processes by the citizen and the rest of the processes, a long time of verification and customer notification is added which has a negative implication on the citizens' satisfaction and usability. This challenge has been recognized by the DEG authority and it confirmed the main reason of this challenge is due to the lack of backend offices integration and the lack of a seamless mechanism which allows information sharing between the government departments. The DEG authority has embarked a new project for the government enterprise architecture in alignment of a new strategic objective towards the transformation to "i-government".

1.3 The new research challenge

Currently most of the e-services are accessed through different government department portals and not through the official e-government portal known as dubai.ae. The government portal acts as a catalogue of the government e-services and directs the citizens to the respective government portal once the e-service is selected. A citizen of Dubai will have to access multiple portals to complete a cycle of a single e-service. The DEG authority is striving to achieve the goal of integration. The reluctance of integration by all the government departments has contributing factors including the fear of security failures.

In this thesis document a new security model is developed for the e-government authority and its affiliated government departments. It is meant to be used as a reference and a standard for assessing the level of security in each department and as an assurance of government department's good security level.

The new security model will also assist in ascertaining the current level of security of each department, giving the confidence to other departments and serve as a mitigation action of the risks that may exist in the future.

1.4 Research objective

This research focuses on building a new security model for the e-government of Dubai. Initially the aim of the research was to build an information security model for any e-organisation and was then narrowed to address e-government security.

The objectives of the research were as follows:

1. Establish the security requirements for Dubai e-government.
2. Collate state of the art approaches and methods for the e-government security.
3. Develop model for evaluating the security level for inter-government information sharing.
4. Test the model in the Dubai e-government context

The research questions assist in understanding the scope of work for this research. There are two main research questions:

1. What are the security concerns and requirements for Dubai e-government?
2. What are the existing models addressing the different needs of the information security and why would a new model be evolved from there?

1.5 Research process/methodology

The author of this thesis selected a research methodology mixing the quantitative and qualitative methods as explained by Creswell (Creswell, J. W., 2003). The questionnaires designed for collecting data had open-and-closed ended questions to obtain both quantitative and qualitative data for the analysis.

An extensive literature review of existing security models was carried out. Information security models addressing information flow and sharing, e-commerce security, Internet optimization, e-government services security, human behavioural effect on cybercrimes, networking security rating and other aspects of security, were studied and analyzed. The reviewed models contributed to the information security field by addressing one or two aspects of security. The structure of these models varied from mathematical structure, to pure graphical representations. The review of strength and weaknesses of these models assisted in building the conceptual design of the new model based. **Figure 1** illustrates how

the process of review of the existing models led to conceptualizing the new model. This shall be further described in chapter 4.

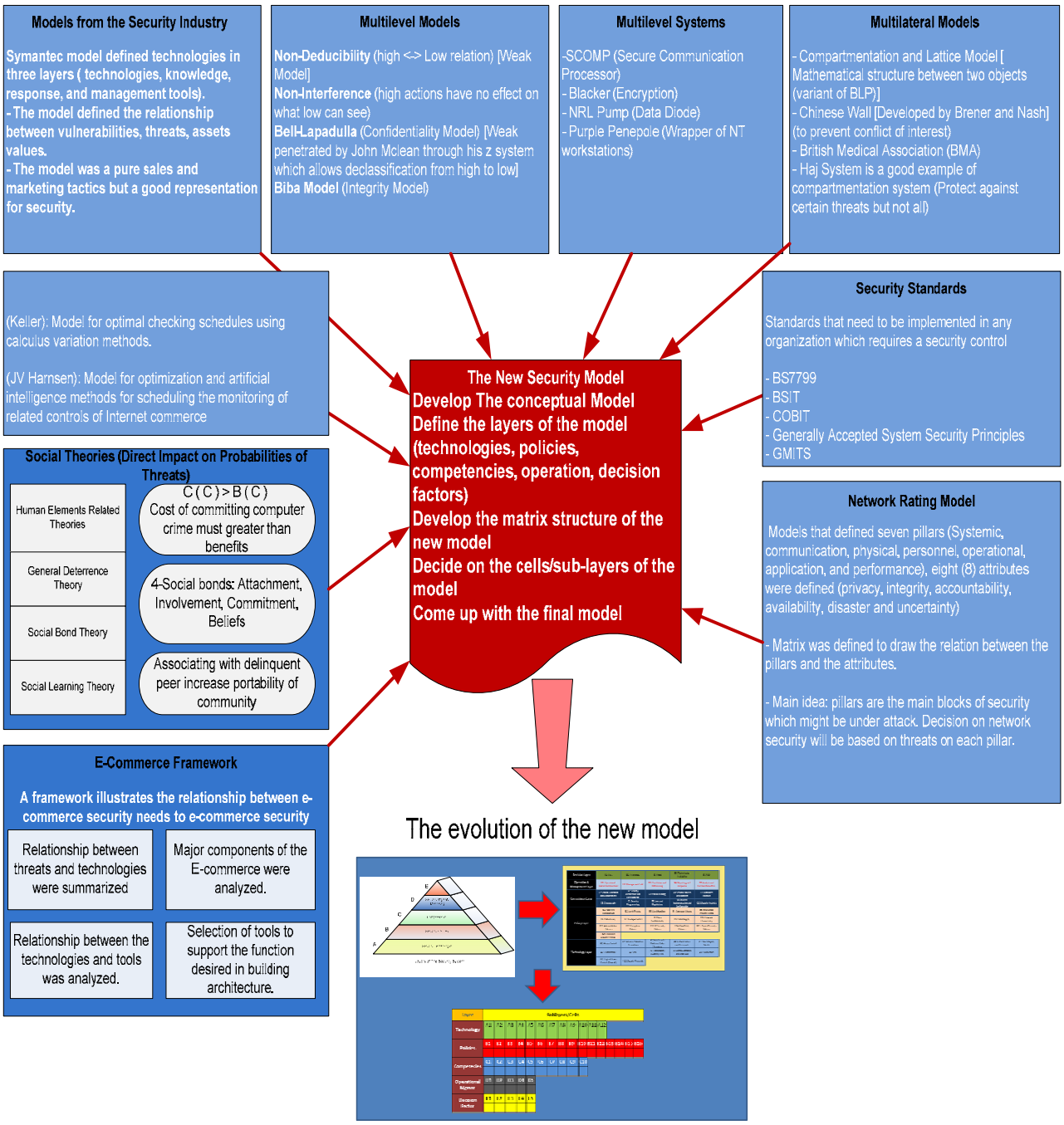


Figure 1: Different models leading to new one

The data collection tools

Two questionnaires were developed for data collection. The first **questionnaire (A)** targeted the government department leaders and executives who have the authority in their government departments. The objective of the questionnaire was to identify the type of services offered through each department; the security programmes implemented addressing the internal/ external threats on the e-services.

The second questionnaire (questionnaire (B)) targeted the information security practitioners in the e-government authority and the government departments. In addition it was sent to other information security practitioners who are known as strong references in the information security field in Dubai. The key objectives of questionnaire B were to identify internal/external threats and to build the counter threats model for the governmental departments. In addition it was to confirm the need of each layer and sub-layers of the new model.

The following diagram illustrates **(Figure 2)** the objectives of each questionnaire and how both sets of objectives lead to the achievement of the final objectives. The refined model was then validated with the relevant authorities in Dubai.

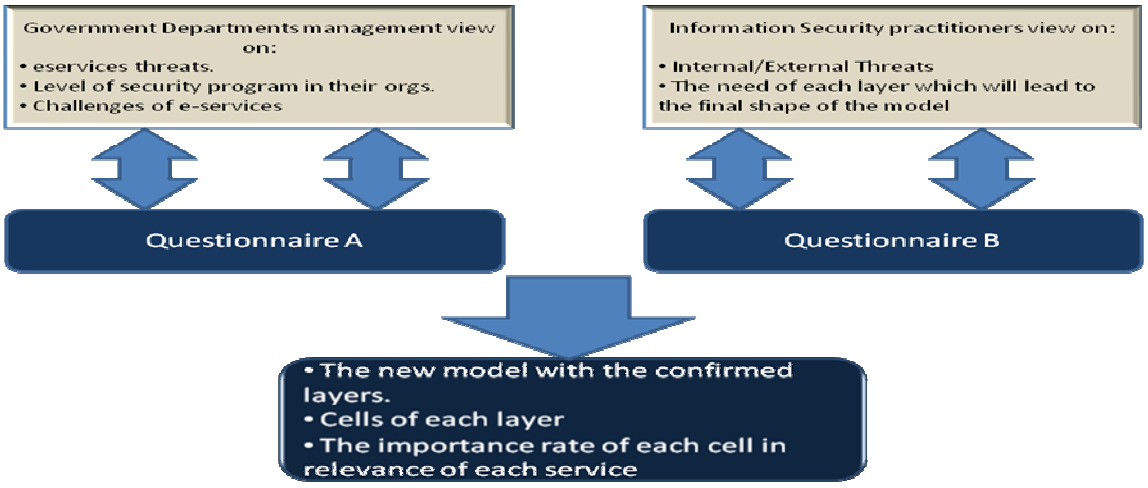


Figure 2: The questionnaires objectives

1.6 Contribution to knowledge

The model is an advance on existing models in its comprehensive nature to address the variety of threats to information security. It has an adaptable structure that can be extended as new threats emerge. In addition, the model is easy to understand and used by non-technical people with management responsibility for the e-government security.

The new model presented in this thesis provides the e-government authority and its affiliates a structured methodology to assess the security level in the government departments, a checklist of all the security elements required to build a robust security programme and architecture, and a mean to align the different views on the needed security levels for transparent information sharing. It can also be evolved to be an international framework for the government security architecture and a standard used by e-government authorities worldwide. The new model addresses some of the main domains of ISO17799 by addressing policies and operational management, and the people capability maturity matrix (PCMM) through addressing the competency layer.

The new model developed through the research work of this thesis has four strong characteristics:

- **It can be used for multiple purposes:** The new model can be referred as a comprehensive security architecture which addresses more than the technological aspect. It can also be used as a checklist for what's implemented and what's in the future plan and can easily be turned into a measurement tool for the security level of the government department. Finally, it can be used as a strong awareness tool for government executives to give them a holistic view of all the security aspects required in their organization.
- **The model is flexible and not biased** to any technology, policy or any other security aspects: The sub layers presented in the model are academically researched independent from any industry or brand bias.

- **The new model is independent of any theory, threats, sector or architecture** and it can be placed as part of any Enterprise architecture for any government department.
- **Complement the previous models:** The new model developed addresses aspects complementing other models such as the competency aspect which was not addressed by the other models researched, the decision aspect which was missed out from most of the security models in the field of information security and the link between all the five layers which gives any security model a strength to stand as an independent security programme.

1.7 Thesis document structure

Chapter 1: Introduction

In chapter 1, an introduction of Dubai government and city was given in order to provide the reader a good background of Dubai the area of the case study of this research. The chapter addresses the DEG authority initiative, and the type of services the e-government is offering.

Chapter 2: Literature review

This chapter has two main parts which provide a holistic view for the reader on the threats affecting the online services, and how to come up with a model addressing all of them. The first part is an introduction on the evolution of the e-world and how the e-governments were evolved subsequently. It briefly addresses the DEG authority goals and challenges. The second part of this chapter explains the models and theories the author came across during the literature review phase of this research study. This section gives the reader a good background of the well known security models and theories. It also highlights the weaknesses of each model.

Chapter 3: A structured research methodology

A background on the research methodologies, knowledge claims, research strategies, and data collection was given as the first part of this chapter. The implemented research process and methodology for this research study was explained subsequently. The last part of this

chapter addressed the validation process and the objectives achieved through the research study.

Chapter 4: The five security layered model using matrix representation

In the first part of this chapter, the author introduces the conceptual model using a pyramid shape representation. The objective is to establish the layers needed in the model. The model evolved to a matrix structure to represent all the layers and sub layers. The main part of this chapter is the justification of each layer of the new model and establish how they can contribute to security evaluation. Each layer and its sub layers were referenced to literature reflecting other researchers' opinions on their importance and criticalities. The final structure of the model is presented in the last part of this chapter including all the sub layers.

Chapter 5: Case study of Dubai e-government security requirements

Dubai e-government was taken as a case study; a survey was developed for the management of Dubai government in order to collect the different views of the security needs, online threats and challenges from management perspective. The first part of the chapter addresses the purpose of the research, target interviewees, format of the questionnaire and the method of data collection. The pilot questionnaire and benefit of this process are highlighted. In the last part of Chapter 5, the analysis of questionnaire results is presented.

Chapter 6: Dubai e-government security model survey analysis

Another questionnaire was developed in order to collect the views of the top information security practitioners in Dubai who directly or indirectly contributing to government e-services. The questionnaire structure, design, and objectives were explained in this chapter. A pilot questionnaire was also carried out to collect the feedback and depict the areas of weaknesses in order to enhance prior to the final questionnaire deployment. The highlight analysis of the questionnaire results was reported in this chapter reflecting the correlation between the different layers of sub layers in the new model.

Chapter 7: Validation analysis

The validation mechanism is explained. Input from key authority in Dubai e-government was used to confirm the validity of the model.

Chapter 8: Discussion, future research work and conclusion

This chapter provides a summary of the results and the achievement of the research study. It also compares the questionnaires results with the developed model and how the new model presented in this thesis document contributes to the knowledge in the security field. As a conclusion of this chapter, the author indicates how the presented research study can evolve to a further research. The author concludes with addressing the limitation of the research study conducted in this thesis.

Appendices

- **Appendix A:** The management questionnaire-Questionnaire A
- **Appendix B:** The IT security practitioners questionnaire-Questionnaire B
- **Appendix C:** Feedback Form for both questionnaire A & B
- **Appendix D:** Validation Forms and confirmation emails from e-government authority and government departments.

Chapter two: Literature review

2.1 Overview

Information Security is:

1. The process of identifying events that have the potential to cause harm (or threat scenarios) and implementing safeguards to reduce or eliminate this potential.

2. The safeguard, or countermeasures, created and maintained by the security process (Schechter, S., 2004).

Securing information can be referred back to the ancient civilizations when many civilizations started to adopt models of secrecy to communicate freely without the risk of eavesdropping. The Egyptians started using cryptography in 3000 BC applying Hieroglyphics (Schneier, B,. 1996) to conceal writings from unintended recipients. The science of Hieroglyphics was born in the Greek civilization and the word Hieroglyphic meant sacred carvings. In 400 BC, Spartan military used cryptography in the firm of papyrus or parchment wrapped around a wooden rod. This was known as 'Scytale' (Schneier, B,. 1996). The evolution of developing new security methods to secure valuable information to nations, armies, individuals, and organisations continued afterward. Some were based on pure cryptographic knowledge while others based on policies, rules, and mathematical foundations. In the early 1970's a new model was developed known as Bell and Lapadula model (Bell, D. and Lapadula, L., 1973). The model objective was to ensure the confidentiality of the information based on a military-style classification in the early 1970's. The model was widely accepted and found to be practical. In 1985 McLean (Mclean, J., 1990) raised an argument about the security of the Bell- LaPadula model and the strength of the basic security theorem in proving a secure system or not. McLean's research introduced a new area of the security field addressing a threat of the covert channel which allows a bypass of the security rules. In 1977 another model was developed addressing the integrity of the system known as the Biba model (Bishop, M., Cheung, S. and Wee, C., 1997). A combining model of both BLP and Biba was developed by Lipner

in 1982 (Lipner, S., 1982). The development of new models continued and in 1987 a model addressing the integrity challenge was developed by Clark and Wilson (CWM) (Bishop, M., Cheung, S. and Wee, C., 1997). CWM imposes integrity controls on data and its transactions. It also sets two types of rules; certification rules which are group of restrictions on the integrity verification procedures (IVPs) and the transformation procedures (TP) (Clark, D. D. and Wilson, D. R., 1987). Issues such as conflict of interest led to the development of new models based on security policies such as the Chinese wall model (Brewer, D. F. C. and Nash, M. J., 1989) which was derived from the British laws addressing the conflict of interest. As the number of models increased, challenges continued to increase and researchers continued to search for different solutions through new models or enhancements of existing ones. The foundations of the models were different. Security models were developed following different research strategies. Some were qualitative while others were based on quantitative approach. A good model reflecting the quantitative approach is the scheduler model. The model was built to measure and improve the security of an existing application within a computer (Schechter, S., 2004).

The objectives of some models were developed to protect computer system such as the "Multilevel Model" (Thuraisingham, B., 1995) while others were developed to provide security across boundaries of multiple organisations such as "Multilateral Model" (Sadeqhi, A. R. and Stuble, C., 2005).

The spread of the Internet and the evolution of the e-world and e-government have increased the power and value of the information for the government organisations. Information security science has evolved to be the main factor and the supporting element of the Internet spread. This chapter provides a detailed overview on the e-government evolution as part of the "e" world evolution, literature review and the classification process of threats on the e-services launched by the e-government. The structure of the chapter is as follows:

The first part discusses the evolution of the e-world and its impact in the Middle East. The change in culture and life style is addressed briefly. The second part covers the literature reviews conducted for models and theories tackling the confidentiality, integrity, and availability of the information and how threats are handled through these models.

2.2 From the e-world to the e-government

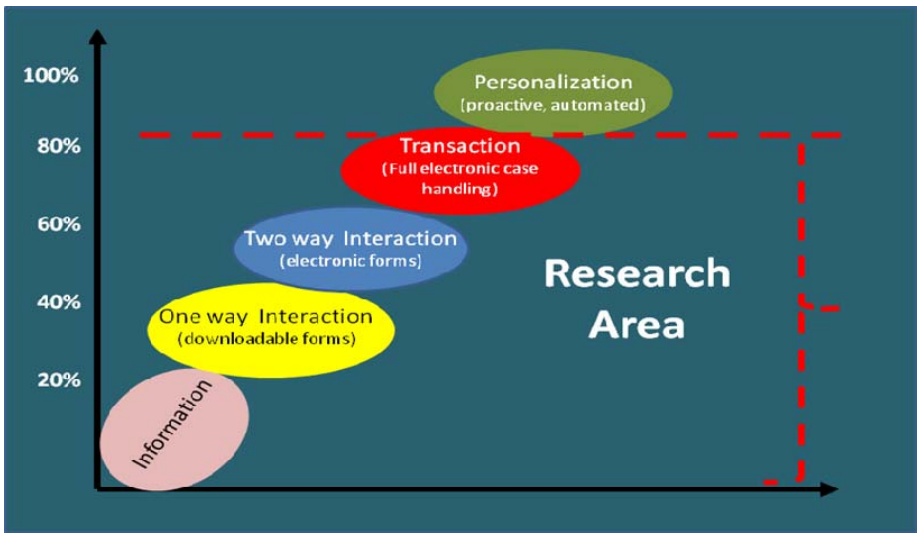
The growth of the virtual world is inevitable. The concepts of virtualization and globalization go hand to hand and the level of acceptance for such new culture is increasingly noticeable. The paradigm shift is driven by enterprises, entrepreneurs, visionaries, professors, customers, and even legislators and governments. The virtual world is the world of no boundaries where governments and business leaders would like to invest on. There is no doubt in our minds that our world has changed dramatically in the past decade. The new e-world represented by the letter "e" is not only impacting the definitions of some of the words which we are used to in our daily life and the technology arena, but the style of life, culture, social bonds, and methods of communications. Relyea mentioned that the term of 'e-government' was introduced by a joint report of the National Performance Review and the Government Information Technology Services Board in 1997 (Relyea, H.C., 2002) entitled as "Access America: Reengineering through Information Technology". Information Technology leaders and security practitioners were always emphasising about e-commerce, e-business, and e-governments. Today, we do have more e's than we ever expected. Every conventional society element can have an "e" format of it. The e-learning, e-library, e-auctions, e-markets, and e-entertainment for instance represent conventional services but in the most automated and efficient way which made governments and leaders encourage the launch of more e-services. The shift in the mindsets in modern societies is becoming a rolling snow ball accelerating at a faster speed and growing with its mass and value.

The adoption of the e-model was performed by many organisations, governments, and educational institutions selected different aspects of it. The transactions of commerce

evolved to e-commerce, governments' services to e-governments e-services, business to e-business and many others.

The evolution of the e-government started in the 1990's world wide aimed at providing online services 24 by 7 to the public (Benabdallah, S., Fatmi, G. E. and Ourdiga, N. B., 2002). The initial services were all related to information publishing. The development in the e-government services continued to be categorized into three based on the purpose of the services and the perception of the end users as most literature state (Anonymous, B., Mark., Locher, L. J. and Doyle, C., 1998).

The idea behind the establishment of an e-government is to provide public services to the public and private sector through a single point of access known as the e-government portal (Lambrou, M. A., 2003). According to Glassey (Glassey, O., 2004) the e-government services are categorized as informational, communicational, and transactional services.
The e-government online services vary from providing simple information to full cycles of complex online services involving financial transactions **(Figure 3)**.



(Wauthers, P., Nijskens, M. and Tiebout, J., 2007)

Figure 3: E-services Maturity Level

Narrowing down the discussion from the world to the Middle East, the e-model has received a wide acceptance by many governments in the Middle East where dramatic change in the concept of the electronic world, digitization, and e-services has been noticed. In 1990's the culture of having knowledge workers with their laptops in coffee shops, malls and public places did not exist. The lack of ubiquitous connectivity was an obstacle for those who wanted to work from home, or public places. Nowadays and with the wide spread of the Internet, working in public areas or from home is possible in Dubai and many cities in the region. The high demand of the knowledge workers for the Internet connectivity in Dubai has driven the service providers to respond fast and provide Internet connectivity (wired and wireless) everywhere in the society. It also encouraged the government to provide e-services in order to reduce the travel needs of the citizens and enhance efficiencies. The physical interaction with the governmental departments in order to complete a simple process is no longer accepted by the knowledge workers which pushed governments to find an alternative to offer their services to the public. Dubai e-government was the first to launch its government services over its portal and the number of services continued to increase to reach around 600 services (Geray, O., Feb 2007).

2.2.1 E-government security challenges

The spread of the e-services raised another challenge for governments in the Middle East. The government information will need a strong protection programme in order to avoid any breach which might jeopardize the government operation or disclose the citizens' private data. In Dubai the trust relationship between the e-government authority and the other governmental departments is all based on how confident the government departments would feel toward the security programme applied in the e-government infrastructure, the telecom service providers, and the other government departments. One of the main factors to increase the confidence and the trust relationship is to have a high level of security awareness. Being well informed about the security policies, architectures, competencies supporting the security functions and the operational procedures in the government departments will assist in raising the level of confidence and trust. The challenge of achieving the security awareness has been there for a while and since the inception of the e-

government programme. Government departments took the responsibility of protecting their e-services but the security programmes implemented in each government department is different and varies from network security to application security levels. Their objectives were to encourage the public to use the government e-services offered through their individual portals or the common portal gateway. These services might be provided directly from the e-government authority or any of its affiliated government departments. “The milieu of citizens, agencies, and commercial corporations around the e-government authority shall raise the security concerns around inter and intra communication” (Conklin, A. and White, G., B., 2006), Many researchers presented different models to address the security concerns of the e-government and to measure confidentiality, integrity, and availability known as the C.I.A triad. “Security issues are conceived to comfort the public in using e-government services and government administration and agencies to access, share and exchange information security”, (Benabdullah, S., Fatmi, G. E. and Ourdiga, N. B., 2002).

Information sharing was always considered a concern but need to exist between the governments departments. The requirement of having information sharing between government departments in order to complete an e-service process, for example, sharing the citizen profile, or authenticating an applicant, started to be stronger with the need of having single citizen profile and strong integration in the backend system. Despite the strong need of information sharing and the intensive communication between the government authority and its affiliates, the flow of information between different government departments always raises security concerns (Conklin, A. and White, G., B,. 2006). It is an inevitable challenge for the e-government and need to be addressed through the adoption of a security model or a change in the method of information sharing.

Moreover, the type of information to be exchanged and the purpose of the information use determine the level of risk the government will need to consider. According to Conklin (Conklin, A. and White, G., B., 2006) the level of information sharing between the police department and the water department is different than the police department and the public.

The change of information classification is a threat that needs to be addressed by the e-government authority. The process of information sharing is not performed through technology only. The operational procedures, human, policies and decision factors can have positive or negative impact on the process.

2.2.2 The threats impact on the e-government services

Similar to the e-business model, the government e-services depend on the reliability of the technological infrastructure and its security, the integrated processes and their security checks, and the integrity and competency of the supporting staff. The e-government uses ICT to make the interaction with citizens and businesses easier and seamless with the government. The threats of lacking any of the key elements required to run or launch an e-service shall always be a concern for the e-government. The government e-services have a larger population of users in comparison to e-business e-services which have specific users. The users of government e-services users are the citizens who are the people who live in the country, business corporations, visitors or tourists. Having a larger population will always increase the probability of having malicious attack on the online service.

The lack of public confidence caused by the threats on the e-services will be noticed by the low level of use of any e-service offered by the e-government or any of its affiliates. The electronic governance of the e-services is a worldwide topic where many researches were conducted to address how possibly it can be supported. As mentioned by Mitra, “the serious needs of ensuring security on the website vis-à-vis protection of privacy and the prevention of abuse are overwhelming concerns that persuade the use of such models” (Mitra, A., 2005). It is a clear indication that the need of security has a direct link to the use rate of the e-service. The increase number of threats on authentication, authorization, confidentiality, and non-repudiation of any e-government e-service has negative impact on the proliferation of such service or any associated services (Turban, E., King, D., Lee, J., Warkentin, M. and Chung, M. H., 2001).

2.2.2.1 An overview on Dubai e-government (DEG) authority

"Dubai as a leading business hub in the new economy has launched various initiatives to adopt a knowledge economy and to utilize information and communication technology (ICT) as a key enabler" (Geray, O., Feb 2007). Prior to the launch of the DEG authority, the government of Dubai provided its public services through the traditional and conventional means which required a direct physical interaction with the citizens/public. A repetitive number of physical interactions with government departments were sometimes needed for one process causing the applicants loss of time and great level of frustration. This indeed pushed the government of Dubai to find an alternative through the e-government concept and established the DEG authority to be responsible for the coordination and collaboration between the government departments in the e-government initiative. The objective was to put "e" in front of every government service and digitize the manual processes in order to transform its internal and external relationship with the use of modern information and communication technology (ICT) (Bertucci, G., 2005). The new era of e-government is a paradigm shift in Dubai allowing businesses and individuals to apply for government services through a common governmental portal. The government, business and individuals (citizens & residents) are the pillars of Dubai's economy. Having a strong interaction between these pillars is imperative and will be the key of Dubai strong economy (Bertucci, G., 2005).

Through the first phase of analysis the DEG authority has identified around 2240 public services. The services are provided by the 26 government departments in Dubai government. Today only 75.8% of the public services (1700) are provided electronically. The maturity of these services varies from information publishing to full transactional services. DEG has invested a lot to enhance the quality of the websites and the electronic services. An annual assessment is performed on the quality and a rate of 62% was given on the websites quality.

Although most of the e-services are coming from government departments, DEG has proactively launched some e-services to the citizens and the government departments. There is a significant increase in the usability of the common e-services launched by DEG. For instance, calls routed through the DEG authority contact centre for AskDubai service increased 23% in 2006 reaching more than 166000 calls. More than 3.1 million text messages were sent through DEG's mDubai unified mobile services.

2.2.3 DEG authority strategy goals

- To simplify and streamline government services by utilizing technology as a key enabler.
- To achieve a customer centric approach for government services provision by increasing effectiveness and efficiency.
- To come up new government services and join-up existing government services by exploiting new potentials arising from Dubai e-government (DEG) authority.
- To modernize and standardize internal government processes regarding procurement, finance and human resources (Bertucci, G., 2005).

The following table **(Table 3)** illustrates the affiliated departments with the DEG authority and the percentage of the e-services launched within the department:

Table 3: E-services launched by DEG authority (2006) (Geray, O., Feb 2007),

NO	Department Name	% of e-Services Launched
1	Awqaf and Minor Affairs Foundation	100
2	Department of Health and Medical Services	75
3	Department of Tourism and Commerce Marketing	81
4	Dubai Airport Free Zone Authority	100
5	Dubai Chamber of Commerce and Industry	100
6	Dubai Civil Aviation	98
7	Dubai Civil Defence	100
8	Dubai Courts	23
9	Dubai Customs	75
10	Dubai Development Board	100
11	Department of Economic Development	100
12	Dubai Electricity and Water Authority	99
13	Dubai Government Workshop	60
14	Dubai Land	100
15	Dubai Media Corporation	100
16	Dubai Municipality	100
17	Dubai Police	79
18	Dubai Public Prosecution	100
19	Roads and Transport Authority	100
20	Dubai Transport Authority	100
21	Islamic Affairs and Charitable Activities Department	66
22	Naturalization and Residency Admin	47
23	Real Estate Department	88

An analysis was conducted on the government department e-services and their types based on the UN categorization as part of DEG 2006 Strategic Progress Review Report (Dubai e-government Authority). The results are illustrated in **Table 4:**

Table 4: Dubai government departments e-services (Geray, O., Feb 2007),

No	Department	Informational		Interactive		Transactional	
		Total Services	e-enabled services	Total Services	e-enabled services	Total Services	e-enabled services
1	Awqaf and Minor Affairs Foundation	0	0	0	0	30	30
2	Department of Health and Medical Services	11	11	14	13	56	37
3	Department of Tourism and Commerce marketing	2	0	3	3	11	0
4	Dubai Airport Free Zone Authority	2	2	2	2	184	184
5	Dubai Chamber of Commerce and Industry	5	5	9	9	0	0
6	Dubai Civil Aviation	0	0	2	0	119	116
7	Dubai civil Defence	2	0	4	0	27	27
8	Dubai Courts	9	0	53	52	375	49
9	Dubai Customs	0	0	11	11	65	45
10	Dubai Development Board	6	6	19	19	0	0
11	Department of Economic Development	17	17	17	17	106	106
12	Dubai Electricity & Water Authority	32	31	23	22	48	47
13	Dubai Government Workshop	0	0	6	6	4	0
14	Dubai Land	16	16	3	2	4	4
15	Dubai Media Corporation	1	0	0	0	6	4
16	Dubai Municipality	70	70	13	13	417	417
17	Dubai Police	17	16	2	2	56	41
18	Dubai Public Prosecution	1	1	7	7	104	104
19	Roads & Transport Authority	4	2	8	8	26	15

20	Dubai Transport	2	2	0	0	11	11
21	Islamic Affairs & Charitable Activities Department	19	14	9	4	4	3
22	Naturalization & Residency Administration	0	0	0	0	150	71
23	Real Estate Department	1	1	1	0	14	13

There is a difference between Table 3 and Table 4 as some new departments were added while some also were merged or dissolved. Dubai continues to revamp its government structure and strive to make the government structure more efficient to serve the public. The government departments restructure shall not affect the number of e-services unless the business processes supporting the e-services get changed or reengineered.

It was found from the statistical analysis that 83% of the government services were identified as transactional services, 7% were identified as interactive services and 10% were identified as informational services. Although transactional services were well enabled in many government departments, the low percentage of interactive services raises concern about the value chain and the processes of the transactional services.

2.2.4 The lack of information sharing in DEG authority

There is no doubt that automating government functions will help to increase customer service levels and decrease costs (Evans, D. and Yen, D., 2005). The automation of the government function will require integration in order to achieve the maximum efficiency between the different government departments. Many e-governments are moving towards the new concept of i-government. A concept which simply means the integration of the backend systems of the e-government infrastructure. The integration will assist the e-government to achieve more correlation of the citizen information and have a single profile for the citizen using the e-services provided through the e-government portal. DEG authority is working on integrating the e-services and the backend systems of the various government departments in order to transform the e-government to i-government. Many challenges are encountered during the integration process of the government departments.

One of the key challenges the DEG authority is facing is the lack of common reference for a security architecture or assessment. This is a constraint for the integration of the citizens' database between the various departments of Dubai government. An extensive research was conducted on various security models which might address the need of information sharing and strengthen the trust relationship between the government departments. The following section explicitly explains the literature reviewed during the research process.

2.3 Existing information security models and theories

Many journals and literature were reviewed to analyse the existing models and theories developed to evaluate the information security level in an organisation or between group of organisations interacting with each other through information sharing or transactional services. The focus was on the models and theories researchers and scientists came up with or adopted in developing security systems, or models. Reviewing the objectives of these models was also part of the literature review process of this research.

The scope and the objective of the research were clear from the initial stage of the literature review. Journals addressing information security models, theories of systems and enterprises protection, human behavioural theories and the cybercrimes, decision factors in the information security, and security frameworks and standards were reviewed, analyzed, and categorized based on the area of the research they address. The review process focused on finding supporting arguments for the need of a new model. The strengths of the existing models were considered as good characteristics to have in the new model and the weaknesses been the supporting factors to justify the existence of some of the layers and shape the structure during the development process. Some of the journals and proceeding articles were reviewed to get strong academic support on some of the views related to e-government or organisations' information security. The criteria of selection were based on the strength of the argument the journals was presenting, the popularity of the publisher in the information security field, and the clarity of the concept to reader. The CIA triad; confidentiality, integrity, and availability, are the concepts which act as the fundamental

security objectives for data, information, and computing services (Stallings, W. and Brown, L., 2008).

2.3.1 Multilevel and multilateral models

Multilevel models were developed to protect the confidentiality and the integrity of information. These models look at the nature of information flow between entities and how security of the flow could be governed by rules. There are four models address the multilevel security:

A) Nondeducibility Model.
B) Non Interference Model.
C) Bell-Lapadula Model (Confidentiality Model)
D) Biba (Integrity Model)

2.3.1.1 Non-deducibility model

The Sutherland's non deducibility model developed in 1986. The model explicitly explains that information can flow from high-level objects to low-level objects if and only if some possible assignment of values to low-level objects in the state is inconsistent or conflicting with a possible assignment of values to the state's high level objects (McLean, J., 1990), **(Figure 4)**.

The model can be expressed mathematically as the following:

Assignments H & L → H for high level objects

→ L for low level objects

No flow of information from high (H) to low (L) unless

P(H)>0 & P(L)>0→ P(H|L)>0 (Mclean, J., 1990)

The non deducibility model has been observed with a weakness as it is considered as a model for information sharing not information flow. As per the security definition of information flow, the information must be allowed to flow from low to high level objects

bidirectional. The non-deducibility model fails this definition and therefore, it was categorized as a good model for data compartmentation rather an information sharing.

The flow of information security can be presented in the following mathematical representation using Bayes' Theorem with the condition as follow:

P(H|L)P(L)= P(L|H)P(H) condition (1)

It follows that:

P(H)>0 & P(L)>0→P(H|L)>0 if and only if P(H)>0&P(L)>0→P(L|H)>0

Knowing that P(H|L) = (P(H|L)P(H))/P(L) & P(L|H) = (P(L|H)P(L))/P(H)

Replacing P(H|L) and P(L|H) values, the author found that the above condition holds:

((P(L|H)P(H))/P(L))P(L) = ((P(H|L)(PL))/P(H))P(H) this will lead P(L|H)P(H) = P(H|L)P(L) which holding condition (1)

The mathematical expression represents the need of information flow to be bidirectional. The bidirectional concept of information flow is maintained by limiting the objects when the system is secure with non-deducibility model.

If P(H)>0 & P(L)>0→ P(H|L)>0 where H is the assignment sequence to the system's high level input port & L is an assignment sequence to system's low-level input and output.

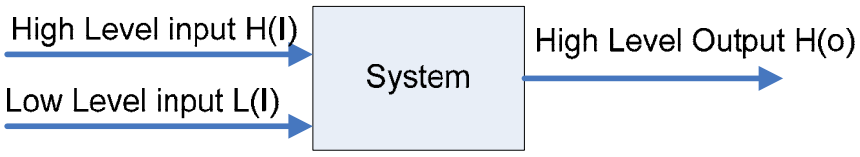


Figure 4: High and low level inputs/non deducibility

Most of system's high level output can only be generated from low level input **(Figure 5)** Researchers and analysts think that non-deducibility is weak since there is nothing to stop low making deduction about high level input with 99% certainty.

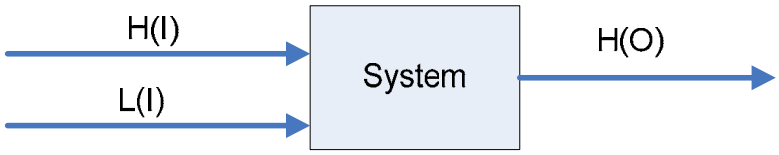


Figure 5: High level output from low level input

2.3.1.2 Non-interference model

The non-interference model was developed by Goguen and Mesguer in 1982 (Goguen, J. A. and Mesequer, J., 1982). The concept of the model is that high actions have no effect on what low can see. "A system is non-interfering if its low-level output was independent of its high-level input in the sense that for any system with output function out (U,I), whose value is the output generated by input history I to user U, out(U,I) = out(U,I*), where I* is I purged of all inputs from users with security levels > U's**"** (McLean, J., 1990). This is another model which is related to policies within a system which can represent as a node for the e-services.

2.3.1.3 Bell-Lapadula model

Bell-Lapadula or BLP is the most well known model to address confidentiality of information. It was developed in 1973 by Bell and Lapadula and became a prominent model for the Mandatory Access Control (MAC) and a true implementation of the multilevel security policy concept (Lindgreen, E. E. O. R. and Herschberg, I. S., 1994). The model is considered as a multilevel security model. The model was implemented in many systems which became known as multilevel secure systems (Anderson, R., April 2001).

The Bell-Lapadula model has two main properties (Anderson, R., April 2001):

1) The property which sets the policy of the read control in the system. The rule of this property that a lower level object can't read a higher level object or what's known as No Read Up (NRU). This property blocks exposure of secured data handled by objects with high level of security.

2) The *property (Star property) which blocks objects with higher security level to write data to objects with lower security level.

In the BLP model, access to the system is classified as: A) **The Mandatory Access Control (MAC)** which is applied when the system enforces a security policy independently of users' actions. B) **The Discretionary Access Control (DAC)** which is applied when users can take their own access decision about their files.

Being the most popular model in data security, a lot of criticisms from researchers in the security field have posted critiques on the BLP model pointing out loop holes. The scientific argument raised by Mclean illustrated that BLP model rules were not in themselves sufficient to provide security. As supporting evidence McLean introduced a system called systems "Z" (McLean, J., 1990) with BLP rules and policies embedded. The system allowed the user to request the system admin to declassify any file from high to low. Through this method users with a low classification in the system can read any high file without breaking the BLP assumptions. The counter academic argument by Lapadula was based on the fact that the breach of security was due to changing labels which is not a valid operation in the BLP core model and any system which applies it. McLean's debate was based on his analysis on the BLP model and findings which indicated that checking the validation of any system operation is not part of the scope. The scientific argument led to an introduction to the tranquillity property; a property which defines two states of security; strong and weak. The strong security state has security labels that never change during the system operation. The weak security state has security labels that never change in such a way as to violate a defined security policy.

2.3.1.4 The Biba model

The Biba model or as known "Bell-Lapadula upside down" was developed by Ken Biba. The model addresses the integrity aspects only and does not address the other two aspects of C.I.A (confidentiality, Integrity, Availability) triad. The basic elements of the Biba have a similar structure as the BLP model (Stallings, W. and Brown, L., 2008), The Biba model

addresses the Low Water Mark Principle which technically means that the integrity of an object is the lowest level of all the objects that contributed to its creation (Anderson, R., April 2001). The low water mark concept was implemented in the industry as part of a system called LOMAC operating system; an extension to Linux Operating System (Fraster, T., 2001). The operation of LOMAC OS reflected the embedding of the low water mark. The way LOMAC OS was applying the water mark concept is by classifying the file systems into network and system files. The operating system has network files and system files. The network and system files have different levels of security. The system files are set with the highest security level and always protected against low security levels objects. The security level of the file system gets downgraded to low integrity if an access from an object is required. The downgraded file will not be able to open or write to a system file. A system file can be a password file for instance (Anderson, R., April 2001).

2.3.2 Multilateral security

As discussed in the previous section the multilevel concept represented by BLP and Biba models focuses on protecting the information vertically based on a standard data classification. Another set of models were developed in the field of the information security following a multilateral concept. These models define policies and rules to protect information flow horizontally. There are three models that represent the multilateral security model concept.

The Three Multilateral Models:

- Compartmentation and Lattice Model.
- Chinese wall.
- British Medical Association (BMA)

2.3.2.1 Compartmentation and lattice model

"The compartmentation model is used by the intelligence community. The term compartmented security is used in the U.S as a common terminology for the Multilateral security as it is called in England and the rest of the world", (Anderson, R., April 2001). A

good compartmentation based model is the lattice model which is a variant of BLP. The Lattice model is a mathematical structure in which any two objects A&B can have dominance relation A>B or B>A. The model is defined by a tuple with five components (SS, OS, CS, *, →) where SS stands for set of subjects causing the information flow, OS stands for the set of objects capable of storing information, CS stands for set of security classes, * is the combining operator and →is the flow relation (the legal flow) (Jie, W., Fernandez, E. B. and Zhang, R. (July 1992). The relation between the different classifications and how a person can have an access to a certain classification but not to another is illustrated in **Figure 6**.

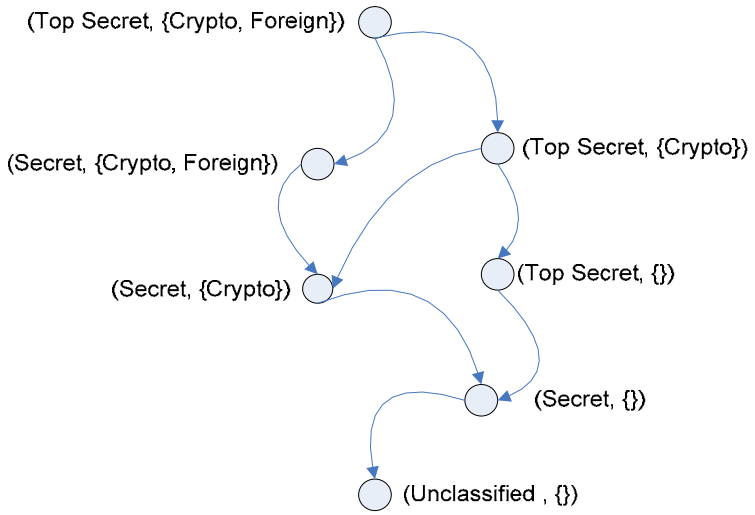


Figure 6: Lattice labels

(Anderson, R., April 2001)

A good application of the Lattice model is the system used for the control of Haj (Pilgrimage) entries in Saudi Arabia. The system controls information sharing through applying algorithms in systems using least upper bonds in the Lattice Theory. The algorithm made all compartments by default as confidential and the combination of data from different compartments is secret.

2.3.2.2 The Chinese wall

The Chinese Wall model was developed by Brewer and Nash (Brewer, D. F. C. and Nash, M. J., 1989) to prevent any conflict of interest with an organisation or between an organisation and its clients. The model is mathematically expressed as shown below:

Let C= client

Y(C)= C's company

X(C)= C's competitor

The Chinese wall model has two main properties which act as the main two rules of the model. Both properties have a mathematical representation as illustrated below:

1. **The simple security property**

"A subject s has access to C if and only if, for all C's that s can read, either $Y(C) \not\subset X(C')$ or $Y(C) = Y(C')$", (Anderson, R., April 2001).

2. **The *property**

"A subject s can write to C only if s can't read any C' with $X(C') \neq 0$ & $Y(C) = Y(C')$" (Anderson, R., April 2001).

The model addresses a threat which is not related to a technology aspect of the security architecture. The conflict of interest threat is a pure human behavioural issue which affects the security programme of the organisation.

2.3.2.3 The British medical association (BMA)

The BMA is a model developed to describe the medical information flow while abiding to the medical ethics and standards (Anderson, R., April 2001). The model assists the medical institutions to exchange information among them while maintaining the privacy of the patients' records. The content of using technology as a method of transferring patients' records and data securely was raised by many countries and medical organisations. Many governments agreed on the methodology of applying the BMA model. The German government (Anderson, R., April 2001) was one of the leading countries using the smartcard technology promoting the idea reflecting its pros and cons. The government of Iceland has initiated a project to build a national medical database that will have medical,

genetic and genealogical data". The BMA model sets the ethics and rules of engagement between institutions inter and intra boundaries of the country.

2.3.3 Application of secure systems

Many products in the industry applied the multilevel security model. The purpose of studying these products was to indicate the possibility of building products (military use or commercial) which can reflect policies and models.

2.3.3.1 SCOMP (Secure Communications Processor)

SCOMP was one of the earliest products developed to reflect the multilevel concept and policies. The project was a collaboration between Honeywell and the US department of defence (DoD) (Akers, R. L., Krohn, M. D., Lanza-Kaduce, L. and Radosevich, M., 1979). The product has four rings of protection and the Operating System is using these rings to maintain up to 32 separate components and to allow one way information flows between them. The security kernel was kept to minimum in order to allow the computer to perform the day to day business operation. This product was used in the military applications such as Mail Guards which is a special firewall that allows mail to pass from low to high but not vice-versa (what's known as data diode). SCOMP was the only machine rated as A1 in 1984 which is the highest security rate a computer system can obtain. The kernel was represented in mathematical values in order to get the rating.

2.3.3.2 Blacker

"Blacker is an example for an encryption device designed to incorporate multi level security (MLS) technology", (Anderson, R., April 2001). The idea of blacker is to separate the encryption processors from the clear text processor by assigning colour codes. The enciphering processor (Encryption processor) has a colour of black while the clear text one has a colour of red. The device was rated as the highest in security rating. It was given A1 as the only communication security device with A1 evaluation. Motorola had tried to produce the second series or a successor but was not able to obtain the same rate. A rate of B2 was given to the new box.

2.3.3.3 NRL pump

The NRL Pump was developed by the Naval Research Laboratory. NRL Pump is one-way data transfer device (data diode) using buffering, while limiting the bandwidth of possible backward leakage by number of mechanisms such as timing randomization of acknowledgement messages. The way the pump works was described in an algorithm format by Lanotte and Tini (Lanotte, R., Maggiolo-Schettini, A., Tini, S., Troina, A. and Tronci, E., 2004). The operation of the pump can be summarized as follows:

- A low agent sends a message to some high agent through the pump.
- The pump stores the message in a buffer and sends an acknowledgement to the low agent.
- The low agent can't send any new message until the acknowledgement of the previous message is received.
- The pump stores the message until the high agent is able to receive it.
- The high agent receives the message and then sends an acknowledgement to the pump.
- The high agent does not acknowledge some received message before a fixed timeout expires. The pump stops the communication.

The following algorithm represents the operation (Lanotte, R., Maggiolo-Schettini, A., Tini, S., Troina, A. and Tronci, E., 2004)**:**

LS: represents the low system
P: represents the pump
HS: represents the high system
A→B: msg represents the message msg sent from A to B
Ls→P: reqL: the low system requests to the pump to start a communication with a high system.
P→LS: validL: the pump checks if the low system is a valid process and, then it acknowledges its request.
P→HS: reqH: the pump requests to the high system to start a communication with the low system.
HS→ P: valid H: the high system checks if the pump is a valid process, and then it acknowledges its request.

P→HS: grant H: the pump communicates to the high system that the communication can start.
P→ LS: grant L: the pump communicates to the low system that the communication can start.
The NRL pump is an implementation of a data transfer methodology based on an algorithm. The algorithm sets the rules on how a system can communicate or transfer data to another. It was found to be a strong mechanism for transferring data or exchanging information but yet has no comprehensive analysis on the other factors which might affect the security programme between two different organisations. Although the algorithm can be placed and enforced on systems designated for intra organisations communication, the policies on these systems and the competencies responsible for supporting these systems will have a direct impact.

2.3.4 The Fundamental Approach for Network Security

Schumacher and Gosh from Arizona State University presented an interesting Network Security Rating Model (NRM) (Schumacher, H. J. and Gosh, S., 1998) using a unique approach which was found similar to the approach the author is following to develop the new model. The network security rating model objective is to set a rating for the network security across different sectors. The first step was to identify the characteristics of any secure network regardless of the sector and independent of any specific threat. The approach was described as **orthogonal model** approach and was developed in 1996.

Seven perspectives were defined in the new model. These perspectives referred to as "pillars" are:

1. Systemic
2. Communication
3. Physical
4. Personnel
5. Operational
6. Application
7. Performance
8. Design correctness

A list of attributes was defined such as privacy, integrity, accountability, availability, reliability, connectivity, recovery from disaster, and uncertainty.

The relationship between the attributes and the pillars of the model is what determines a good security for an entity. Ideally a 100% security means that each attribute needs to be protected in each pillar but in reality this might not be cost effective. Decisions related to the network security will be "based on the perceived threat to a particular pillar and/or attribute and the level of risk that the security management is willing to assume". The main idea behind the model is that the eight pillars represent the main blocks of security which might be under attack. Each block represents an orthogonal conceptual view of the network security. In Gosh's paper, the fuzzy set of Zadeh (Zadeh, L.A. , 2000) was introduced to address different aspects of security networks. The dynamism of the complex networks and the high level of uncertainty associated with the occurrence of attacks and system errors position the analytical modelling as ineffective. Fuzzy sets as far better approach to use for the network stability monitoring.

2.3.5 Human elements related theories

2.3.5.1 The general deterrence theory (GDT)

Social theories such as the General Deterrence Theory (GDT) state that any illegal or criminal act or behaviour can be deterred if the perpetrator is aware of the consequences and legal implications of his actions (Smith, D. A. and Garton, P. R., 1989). As stated by Lee & Lee, "The theory assumes that individuals make decisions based on maximizing their benefits and minimizing their cost" (Lee, J. and Lee, Y., 2002). A crime can only be committed if the benefits from the crime act exceeds the cost of the punishment. If an intruder knows that the computer laws and regulations are not strong enough, the temptation of conducting unauthorized access to e-business entities will be strong. It can be assured that attackers and hackers can even try and use the e-business entity as a virtual lab for new exploits since no law or punishment can deter them. This indeed will create performance degradation on the e-entity or might even lead to Denial of Services (DoS) attack.

The equation got to be balanced between the type of intrusion and the loss caused by it with the severity of the punishment. Attackers will weigh their chances and such deterrence might prevent some if not all attacks on entities.

A real world case of the deterrence theory was learned from the Chinese hackers security case. Two hackers were sent to the death sentence by Yangzhou Intermediate Court of Jiangsue in 1998 (Haney, C., 1999). This case was used by many security practitioners as a good example of deterrence theory and its effect in reducing cyber crimes.

2.3.5.2 The social bond theory

The Social Bond (Gottfredon, M. and Hirschi, T., 1990) analysed the social effect in computer crimes from a different angle "The theory basically assumes that all people are naturally inclined to commit crimes unless a strong control mechanism exist or "social bonds". In the theory, 4-social bonds factors were identified: Attachment, Involvement, Commitment, and Beliefs. In 1999, Costello and Vowell discovered a direct relation between the four social bounds factors and the reduction of deviant behaviours (Anderson.B, Homes., et al., 1999)

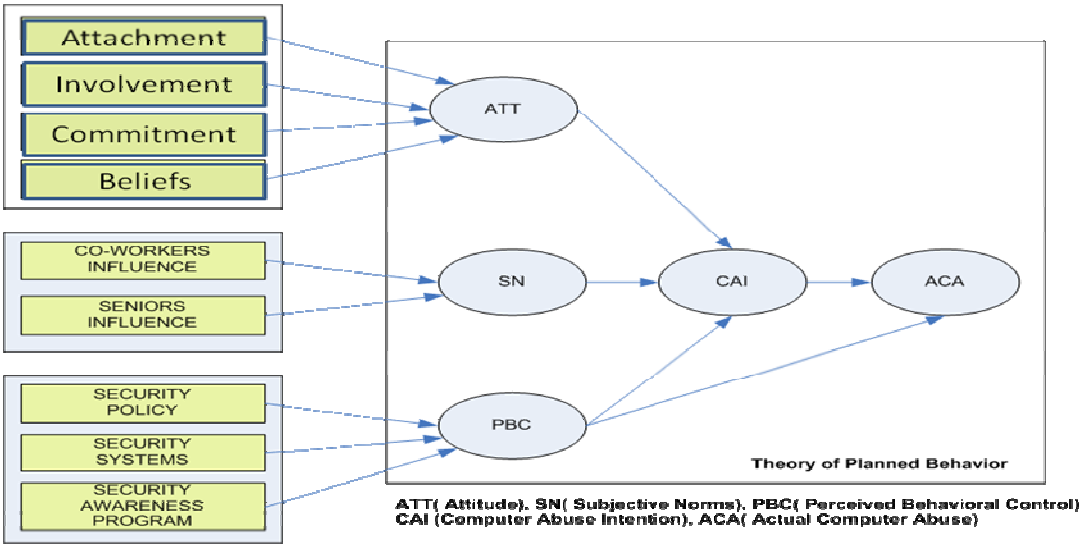
2.3.5.3 The social learning theory

The Social Learning Theory (Akers, R. L., Krohn, M. D., Lanza-Kaduce, L. and Radosevich, M., 1979) assumes that a person commits a crime because he or she has come to associate with delinquent peers, who transmit delinquent values, reinforce delinquency and function as delinquent role model (Lee, J. and Lee, Y., 2002). The theory discussed two sources of social learning, Co-workers influence and Senior Influence. "The probability that people will engage in criminal and deviant behaviour is increased and the probability of their confirming to norm are decreased when they differentially associated with others who commit criminal behaviour" (Lee, J. and Lee, Y., 2002). The influence can be effective only if a person is not aware of righteousness and wrong or if righteousness is misinterpreted by a person. A person can be protected if he is fully aware of what's right and what's wrong and can stop such influence if he comprehends that such influence will lead him to commit wrongful behaviour. Most of the people will not be able to stop or

restrain from those who are wrongly affecting them since the friendship relation might cause a blur and misguide the judgment of the person.

2.3.5.4 The three social theories (GDT, social bond, social learning)

A good model developed by J.L and Y.L links the General Deterrence Theory (GT), Social Bond Theory, and the Social Learning Theory to computer crimes (Lee, J. and Lee, Y., 2002). The model **(Figure 7)** used the social theories which were developed in the past to derive the three reasons of committing computer crimes or abuse; the Attitude abbreviated in the model as (ATT), Subjective Norm (SN), and Perceived Behaviour Control (PBC). The three main factors will not lead directly to computer abuse or misconduct. The intention will be built up leading to an actual computer crime. The model illustrated that each element contributing to the computer crime has different feeders. The ATT element gets constructed from the attachment, involvement, commitment, and reliefs. The subject norm factor has different reasons to be built. It is directly related to co-workers influence and senior influence. The PCB has a direct relation to the main components of any security programme; policies, security systems, and awareness programmes.



(Lee, J. and Lee, Y., 2002)

Figure 7: The three social theories

The above diagram shows that computer crimes are not necessarily due to technological aspects only. Crimes might be conducted due to inappropriate security policies, light punishment of computer (Skinner, W. F. and Fream, A. M., 1997), or discrimination of sanction based on the level or privilege of employees (Straub, D. W., 1990). The implementation of non IT related countermeasures could effectively lower threats caused by internal errors (Arthur, J. C. and Quey-Jen, Y., 2006).

2.3.6 The e-commerce security model

Various e-services can be provided from an e-commerce organisation. E-Services are offered to different customers from different market sectors. The geographical boundary doesn't exist or act as a constraint for e-commerce organisations market expansion. A model was developed to address the e-commerce threats. The objective of the model was to identify the recognized threats on the e-commerce e-services. The e-commerce security model developed by Kesh, Ramanujan, and Nerur (Venter, H. S. and Ellof, J. H. P., 2003) was analyzed and found to follow the approach of securing e-commerce/e-enabled services through technology. This was illustrated through the final model diagram **(Figure 8)**.

The relationship between different threats and techniques is illustrated in **Table 5** (Gottfredon, M. and Hirschi, T., 1990). It aims to address all possible threats for the e-commerce and the technologies which will be needed to mitigate these threats. The tools and the supported technologies which can be used in the e-commerce model were showing 1-1 or 1-many relationship between threats and security measures. The major components of the E-commerce systems were studied by the architects of the model in order to come up with a model to address all aspects of E-commerce security. The components analyzed were the E-commerce Development Platforms, Database Management Systems, Operating Systems, and the Network Infrastructure.

The strength of the final model developed by the researchers was in drawing a good relationship between the technologies and the tools used to implement these technologies. As illustrated in the final model **(Figure 8)**, there are some technologies which will overlap

with each other in terms of functionalities and might be eliminated from the security architecture. The different security tools can be selected based on functionality desired and the layer of security it needs to protect.

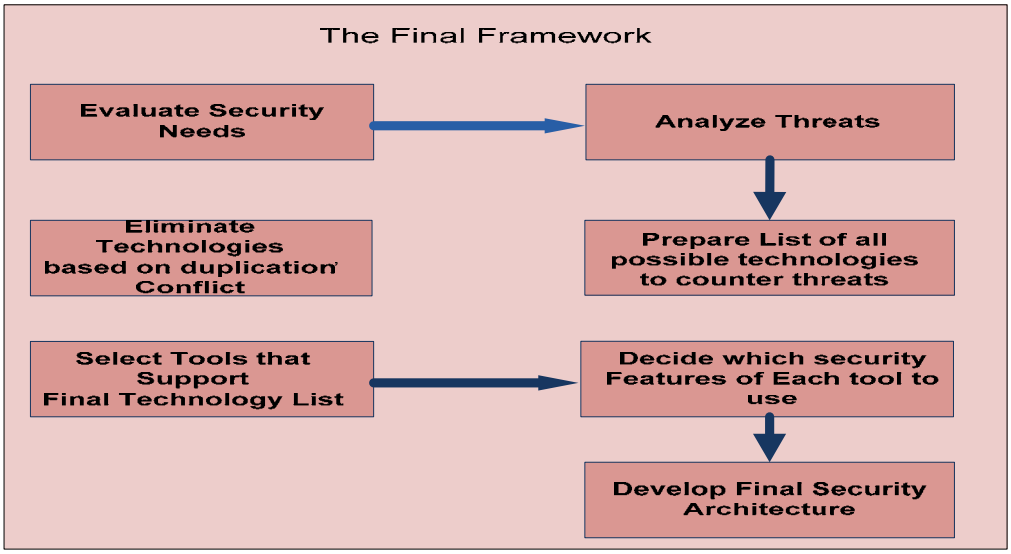


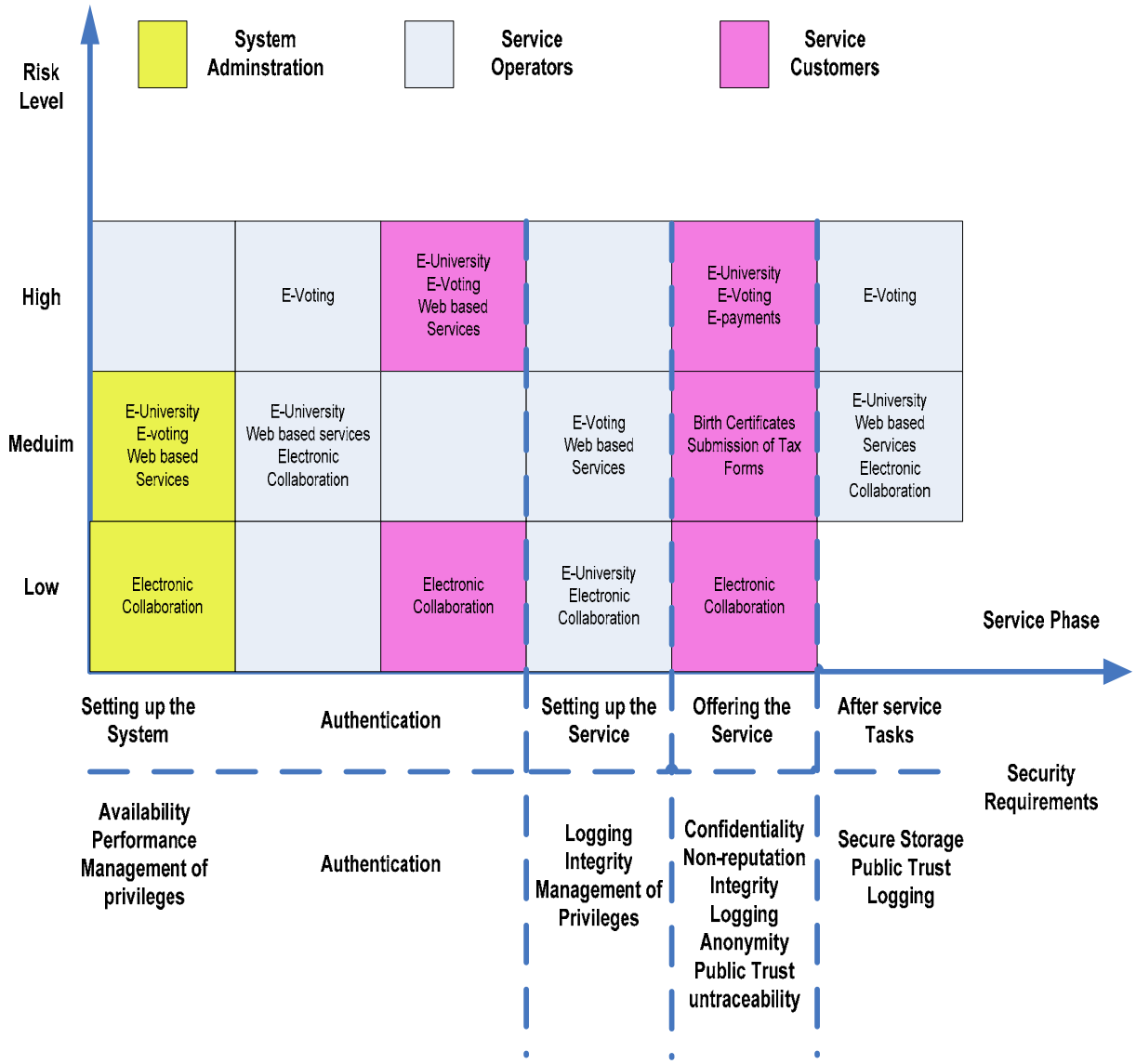
Figure 8: E-commerce security model and framework

Table 5: Threats vs. Technologies

Code	*Threat*	Code	Security Measure
T1	Gaining Physical access to premises	S1.0	**Physical access control Locks**
		S1.1	**biometric authentication**
T2	Wiretaps	S2.0	**Time domain reflectometer**
		S2.1	**Optical time domain reflectometer**
		S2.2	**Intrusion detection systems**
T3	Packet sniffing	S3.0	**Anti-sniffing tools**
		S3.1	**Strong authentication**
		S3.2	**Cryptography**
		S3.3	**Switched architecture**
T4	Impersonating	S4.0	**Password complexity requirements**
		S4.1	**Kerberos**
T5	Gaining access to information	S5.0	**Firewalls**
		S5.1	**Symmetric encryption (DES)**
		S5.2	**Triple DES (3DES)**
		S5.3	**AES**
		S5.4	**Pretty good privacy (PGP)**
		S5.5	**Public key infrastructure (PKI)**
		S5.6	**IPSec**
		S5.7	**SSL/SET**
T6	Integrity	S6.0	**Error checking/Correcting MD5**
		S6.1	**Cyclic redundancy check**
		S6.2	**Forward error correction**
		S6.3	**Hash functions**
		S6.4	**Secure hash algorithm (MD4 or MD5)**
T7	Non repudiation	S7.0	**Digital signature**
T8	Viruses	S8.0	**Anti-virus software**
		S8.1	**Network segmentation**
T9	Denial of service attacks	S9.0	**Quality of service (QoS)**
		S9.1	**Implementing router filters**
		S9.2	**Install patches against TCP SYN**
		S9.3	**Disable unused/unneeded network services**
		S9.4	**Appropriate password policies**
		S9.5	**Quotas for operating systems**
		S9.6	**Strong authentication and authorization**

2.3.7 *Lambrinoudakis security framework*

There is no doubt that most of the government e-services are supported by solid technology infrastructure. A typical risk assessment covers mostly the technological platform supporting the services. The objective of placing these technologies is to protect the services from being maliciously altered or blocked known as "Denial of Services". The methodological approach of Lambrinoudakis et al was found very illustrative. (Lambrinoudakis, C., Gritzals, S., Dridi, F. and Pernul, G., 2003). The framework was developed to identify and organize the security requirements for the information systems supporting the e-services offered by the e-government **(Figure 9)**. A risk analysis was conducted on the e-University which represents a suite of services and allows remote accessibility. Lambrinoudakis divided the cycle of the e-University service launch into 5 steps (setting up the supporting system, authentication, setting up the service, offering the service, and after service task). Each step was given a risk level and assigned security measures as indicated in **Table 6.** The framework did not address the human aspects of the cycle, competencies requirements, and the need of the enforcement of the security policy throughout the cycle. It only addressed the operational and management aspects such as logging and storage. Taking into consideration that most of the e-University users will be from the age of 16-24 years, matching the same age of most of the hackers in the world, there is a strong probability that the e-University service will be a good target to cyber attacks. The competency of security staff must be equivalent if not better than the attackers' capabilities and the policies must be developed to block internal and external threats. Ignoring these two key security aspects was found as a weakness in Lambrinoudakis framework.



(Lambrinoudakis, C., Gritzals, S., Dridi, F. and Pernul, G., 2003)

Figure 9: Lambrinoudakis Model

Table 6: e-university risk level & security requirements

Suite of Services	Service Phase	Actor type	Risk level	Security requirements
e-University	Setting up the system (setting up the hardware and software infrastructure required for the operation of the designed services)	System administrators	Medium	- System availability - Performance - Management of privileges
	Authentication	Service operators Service customers	Medium High	- Authentication
	Setting up the services (course organisation and material preparation0	Service operators	Low	- Integrity - Logging
	Offering the service (offering on-line courses and other supporting – educational-tasks to students	Service customers	High	- Confidentiality - Integrity - Non-repudiation - Logging
	After service tasks (maintaining progress-issuing certificates, etc)	Service operators	Medium	- Secure storage - Logging

(Lambrinoudakis, C., Gritzals, S., Dridi, F. and Pernul, G., 2003)

2.3.8 The analysis of networked systems security risks (ANSSR)

The Analysis of Networked Systems Security Risks (ANSSR) follows the approach of analyzing threats from one source, the attackers. This has given the model a weak position as attackers only take advantages of weaknesses which might be related to technologies, policies and other aspects (Bodeau, D. J., 1992). Other possible threat sources such as human errors, structural failure, or natural disaster are not considered.

The model identified 5 types of deliberate attackers types:

- Users(including trusted users)
- Developers
- Maintainers
- Customers
- Outsiders

The model sets the right measures on the threats scenarios, based on the understanding of the two associated measures with any threat: the likelihood of Initiation and the likelihood of Impact. The likelihood of initiation depends on the attackers' expectation while the likelihood of impact depends on the capability of the attacker and the system safeguard.

This approach was effective but it doesn't cover all aspects of the threats analysis, as the likelihood of initiation is only linked to attackers only. There are other sources of threats which may cause a direct damage or loss to the e-service. These factors can be considered as the root cause of any attack attempt.

2.3.9 Models for checking internet commerce

Many models were developed for enforcing checks for the Internet Commerce. Some of them were concentrating on equipment which will perform checks related to scheduling with fixed regular time period. A seminal model was developed by Eisen and Lienbwitz for the replacement of random deteriorating equipment that remains current and relevant (Hansen, J., 2001). Keller addressed the issue of optimal checking schedules using calculus of variation methods (Keller , J., 1974). Different controls for monitoring the Internet were developed by many researchers. A mathematical model was developed by JV Hansen (Hansen, J., 2001) for optimization and artificial intelligence methods for scheduling the monitoring of related controls of the Internet Commerce (IC).

The optimization model has the following key elements and assumptions:

1. Controls are to be checked at a fixed time interval t.
2. Number of controls remains constant and immediately after a control check, the cost of control failure (CCF) is L0.
3. The cost of monitoring is constant M.
4. The cost of control failure increases at a fixed rate r.
5. After a time t since last check, the CCF is L0+rt.

The control system is in existence for a total time T and the number of checking intervals is N=T/t, therefore; cost (total) (CT) over time is the sum of CCF and the cost of checking. The objective is to minimize C (T).

The mathematical model was explicitly explained by Keller (Keller, J., 1974). The objective for analyzing such a model was to learn how mathematical models are built to reflect an idea related to Internet Commerce or e-business. Expressing controls, cost of monitoring and other elements of the Internet commerce in a mathematical formula is a new area of learning during the analysis of Keller's model.

2.3.10 The security standards

Models alone will not provide comprehensive security programme to the organisation. In this section, well known security standards will be addressed to reflect the applicability in different types of organisations. Security standards address the minimum mandatory rules an organisation is required to follow in order to provide an acceptable security level (Karabacak, B. and Sogukpinar, I., 2005). Having a security model that addresses technology only and implemented across multiple organisations will be a challenge unless the model is complemented by security standards and policies.

2.3.10.1 BS7799

The British standard was originally launched in 1999 and was named as BS 7799-2:1999 and was changed to ISO/IEC 17799 in 2005 (Karabacak, B. and Sogukpinar, I., Sept 2006). British Standard 7799 covers the management of information security. It has 133 controls

in 11 different domains. The objective of the standard is (Hone, K. and Eloff, J. H. P., 2002), "to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used". The standard explains what needs to be included as a minimum in the security policy to guarantee the baseline of protection for any organisation.

Many software solutions were developed to assist in obtaining the ISO/IEC 17799 certification. These applications ensure that all domains are covered and all controls are set in place. The author explored some of the well known applications used for this purpose such as Riskwatch (Riskwatch, 2005) and Corba which was used for the compliance check of ISO 17799. (C&A systems security limited, 2000).

2.3.10.2 BSI IT baseline protection manual

This standard was developed by German Bundesamt Fur Sicherheit. The standard covers controls to safeguard organisations. The main goal of the standard is to "achieve a security level for IT systems that is reasonable and adequate to satisfy normal protection requirements and can also serve as the basis for IT systems and application requiring a high degree of protection".

2.3.10.3 COBIT

The Control Objectives for Information and related Technology, COBIT, was developed by the Information Systems Audit and Control Association and Foundation (ISACAF). The standard was released 10 years ago. The last version of COBIT 4.0 was released in 2005 and it has 34 high-level control objectives or processes are referred to in some journals grouped in 4 domains (Hardy, G. (2006):

- Plan and organize
- Acquire and implement
- Deliver and support
- Maintain and evaluate

Each of the 34 processes has a Control Objective (CO) and each CO is divided into a set of Detailed Control Objectives (DCO) (Solms, V. B., 2005). There are 316 DCOs defined for the 34 control objectives/processes.

COBIT provides management and business process owners with an IT governance model to manage risks associated with IT (Hone, K. and Eloff, J. H. P., 2002). The mission of COBIT is "To research, develop, public and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors" (Hone, K. and Eloff, J. H. P., 2002). COBIT was found as a good model to use not exclusively for information security. The model addresses the information technology governance issues and one of them is information security.

2.3.10.4 Generally accepted system security principles (GASSP)

GASSP was published by the United States of America's National Research Council (I2SF99). The foundation of the GASSP Committee began in mid 1992 having four main objectives (Ozier, W., 1998):

- Promoting good information security practice
- Building a focal point of reference and legal reference for security principles, practices, and opinions
- Continuous improvement of the effectiveness and efficiency of the IT security functions.
- Having a common body of knowledge for the Information security certification.

This standard is the least known since its U.S centric. The GASSP contains the following pervasive principles (Krull, R. A., 1996) :

- Accountability Principle
- Awareness Principle
- Ethics Principle

- Multidisciplinary Principle
- Proportionality Principe
- Integration Principle
- Timeliness principle
- Reassessment Principle
- Democracy Principle

2.3.11 The infosec model

During the research process, a multi layers model was found called "Infosec Model" **(Figure 10)** developed by Ryan & Ryan (Nichols, R. K., Ryan, D. J. and Ryan, J. J. C., 2000) consists of different layers covering different aspects of security. The model was analyzed and reviewed in order to know the purpose of the model, its layers structure and how they were constructed together, its academic background, and its validity.

The InfoSec model considers the threat analysis as the foundation of all layers represented within the model. The approach to develop the model was based on the need of having enough measures to get an insurance policy covering all critical assets. The model was derived as part of the need of Information Protection Architecture (Nichols, R. K., Ryan, D. J. and Ryan, J. J. C., 2000). Its risk assessment management is base on the protection of confidentiality, integrity, and availability.

As it is shown in **Figure 10** the R&D section which includes the architectures, design, development and evaluation is built on top of the acquisition and operation and maintenance.

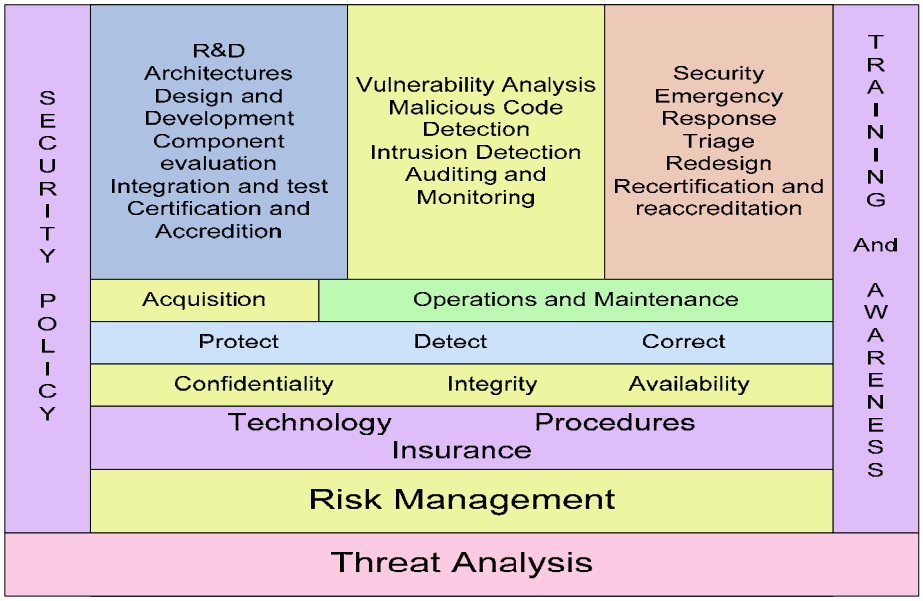


Figure 10: InfoSec model

The infosec model has the following objectives (Nichols, R. K., Ryan, D. J. and Ryan, J. J. C., 2000):

- Minimizing Vulnerabilities to our information assets and computer systems.
- Choose appropriate countermeasures to prevent digital espionage.
- Reduce the likelihood of successful attacks.

The architects of the InfoSec model stated that the above objectives can be met through the complement of the layers with each other.

2.3.12 Security models used as marketing tools

A search for models used by the industry or security vendors was conducted. A model from Symantec **(Figure 11)** was found to be comprehensive where different layers of the security programme were covered through products and services offered through the Symantec products portfolio. The purpose of the model was to assist Symantec customers to implement security architectures, processes, and policies. It was observed that the objective of the model is to position Symantec as a service provider not a commodity seller. The tool was used as a marketing tool rather than a scientific approach but yet was found as

a good reference to technology elements required to complement different functions. Symantec has another view of the information integrity which combines information security and information availability. The main purpose of information confidentiality or security as presented by Symantec is to protect the information from being disclosed to any unauthorized person. Information integrity is to protect the data from unauthorized malicious or accidental data changes. The information availability is to ensure that data is available when it is needed. The combination of both information confidentiality and availability will ensure the integrity of data as indicated below:

> Information Security + Information Availability = Information Integrity (Symantec 2002 230)

Although the Symantec model is categorised as a marketing and sales tool, it reflects three important layers of any security programme; the technology, knowledge and response, and management of risk. The model clearly illustrates that each layer requires different security elements which collectively contribute to build the strength of the layer.

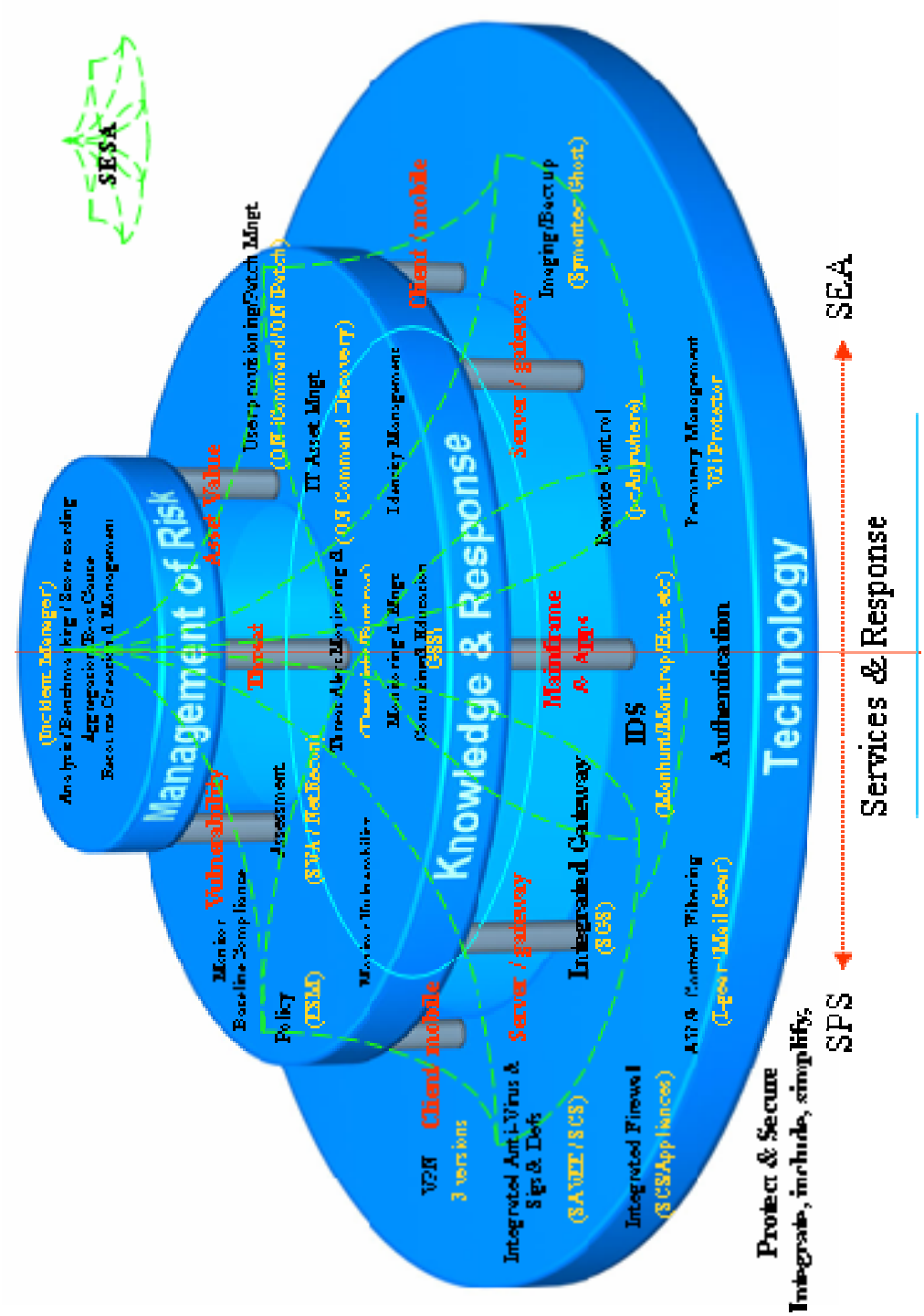


Figure 11: Symantec industrial model

(Symantec , 2002)

2.4 Literature review analysis

The main objective of security models is to protect the organisation information and intellectual property. Government information is classified as the most valuable and confidential as it includes the citizens' private information. Whether it is governmental or commercial information, it is usually stored in the local IT infrastructure of the custodian organisation. Sharing governmental information between government departments is considered the highest risk a government department in Dubai considers.

The literature reported is analysed to discover common characteristics of information security. The analysis is reported in four tables according to the nature of the literature. The characteristics are distilled from the content of the papers. Each column represents a key paper reported. The cell in the table indicates if the paper addresses the characteristics in the row.

The definitions of the characteristics:

Structured in layers: The model was represented in a visual representations with all the layers related to it.

Coverage of security aspects: The main areas of security (technology, policy, operation, human aspects, etc) addressed by the model.

Explicitly explained: The literature explained the models in detail.

Government or commercially used: The models are used by government and non government organisations.

Applicability to any sector: The model can be applied to any sector or industry.

Addressing information flow: The model addressed information flow within a system or addresses the flow of information across multiple systems/networks.

The first table **(Table 7)** summarises the information security models explained in section 2.3.1 and 2.3.2.

Table 7: Models in Section 2.3.1 and 2.3.2

Characteristics	Models							
	Non Deducibility	Non Interference	Bell-Lapadula	Biba	Comp & Lattice	Chinese wall	BMA	Internet ops
Structured in Layers								
Coverage of Sec Aspects								
Technology							■	■
Policy	■	■	■	■	■	■	■	■
Human behaviour and awareness								
Ops and Mgmt							■	■
Explicitly explained	■	■	■	■	■	■	■	■
Government or commercially used							■	
Applicability to any sector	■	■	■	■	■	■	■	■
Address Info flow								
Within One System or entity	■	■	■	■	■	■		
Within Several Systems							■	■

Table Key:

Yes	No
■	

Gap analysis: The majority of the models above are not addressing more than one aspect of information security and focus on the security of a single system or node. It has also been observed that the above models are not structured in terms of layers and modelling principles.

The second table **(Table 8)** summarises the models applied in particular system reported in section 2.3.3.

Table 8: Models with application

Characteristics	Application of Models		
	SCOMP	Blacker	NRL
Structured in Layers			
Coverage of Sec Aspects			
Technology	■	■	■
Policy	■	■	■
Human Behaviour and awareness			
Ops and Mgmt			
Explicitly explained	■	■	■
Government or commercially used		■	
Applicability to any sector			
Address Info flow			
Within One System or entity	■		
Within Several Systems			■

Table Key:

Yes	No
■	

Gap analysis: The security technologies above are implementation of the security policies and models discussed in the first table. Since they are technologies and implementation policies from the above models, they cover two aspects (technologies and policies). They are not structured as models and their usage is limited to military use.

Through the literature review, the author learned different models and methods of securing the exchange of digital documents over the Internet or public networks. Methods such as digital signatures, different cryptographic techniques, setting higher factors of authentication (Kaliontzoglou, A., Sklaros, P. and Karantjias, T., 2005) were considered during the construction of the new model. It was clearly observed that there is no comprehensive model which addresses all areas or aspects affecting the security of the information. The two models found to be partially comprehensive, during the literature

reviews, were the Network Rating Model (NRM) (Schumacher, H. J. and Gosh, S., 1998) and the InfoSec model (Nichols, R. K., Ryan, D. J. and Ryan, J. J. C., 2000).

The third table summarises the models that have structured representation.

Table 9: Structured models

Characteristics	Models					
	NRM	3 Social Theories	E-Commerce	Lambrinoudakis	InfoSec	Symantec
Structured in Layers	■	■	■	■	■	■
Coverage of Sec Aspects						
Technology	■		■	■	■	■
Policy		■			■	■
Human Behaviour and awareness					■	
Ops and Mgmt				■	■	■
Explicitly explained	■	■	■	■		
Government or commercially used					■	■
Applicability to any sector	■	■	■		■	■
Address Info flow						
Within One System or entity						
Within Several Systems	■	■	■	■	■	■

Table Key:

Yes	No
■	

Gap analysis: All the above models are structured and have good visual representations. Some of them were explicitly explained while others were not supported by the academic basis, such as the InfoSec model. The majority of the models handle one aspect of the information security. Two of the above models handle two aspects of the information security and one model handles 4 aspects (InfoSec).

The fourth table summarises the security standards reviewed.

Table 10: Security standards

Characteristics	Security Standards			
	BS7799	BSI IT	COBIT	GASSP
Structured in Layers				
Coverage of Sec Aspects				
Technology	■	■	■	■
Policy	■	■	■	■
Human behaviour and awareness				
Ops and Mgmt	■	■	■	■
Explicitly explained	■	■	■	■
Government or commercially used	■	■	■	■
Applicability to any sector	■	■	■	■
Address Info flow				
Within One System or entity				
Within Several Systems	■	■	■	■

Table Key:

Yes	No
■	

Gap analysis: The security standards illustrated above are cover the majority of all security aspects. The only gap that they have is their missing of the competency aspects of the security team and the cost of the implementation of the standards. The different standards which make it difficult for the management of the organizations to understand and grasp which one to use.

From the table, the majority of the analysed models were addressing information security from one or two aspects only. There is no doubt that security technologies reduce the vulnerabilities and identify attacks and breaches. With the evolution of the security technology research more intelligence is embedded within the technologies to allow a fast reaction to attacks and breaches (Gupta, M., Rees, J., Chturvedi, A. and Chi, J., 2006). Few theories were found discussing the socio-technical impact on the security systems. Security researchers defined the e-business security architecture as the combination of technologies,

processes, and people which address the security triad; confidentiality, integrity, and availability. Through practical experience with cybercrimes conducted on various businesses and government, it was observed that the human element and behaviour have important roles in enhancing the e-business security for organisations and governments. Processes and technologies are only tools used to construct security system and the human intervention. Another dimension to look at is the internal business processes supporting the e-services launched by the organisation. The business processes have a direct effect on the efficiency of the organisation (Tanaka, H., Mastuura, K. and Sudoh, O., 2005). Ideally, automating them will enable the organisation to launch e-services faster and to interact with citizens or customers seamlessly. The practical reality shows that the business processes are not always practiced, or even fully automated. Lacking the enforcement and automation of the business processes is what blocks an organisation from transforming to the e-business model. Considering the business processes of any organisation as the main set of processes, the security processes and procedures are a subset of the overall business processes of the organisation. Lacking the enforcement of the security processes subset will not block the organisation from transforming to the e-business model but definitely it will introduce risks which might collapse the model and cause heavy direct and indirect losses. There are many reasons for the failure of implementing the security processes. Some might be due to the lack of deploying the appropriate technologies, competencies, policies, or operational procedures. It can be as a result of inability to take the right business decision by the business leaders of the organisation. Adopting “shortcuts” or “Work around” as known in the business terminology can be a risk for any organisation implementing the e-business model and it can be one of the risk factors. The driver of the shortcut of any process or procedure might be to gain advantage of being the first or for having a differentiator. The objective might be correct as per a good marketing effort but the consequence of overlooking security processes will lead to major losses and sometimes to a total collapse of the organisation. Reluctance to practice processes is a human relevant issue and can’t be solved by the Hard System Methodology (HSM). Studying this factor will need applying the Soft System Methodology (SSM) (Smith, D. A. and Garton, P. R., 1989) and other qualitative methodologies. A comprehensive model which is simple but constructed to

include all relevant elements in an architecture shall provide the foundation to build a solid security programme for any organisation willing to transform to an e-organisation, whether it is a government department of a business corporation.

2.5 Chapter summary

This chapter has three main parts; the first part addresses the evolution of the e-world and how Dubai adopted the concept and embarked the e-government initiative. The second part covers the literature review and the objectives of review the existing models.

In the first part the evolution of the e-world and its influence on many organisations and governments to adopt as a concept and as mean of achieving efficiency and higher customers and citizens satisfaction has been highlighted. Dubai government was one of the early governments in the Middle East adopting this concept in 1999. Through the strong support of the leadership, Dubai government departments started to offer their services in an online format or as e-services allowing the citizens to interact directly with the government beyond the boundary of working hour's limitation and the physical presence. Dubai government established Dubai e-government (DEG) authority and assigned the mission of launching the e-services, coordinating with the government departments, and promoting the culture and concept of the e-government to it. DEG authority was able to influence the launch of 600 online services and came up more e-services which were launched directly by DEG authority. The evolution of the e-government continued but the information sharing between the departments persisted as a challenge. The lack of the backend systems integration and information sharing were linked to low level of trust between departments and the misalignment in the security levels across the government departments. Indeed this derived the need of developing a new model to address this challenge and to be tested in Dubai government for applicability.

Knowing the evolution of the e-government worldwide and the adaptation of the concept in Dubai gave the author the ground to build the research case. The challenges faced by DEG authority in information sharing and integration were discussed explicitly in the first part of the chapter. In the second part, the existing security models were reviewed and analyzed.

Many security models were developed in the past addressing different aspects of security and were the efforts of in dept researches carried by scholars and security practitioners. These models were studied and analyzed in order to highlight the weaknesses and the strengths of each one of them. The objective was to come up with a comprehensive model that addresses all aspects collectively covered in the existing models and the address new aspects considered as gaps in all of them. This process was completed through the literature review conducted on the existing models.

Chapter three: Research methodology

3.1. Overview

This chapter begins with addressing the nature of the research problem. In the second part of the chapter, the author explains the implemented research process and its nine steps. The author then concludes with the chapter summary highlighting all the key findings of the research methodology.

3.2. Nature of research problem

Conducting research in the real world was a challenge for thesis development due to the lack of a central body/authority to provide information for the e-government evolution. Many governmental departments initiated e-services as a proactive step towards the citizens needs in Dubai. The e-government concept in Dubai started as a leadership initiative and evolved to become a strategy of the twenty seven departments in the city of Dubai. Every government department took the initiative to automate its government services and turn them into e-services published to the citizens of Dubai. Since the launch of the government e-services was not initially collaborated with the e-government authority and the government departments themselves, it created the challenge of services and business processes integration. It also created an inconsistency in the evolution of the e-services as some departments were faster than others in reaching the transactional level of the e-services. The followings are some of the key challenges faced during the research process:

- **Lack of transparency**: Since the nature of this research is information security and the case study is a government authority, this particular challenge was anticipated since the beginning of the thesis development process. An attempt was made to address some questions through the questionnaires related to the number of security incidents encountered, the comfort in exchanging information with other government departments, and the perception on the information security in the government departments. These questions were either not answered or answered with reservations by some government respondents. The author has to extract the

information through indirect ways of addressing the questions over the interviews conducted with some of the security practitioners or IT managers in person or through phone interviews. This indeed increased the time and effort in the data collection phase in the research process but was overcome with certain limitations.

- **Lack of the holistic view of the subject matter:** During some of the brief interviews conducted with some of the technology heads of the government departments to explain the purpose of the research it was also noticed that the holistic view the security concept was lacking. The importance of information security to the government departments and to the e-government in Dubai is not strongly believed in many government departments. This was noticed through the low attention the information security departments were given (if they exist) and the weakness/limitation of the security infrastructures within the government departments.

- **Inadequate references:** the author had struggled to find good references or documents about the evolution of DEG authority and all the e-services offered either through the common portal or the governmental departments' sites. The lack of academic case studies on DEG authority, publications, or white papers was a challenge for the extraction of information in the literature review and data analysis.

Despite the above challenges, the objectives of the research as mentioned in Section 1.4 were the pillars of the research methodology and the research process was implemented to achieve them. The literature phase of the research process assisted in finding non-technological security measures which can contribute in building the security architecture in the government departments. The fact that technology was always assumed to be the only element of security which needs to be part of any risk assessment for any organisation has directed the author to search for other elements/measures during the research process. The research of this thesis proves that other aspects such as the availability of the security competencies, security policies, security operational procedures and management, and the

support of the right management decisions, are all contributing to the structure of a comprehensive security model which can address different threats on online services.

3.3. The research design

Research methodologies vary from qualitative to quantitative (Robson, C., 2002). Each method assists the researcher to achieve objectives and goals of the research with tools which enable the researcher to obtain data, analyze it, and present the outputs. Creswell's (Creswell, J. W., 2003) provided three main elements/questions which will need to be addressed in order to come up with a structured and well designed research. The knowledge claim, the research strategy, and method of the data collection are the main pillars of a good research. As it was noted in Creswell's book that "researchers make claims about what is knowledge **(ontology)**, how we know it **(epistemology)**, what values go into it **(axiology)**, how we write about it **(rhetoric)**, and the processes for studying it **(methodology)".** In this research context, the knowledge is information security and the need of building a new model for the e-government intercommunication. The knowledge is obtained from the author's background in the field of information security and from the data collection process during the research study. The value of this research will be reflected through the new model developed and how it will assist the e-government authority and its affiliates in sharing information and ensuring a consistent level of security. The thesis reflects the overall research process and all the relevant research steps taken. The author adopted a methodological approach in reaching the final security model.

Researchers who follow the quantitative approach use the post-positivism knowledge claim. The qualitative approach will reflect the constructivism knowledge claim and it uses narrative, phenomenologies, ethnographies, grounded theories and case studies as strategies of inquires. The pragmatic approach is a mixed method approach between the quantitative and qualitative (Robson, C., 2002).

Personal and professional connection with the Dubai e-government falls into what Creswell referred to as "Backyard" research (Creswell, J. W., 2003). This relationship is clarified

through the research process and strong demarcation lines are set to avoid researcher bias. The data collection and analysis were conducted in methods to avoid any biased, incomplete or manipulated data. Due to the background of the research and being a security practitioner for more than 10 years, the researcher bias issue was recognized from the beginning of the research. To avoid any biased analysis of the research, 16 security practitioners from the different background and different organizations were invited to participate in the technical questionnaire (questionnaire B) in order to record and analyse the different views on the new security model. The practitioners were asked direct questions related to the model and its layers were given the chance through the questionnaire to rate any layer or sub-layer low in order to drop it from model. In questionnaire A, the respondents were given direct and indirect questions related to the security of the e-government. The respondents were also given the choice to select other threats, areas of the security programme which might be running their organizations, and were not directed to give any answer to only support the model. The answers were designed to relate to the new model developed but were set in a method that they don't have to be positive supporting all the time.

The field of information security is a convergence of different scientific and social sciences such as computer science, engineering, psychology, etc, different parts of the most common three knowledge claims (post-positivism, constructivism, and pragmatism) were used. The post-positivism was used due to the reason that the theories, hypotheses, background knowledge of the researcher can affect and influence of the observations of the research (Robson, C., 2002). The author knowledge background in the information security field has informed the data collection process and helps to focus the areas which needed more data analysis to confirm the need of the comprehensive model and the layers which will construct the overall final model. Interviews and questionnaires to learn the different perspectives of security follow the constructivism approach of knowledge claim **(Figure 12)**. This approach as stated above will be qualitative. It can also be argued that since the analysis of the data was based on both qualitative and quantitative approaches, the pragmatism school of thought was also adopted during the research process.

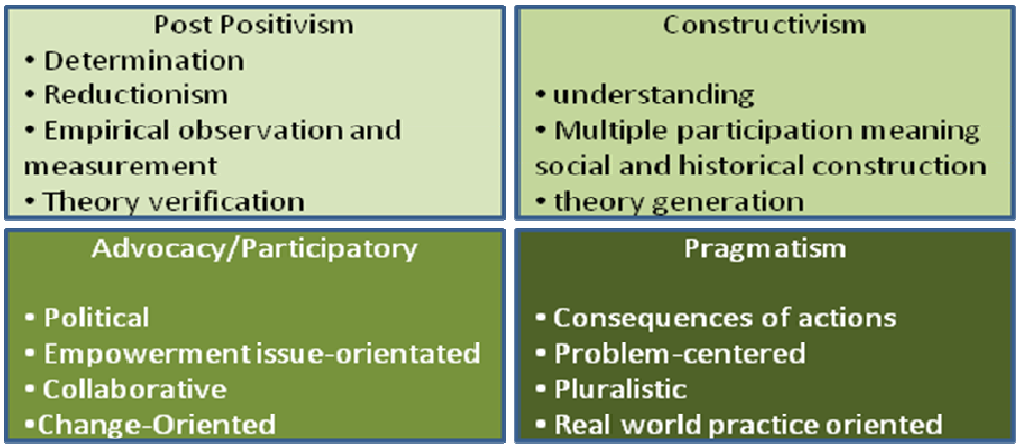


Figure 12: Knowledge claim selected

Source: (O'Leary, Z., 2004)

To draw a clear line between the qualitative and quantitative approaches in the data analysis, O'Leary's comparison **(Table 11)** was found useful to build the knowledge base of both approaches (O'Leary, Z., 2004). Qualitative approach was used when scenarios for applicability or confirming a layer in the model are required. The thematic analysis was practiced and results explained explicitly. The quantitative approach was used where numeric analysis is required for the number of security technologies, rate of importance and percentages for technologies, policies and competencies, the correlation questions related to which technologies, policies, competencies, operational procedures, and decision factors are required for the different types of government e-services.

Table 11: The essential guide to doing research

	Quantitative	Qualitative
Paradigm/Assumptions	Positivism, Empiricism	Subjectivism, Interpretivism, onstructivism
Methodology	Scientific method, hypothesis-driven, deductive, reliable, valid, reproducible, objective, generalized.	Ethnomethodology, Phenomenology, Ethnography, action-research, inductive, subjective, idiographic, institutive.
Methods	Large-scale, generally surveying	Small-scale, interviewing, observation, document analysis
Data Type	Quantitative	Qualitative
Analysis	Statistics	Thematic exploration

In the data collection process, both questionnaires and interviewing methods were adopted. The interview data were analyzed using the immersion approach (Robson, C., 2002) as the author used his professional interpretation skills to understand the reasons of selecting certain technologies by other security practitioners and some of the threats strongly identified by the heads of the government departments. The questionnaires were designed to include open ended questions and closed ended questions in order to give the participants the flexibility to add more comments and points and not be restricted to the answers provided for any question (Creswell, J. W., 2003).

3.4. The implemented research methodology

Kumar (Kumar, R., 1996) summarized the steps need to be taken for a good research process in a single diagram **(Figure 13)** which was used as the base for the research process of this thesis.

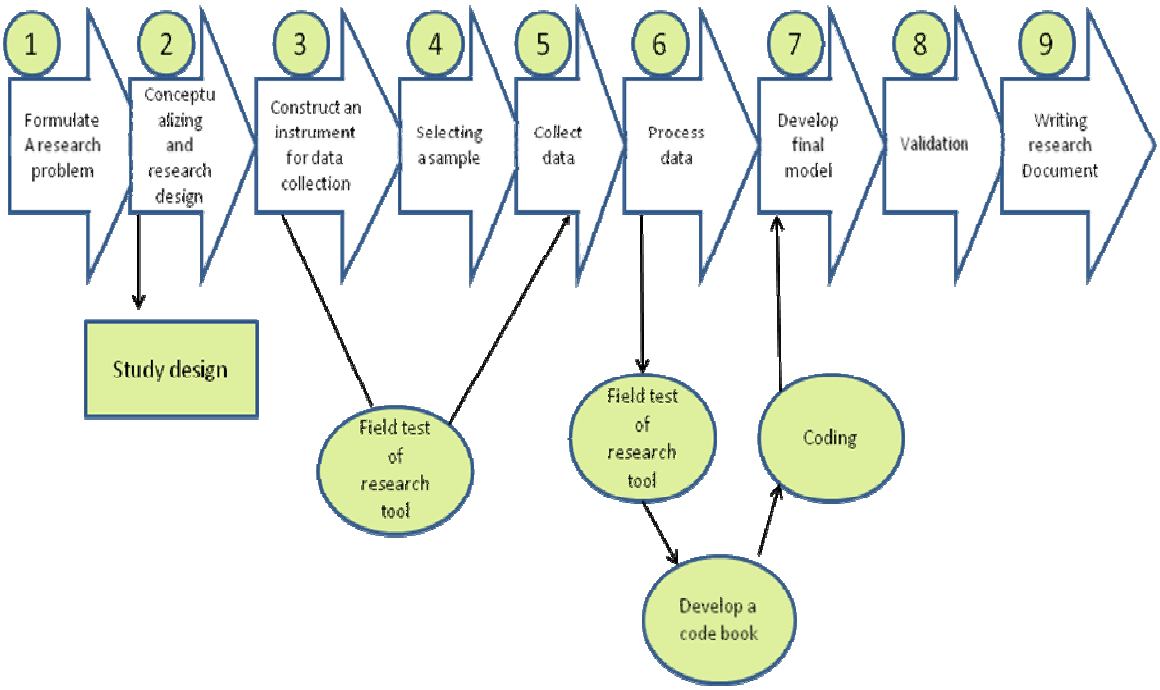


Figure 13: Adapted research methodology from: research methodology, a step by step guide for beginners

Source: (Kumar, R., 1996)

The research process was divided into nine (9) steps where each steps represented a phase in the research methodology for this thesis. The following explains the steps in details:

Step 1: Formulate a research problem

The research problem was formulated in the early stage of the research study for the thesis. The main objective of this research was to find a security model which allows any e-organisation or entity to exchange information with other entities seamlessly considering all the elements or factors which will hinder this communication or lower the trust of information sharing between these entities. The initial stage of the research problem was to address any e-organisation or e-entity and then it was narrowed to address the e-government departments only in order to find suitable case study. Dubai was selected as a case study due to its advancement in the e-government implementation in the region. Being the region of the author will assist in the data collection. The research problem was thought of as a security challenge and the author started to analyze what would be the best model or architecture developed for such a challenge. The author started to analyze the elements which can lower the trust of information sharing between the e-government departments. The output of this phase was the identification of the Dubai e-government 26 departments as the case study for the research.

Step 2: Conceptualizing and research design

During this stage, the author studied and reviewed the literature explaining the existing security models addressing policies and the security triad (confidentiality, integrity, availability) which act as the high level objectives of any security architecture or model. Different types of models were analyzed. Models addressing confidentiality or integrity only were such as BLP or Biba were analyzed. Social and human behavioural model and theories were searched to build the concept of the human aspect in the information security field. The author searched for models, theories, journals, and previous research addressing the elements and the security threats which may have a direct or indirect effect in blocking the inter government information sharing. Literature and models reviewed are explicitly explained in Chapter 2. The review of the literature led to different ideas on how to pursue constructing the new model. It revealed several key characteristics the new model will need to incorporate to be comprehensive such as the link between the security technologies and policies and the need of having strong training programmes of the security staff managing

the security infrastructure. It was established that the existing models and frameworks address one or two aspects of the information security architecture, not all, needed in any organisation. The majority of the literature was addressing technological security solutions or approaches to solve issues related to data integrity or confidentiality. These technological solutions were presented as architectures required or programmes to be installed in the IT infrastructure. The review presented the gap that there is no comprehensive model which addresses all the different aspects needed in any security programme.

Analysing the strength and weakness of literature models, the structure of the new model was designed to address five different aspects of any security programme or architecture; security technologies, security policies, security competencies, security operational and management, and the decision factors affecting the existence or absence of any of the previous security aspects.

The initial structure of the model and its five layers were the output of this phase. The model evolved from a pyramid to a matrix and finally to a periodic table shape reflecting all the layers and sub layers of it to be used and selected in the questionnaires.

Step 3: Constructing an instrument for data collection

One questionnaire was initially designed to collect data from the Dubai e-government. During the development process of the questionnaire, it became evident that there are two main communities which have a direct effect of the e-government operation in Dubai. These can be categorized to management and technical teams. This has led to consider the two dimensions of the questionnaire, management opinion on threats and security measures and technical opinion of the security measures and the layers of the model **(Figure 2)**. Both dimensions contribute to build a holistic view of the security programme for the government departments and achieve the objective of building a new security model. The first questionnaire was titled as questionnaire A and was sent to the heads of the government departments or their deputies. The questions of questionnaire A, were

addressing the need of information security programmes/architectures, types of e-services launched by the government departments, and the recognized internal and external threats. The objective of the questionnaire was to get the management perception on information security, confirm the need of a security model and identify the top internal and external threats recognized by the management of the government departments. The second type of questionnaire was titled as questionnaire B and it was targeting the group of recognised qualified security practitioners in Dubai. The questionnaire was addressing areas such as the internal and external threats recognized by the security practitioners, the rate of importance of each layer and its sub layers, the needed security measures in relation to the different types of e-services (informational, interactive, and transactional) and finally a correlation section which has given the security practitioners the chance to select or drop sub layers proposed to be part of the new model.

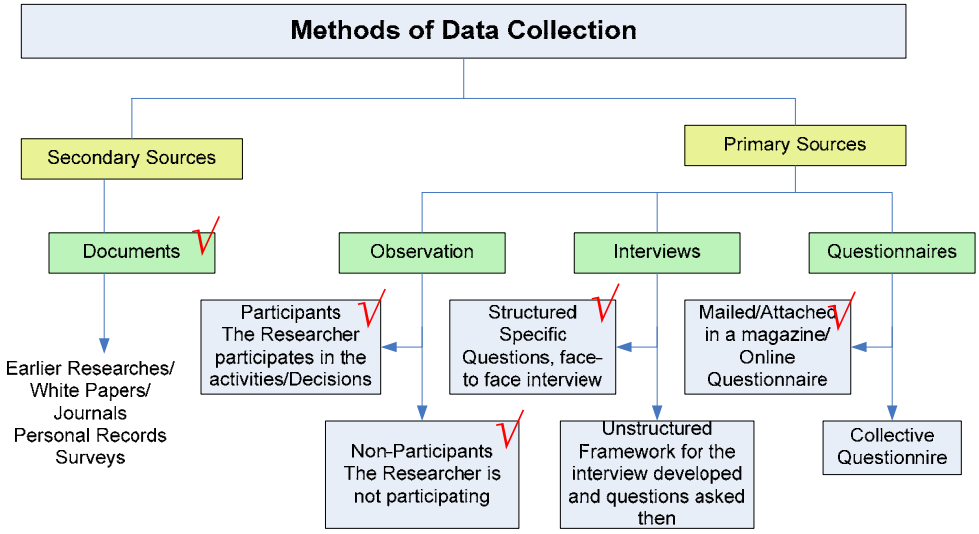


Figure 14: Position of the Selected Data Collection Method

Source: (Kumar, R., 1996)

√ ***Review of secondary resources***:

- Related research papers, journals, industrial white papers, and surveys were researched, collected, indexed, and reviewed by the author. The objective of this step was to have a good repository of all journals and conference proceeds addressing the topic of information security models, e-government security

needs, and the different security aspects which other researches discussed in the past.

- During the course of the research, the author had either read or skimmed through more than 400 journals, whitepapers, conference proceedings, and books. Only 250 references regarded useful to the research were indexed and documented.

√ ***Observation***:

- Participant: The author participated in the activities of the research such as recommending technologies, policies, and competencies which should exist in the e-government from his influence as a CIO of the largest conglomerate in the country and the region and being the first CISSP in the country. The author's organisation is also a key participant of the e-government initiative and having most of the layers of the new model implemented in his organisation will set a high threshold of a good security level.
- Non-Participant: The author acted as a non-participant of the research by observing the data collected from other managers and IT and security practitioners'. The different decisions on what to select in their organisations were recognized and analyzed.

√ ***Structured interviews***:

- Two questionnaires (A and B) were sent to the management and the security practitioners of the government departments with specific and direct questions related to the areas of research interest. A preliminary interview with the director of DEG was conducted to explain the purpose of the research and seek his opinion on the questionnaires and their objectives. Some of the heads of the departments did not have the chance to fill questionnaire and requested the author to fill them during their interviews. A total of 19 managers or heads of government departments participated in the data collection of questionnaire A and 16 top security practitioners participated in the data collection of questionnaire B.

√ ***Mailed/Online questionnaire***

- Both questionnaires A & B were sent to the appropriate participants. The participants were invited based on their management involvement in the e-government initiative, interaction with the e-government authority and its e-services, and based on their strong background on the e-government issues. The questionnaires were sent via email to them and the feedbacks were received through email. Due to the nature of this research and to abide to the research ethics by not jeopardizing the accuracy of the data, the questionnaires were sent directly to the participants and were not published on a website as it was planned to.

Both questionnaires A and B were developed as an output of this phase with different sets of questions addressed to the two categories of respondents (management and technical). The questionnaires were sent and assistance offered to clarify the questionnaires questions if needed.

Step 4: Selecting a sample

Pilot questionnaires were sent to 7 managers in the government departments and 7 security practitioners in Dubai. The pilot questionnaire process will be explained in detail in chapter 5 and 6. The main objectives of the pilot process were:

- Test the easiness of the survey process
- Get a feedback on the clarity of the questions
- Develop a preliminary overview on the possible answers based on the limited sample selected for this process.

The invited participants were asked to fill in feedback forms **(Appendix C)** on the questionnaires to give an overview on the overall questions asked, the language level, length and other aspects which might enhance the questionnaires prior to their deployment to the government departments and the larger sample of the security practitioners.

Once the pilot questionnaires were collected and the feedback was analyzed, the modifications on both questionnaires were made and finalized. The output of this phase was the well structured questionnaires ready to be deployed for the respondents.

Step 5: Collecting data

The questionnaires were sent and all participants were requested kindly to participate in the questionnaires through direct emails. After sending the questionnaires, the phase of data collection started. During the data collection phase, there has been delay in the response. This could not be avoided due to the following reasons:

- Most of the government departments' managers or heads who agreed to participate in the questionnaires had changed their roles and joined other departments and need longer time to confirm their feedbacks in the new organisation.
- The security practitioners had a strong overview of the e-government and the e-services but some of them were reluctant to answer due to the sensitivity of the subject or due to their abidance to the confidentiality agreements and policies they have signed with their organisations. This challenge was overcome by further direct requests sent to the heads of the government departments and the director of DEG to allow the security practitioners to participate in this questionnaire. It has been agreed that the data collected will be used only for the academic research purpose.

A total of a 4 months delay in the response was encountered and caused the data analysis phase to be put on hold. The final objective was achieved at the end and the maximum number of questionnaires were collected from the management participants (19 questionnaires-A collected, out of maximum possible of 26 government departments) and the technical team of e-government (16 questionnaires-B collected). The processing phase was all set to start.

Step 6: Processing data

The collected data from both questionnaires A & B was analyzed using Microsoft Excel for simple statistical analysis. The data was examined against the model built in order to identify areas of support and areas of anomalies where it can be researched further. The correlation part was conducted between different sections of the questionnaires in order to construct the final conclusion of the questionnaire results. The final analysis of the data was analyzed again against the initially proposed security model to confirm the need of the layers or to drop the layers or sub-layers which were found not required by the respondents of the questionnaires.

Step 7: Developing the final model

This stage of the research focused on processing the information which was collected from the questionnaires, compare the results with the initial conceptual model developed in the initial stage of the research, and confirm the layers which are used to construct the final model. There was a minor modification of the new model where the Fear, uncertainty, and doubt (FUD) sub layer of the decision layer was not found as an effective decision factor for the security model in the e-government. This modification was carried out to the structure of the model. The rest of the layers and sub layers were confirmed to be part of the new model based on the rates scored for each one of them. As a result of this stage, the final version of the model is presented in this thesis document.

Step 8: The validation phase

The three validation actions were carried out in parallel.

Action 1: Observation from the collected data and the analysis results has shown the confirmation of the layers initially constructed as part of the conceptual model in the early stage of the research. It also showed the strong interest of the government departments heads and security practitioners to have a common security model or reference which can be used as checklist for the security level and as a recommended comprehensive architecture for all the departments. This was observed from the answers of the both the

management and technical respondents. The technical respondents confirmed the need of most of the sub-layers representing security measures and the management respondents confirmed the existence of different types of threats which can only be mitigated through different aspects of security other the technological ones.

Action 2: The researcher set seven criteria for the success of the model. The seven criteria were extrapolated from Wood's book (Wood, C., 2005) and the guidelines of modelling presented by Lankhorst (Lankhorst, M. ,2005). The success criteria objective was to ensure the usability of the model in the future and identify any area which might affect the adoption of the model and rectify this through a modification on the layers or the sub-layers of the model.

Action 3: The final model was evaluated by the Head of the DEG authority to confirm its applicability and the possibility of adopting it in the future. The Head of the DEG is the only authorized position to enforce the usability of the model and has all the power to drop or modify any layer or sub-layer based on the operational needs of the e-government of Dubai. The outcome could be rejecting the whole model or part of it. Requesting an authority of the e-government to validate a security model independently from the data collected or the practitioners' professional opinion, is a way to counter researcher bias. The Head of DEG was requested to fill two forms (form 1 and 2) in order to confirm the seven success criteria set for the success of the model and the layers/sub-layers implemented in the new model. This activity has given the research more support and eliminated any possibility of the researcher bias. The final confirmation letter of the interest of the DEG in the new model is attached in **Appendix D.**

Step 9: Writing a research document

The research document was written in parallel to each step of the research process. The research document structure is explained in chapter 1 and it covers the literature reviews, findings from the data analysis, the structure of the new model, an explanation of each layer in the new model and the detailed validation process followed for this research.

3.5. Chapter summary

The main areas covered in the research methodology chapter are the scientific background of the research methodology, knowledge claims adopted, the implemented research processes, the methods of data collection, and the validation process followed during the construction of the thesis for the new security model.

The author used the post-positivism, constructivism, and the pragmatism knowledge claims. The research analysis of the data was using both qualitative and the quantitative research strategies. A research process adapted from Kumar's (Kumar, R., 1996) methodology was followed to achieve the research objectives. The qualitative and quantitative data analyses were applied on the data collected from both questionnaires. The qualitative analysis was mostly interpretive using the author's intuition (Robson, C., 2002) and it was mainly for the analysis of the human factors in selecting or rejecting security technologies, committing computer crimes (creating of information threats), and interactions with security systems which include technologies and policies. On the other hand, the quantitative analysis was applied to study security technologies implemented in the region, number of security incidents experienced and setting the rate of the importance for each layer and sub layer.

Chapter four: The five security layered-model using matrix representation

4.1. Introduction

Information security presents a lot of challenges and concerns to governmental and commercial organisations. Models are used as the best method for illustrating new concepts or architectures. Many models were analyzed to find out how comprehensive they are.

The objective of the new security model is to assist in visualizing the combination of different layers of security in order to come up with a mechanism of enhancing the security level of any e-enabled organisation but specifically in using the e-governments as the research case.

During the development process many papers were reviewed and an extensive research was conducted to confirm the need of each layer of the model. A threat analysis method is presented as the first part of this chapter. The author presents the concept of multi threats for a single e-service, the needs of having a model addressing these threats and an application of this concept over the e-university. This multi-threat concept can be considered as the foundation of the need of a multi layer model. In the second part of this chapter, the author argues why the five selected layers contribute to a good security programme. The author continues to explain the different layers and their sub layers. Recognizing the five layers necessary for any security programme and the sub layers has guided the author to build a graphical representation incorporating all these layers and sub layers. The matrix representation of the new model is presented in the last part of this chapter.

4.2. A multi-layer approach for threats classification and analysis on e-government services

To relate the security technologies proposed by the author with e-government security requirements, the organisational model for the security requirements for e-government services namely known as "e-gov-OFSR" has been reviewed. A good description was given in the literature about the model". Security requirements for e-government services such as e-university and e-voting were found as per Costas' analysis as (Lambrinoudakis, C., Gritzals, S., Dridi, F. and Pernul, G., 2003):

- System Availability
- Performance
- Management of privileges
- Authentication
- Integrity
- Logging
- Confidentiality
- Integrity
- Non-Repudiation
- Secure Storage

Many cases were studied which are stressing on the need of applying the right technologies in order to protect the e-government information resources. The case of "Fluxay" and how it was used to intrude the computers using dictionary attack method by scanning for standard ports such as port 79 (Finger), 2049 (NFS), 137 (NetBIOS), etc (Farn, K., Lin, S. and Fung, A. R., 2004) indicated the effect of a technical programme on the corporate infrastructure. Security technologies will play a major role in protecting and mitigating such risks. Though, applying the necessary technologies is not effective enough. The selection of the appropriate technology is also crucial to the security architecture of the organisation. Security countermeasures protecting infrastructure only ignore the fact that most of attacks coming from the application layers through exploits.

The objective of new approach is to turn the threat auditing and analysis process into a detailed 360 degrees analytical process which addresses all the threats related to an e-service. An effective information security programme must consider both IT and non IT related issues (Arthur, J. C. and Quey-Jen, Y., 2006). This analytical process can be part of

the initial thinking and planning of an e-service. The new threats analysis method can be considered as a tool to think about the threats of a new e-service and a method which can be used by security officers and practitioners to highlight a risk and manage its effect.
In the e-services threats section the well known equations of calculating threats and total risks are discussed to illustrate the different element affecting the equation.

4.2.1. Threats impact on online services

An e-service represents a way to allow customers, citizens, and corporations to interact with the service provider over the Internet using a backend support infrastructure of information assets and resources. The information assets and resources have become a source of risk when they are vulnerable to threats as per Rainer and Snyder (Rainer, R. K., Jr, Snyder, C. A. and Carr, H. H., 1991). Threats on the e-services are the same threats of any IT system and can be categorized as:
- Natural threats described by terms such as 'Act of God' or 'force majeure' that include for example, unforeseen events like a flood or an earthquake.
- Accidental threats caused by factors such as missing out in a plan or a procedure.
- Intentional threats caused directly or indirectly by staff who are involved in operation like the deletion of data with intent to transfer funds (Lindup, K. R. A., 1995).

Enterprises tend to solve their Information Systems (IS) security threats with different technical solutions only. Ignoring the potential crisis which might be caused by managerial controls or any human factors increases the impact level on the online services**.** Icove and Vanstorch (Icove, D. C. and Vonstorch, K., 1999) have developed a categorization of threats to IS based on the type of the involved assets. Seven categories were set for the information threats and each category has different attributes:

1. Software
2. Hardware
3. Data
4. Network
5. Physical
6. Personnel
7. Administration

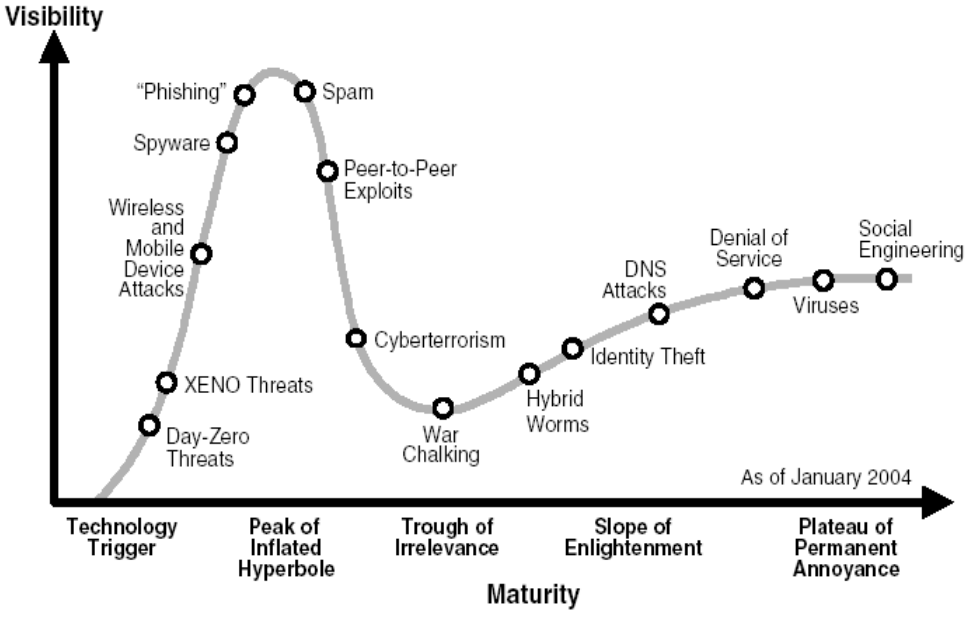
The categorization only simplifies the analysis process of the different facets of the threat. Conducting a detailed analysis on the total number of threats of an e-service going through different process, a set of threats (T) will need to be considered comprising all seven subsets mentioned in Icove paper (Icove, D. C. and Vonstorch, K., 1999) in addition to other threats which may be identified during the analysis process.

Analyzing an e-service is not restricted to the types of the subsets of threats which can contribute to the risk of the delivery failure. There are other dimensions which can be considered for any online service such as the source of threat, the perpetrator types, intention, and the consequences. This approach of analysis was developed by Loch et al (Loch, k. D., Carr, H. H. and Warkentin, M. E., 1992).

Knowing the source of the threat will assist in developing the appropriate security operational strategy and increase the probability of the service availability. Placing the right countermeasure will depend on the knowledge of the source of threat and whether it is within the organisation or it is an external one. The types of perpetrators can be human or non-human. Performing in depth analysis on the type of the perpetrator, background, profile, and motives assist in putting the right security system in place. The dimension of intention is critical to the operation of information technology and the supporting infrastructure to the online service in general. Being able to avoid the accidental errors through strict change management procedures and the enablement of audit trails will filter the incidents which were caused through malicious actions. This will enable the security officers to set the appropriate measures to reduce the likelihood of having an error that can breach the whole security programme. The last dimension is the consequences of any security attack. Consequences vary from disclosure of classified information to a total denial of service to the online service. Each consequence has a cost and a method to prevent. The cost of the consequence is determined as a loss to the organisation which can be minimized or totally eliminated by placing the appropriate security measure which has a cost which must be incurred by the organisation.

The e-service is only a product generated out of an IT infrastructure owned by the service provider or outsourced through a third party. The e-service includes supporting technology, integrated processes, and support staff. The security threats on any of the key elements of the online service will have a direct impact on the service and its users.

Each year we get acquainted with different cybercrime threats either through literature or reports of incidents. The growth of threats continues **(Figure 15)** along with the wide spread of the Internet. The diagram below highlights some of the threats identified and their growth over the coming years. Gartner anticipated that "The threat environment remains scary, with new threat types such as Phishing, adware, spyware and identity theft" (Schroder, N., 2005). The growth of threats indicates that more dimensions of threats will be faced. Dimensions which might need different countermeasures of security to mitigate them. The nature of these countermeasures might be technological or non technological.



XENO: Extended Enterprise Network Oversees

(Wheatman, V., 2005),

Figure 15: Security threats – Gartner

Swiderski (Swiderski, F. Snyder, W.C, 2004) argued that threats of a single application can vary from malicious attacks to unauthorized access. Considering the fact that e-services are generated from business applications and knowing that there are multiple threats for each single application, the author agrees with Swiderski's concept which justifies the need of multiple layers security model. The applications threats analyzed by Swiderski (Swiderski, F. Snyder, W.C, 2004) are:

- Malicious SQL Data in User Input
- Disclosure of Login Information
- Session ID Theft
- User Data Disclosure
- Direct Access to the Database
- Rate Quote Tampering
- Unauthorized Use of Insurance Agent Web pages
- Blocking e-mail Notification
- User Data Tampering
- Blocking New Quote Request Notification
- Account Deletion
- Crashing the website
- Accessing the site without valid credentials.

The above threats represent threats on the technological side of application management (Swiderski, F. and Snyder, W. C., 2004). An e-service is provided through an end-to-end automated process or it is an automation of a process interrupted by a manual procedure which needs direct human intervention. The threat of an e-service might be generated by a technological flaw, lack of good security, lack of knowledge in a security threat of how to handle a threat, no clear and strict operational procedure, or as simple as selecting the wrong timing to launch the service. The author's view is that security threats are built up and constructed in different layers or levels for any e-service. It can be agreed that the severity of the threat on any e-service will always be higher if the threat occurs as a combination of technology, competency, policy, bad operation, and wrong decisions.

A threat is a combination of the capability of the perpetrator and the intention of his action as indicated in **Equation 1 (Table 12)**.

Table 12: Threats and capability table

Threat = Capability + Intent (Equation 1)
Capability = Access + Skill (Equation 2)

A capability element is directly related to the level of competency of the IT staff or the security officers responsible for the infrastructure. A threat (Tudor, J. K., 2002) is a more limited component of risk. As a matter of fact, a threat that has no vulnerability creates no risk. Some security analysts define threat as potential danger to information or an information system (Nichols, R. K., Ryan, D. J. and Ryan, J. J. C., 2000), (Tiwana, A., 1999). A threat can be mathematically calculated as illustrated in **Table 12** only if you can calculate its components**.** Considering all the possible threats to an e-service in the early stage will reduce the effect of the vulnerabilities. In addition, as indicated in **Table 12** having strong security competency will minimize the capability of the attacker (-capability) which will reduce the value of the threat in **Equation (1)**. Having both a strong security competency and technologies will minimize the capability value further and therefore it will reduce the threat value.

The standard method of calculating the level of risk (Tudor, J. K., 2002) is multiplying the threat level by vulnerability weight, divided by the level of countermeasures available to protect the infrastructure and multiplied by the impact **(Equation 3 in Table 13)**. This method depends highly on knowing vulnerabilities and impacts on an asset. It relies on our up to date knowledge on these vulnerabilities and our experience in studying different levels of impact. The two equations below reflect the standard method of calculating risk.

Table 13: Level of risk and total risk formula

Level of Risk = ((Threat × Vulnerability)/Countermeasures) × Impact (Equation 3)
Total Risk = Vulnerability + Threats + Asset Value (Equation 4) (Finne, T., 1996)

4.2.2. Towards a holistic model for e-services security

Based on the review of academic and industrial literature, a holistic approach that could be used to analyse threats of e-services offered by e-governments was not found. Most of the literature studied emphasised the challenges of e-government through the infrastructure protection alone (Smith, D. A. and Garton, P. R., 1989). There is no doubt that the approach of the infrastructure protection will mitigate some of the risks to e-services, but it will not be sufficient to counter all threats. E-services are not always supported end to end by fully automated processes, nor are offered through a common technological infrastructure. The security policies and procedures might not be common for all the e-services offered and the supporting staff might have different levels of competencies. In addition, most of the published approaches considered the impact of threats on different types of services safeguards including physical, procedural, and computer/network security. The e-services can be provided by a single application or multiple business applications. The process of launching an e-service might have a high dependency on the reliability of the technology, the need of developing special security policies related to the e-service, and the availability of competent support staff and the operational procedures. The following are the essential security levels required for e-services as observed from the literatures reviewed in chapter two:

- **A secure technical infrastructure**

  Security technologies have important role in securing the systems and applications supporting the e-services. Technologies such as Intrusion Detection, Antivirus (Schneier, B., 2004), Cryptography (Schneier, B., 1996), VPN (Carroll ,1996), Digital Signature (Schneier, B., 2001) and security protocol (Brewer, D. F. C. and Nash, M. J., 1989), contribute to the success of the e-services by providing the users high trust. Not having all or some of the security measures will have a negative impact and can be considered as a threat on the e-service.

- **Security policy related to the e-service**

  Security policies is a pillar in the security system of any organisation. The security policy is the organisation specific law. It allows employees to know what are the permitted actions to conduct and what is considered as a misconduct as per the organisationrules and regulations (Wood, C. C., 1999). Having a bullet proof security policy will assist the e-enabled organisation to mitigate the threat of internal malicious acts (Kesh, S., Ramanujan, S. and Nerur, S., 2002), (Siponen, M. T., 2001), (Wood, C. C., 1999). Lindup mentioned in his paper that there are several types of security policies which can be implemented in any organisation. An organisation can implement a system security policy, product security policy, community security policy, and a corporate information security policy (Lindup, K. R. A., 1995). Lacking the appropriate security policies or the enforcement of them can be considered as a threat on the e-services. Since the security policy document is made up of groups of policies related to different functions, missing a sub policy can be considered a threat which may compromise the overall security of the e-service.

- **Competent security team and officer**.

  Competency of the staff is obviously a strong requirement of any security system. Having a strong dependency on the staff who are not competent to run the security programme or maintain it will put the overall security system at great risk (Kesh, S., Ramanujan, S. and Nerur, S., 2002), (Gottfredon, M. and Hirschi, T., 1990).

- **Secure operational and management procedures**

  The way security operates is what sets the distinction between a successful security programme and a failure one. A solid security programme will have incident response process, security operational procedure, and all the management tools necessary. The operation and management of the security programme must cover the protection, detection, and the response (Schneier, B., 2001), (Zadeh, L. A., 2000).

- **A systematic method of taking a decision**

  All aforementioned security levels are essential to the success of launching an e-service and the enhancement of the usability of the e-services by the citizens. The time of the launch, method of launching, and the content of the e-service are all factors which need to be considered by the management of the DEG authority. Launching an e-service in the wrong time or allowing an e-service to be launched while the essential security criteria are not met is a threat on the e-service. Setting priorities of the security measures is the key of making the right decision for an e-service.

Figure 16 simplifies the idea of having groups of threats related to each level (technological, security policies, competencies, operational and management procedures, decision impact) of the security programme of e-services. Threats can be related to flaws in the system or policy or due to a weak security operation procedure and security competency. Taking into consideration the impact of the management decision, the threat of taking the wrong decision was also considered. The number of threats varies from one e-service to another and the number of the levels related to the security programme can also increase. It is therefore clear that the vertical axis of the model (the Security levels) can expand to (n) number and the same applies to the horizontal axis (Threats of each level) **(Figure 16)**.

4.2.3. Evaluating the total threat

Simplistically, the total threat value may be considered as sum of probability of the threat in each level for an e-service. Safeguards have to be set in each level in order to reduce the threats associated with it.

From the four equations in Section 4.2.1, then the threat value of each level is:

T(i)= T1 + T2 + T3 + T4,…Tn. This indeed will have a direct impact on the level of risk formula and total Risk formula as mentioned below:

Level of Risk = (($\sum_{i=1}^{n} T(i)$ **x Vulnerability)/Countermeasures) x Impact**

Total Risk = **Vulnerability x** $\sum_{i=1}^{n} T(i)$ **x Threats x Asset Value**

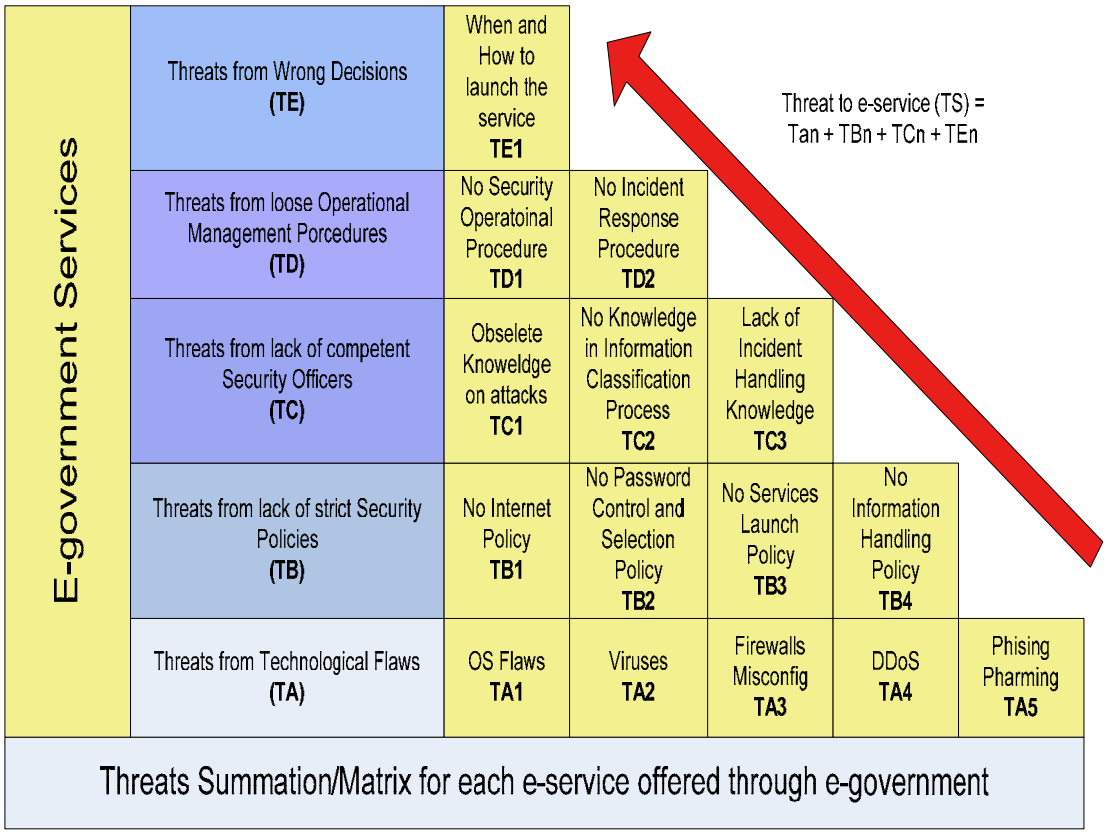


Figure 16: Threats summation matrix

4.2.4. Illustration using e-university Service

Since the e-university service was presented in the Lambrinoudakis framework (Lambrinoudakis, C., Gritzals, S., Dridi, F. and Pernul, G., 2003) as one of the key e-services, this is used to illustrate the use of the multi-layer model. Each layer/level needed for the e-services security has its requirements whether they are technical or non technical (procedural). The approach of analysing the various threats of a single e-service adopted in this research is shown in **Figure 17** and explained in **Table 14**. The threats shown in Table 10 are presented for illustration purpose and not representing all the threats which can be found on the e-service. By applying this comprehensive method of looking at all relevant

threats, accuracy on the real impact of the e-service threat can be achieved and the countermeasure(s) can be applied. The output from this analysis will assist the e-service to be launched with confidence and increase the trust and usability of the users whether they are government organisations or citizens **(Table 10)**.

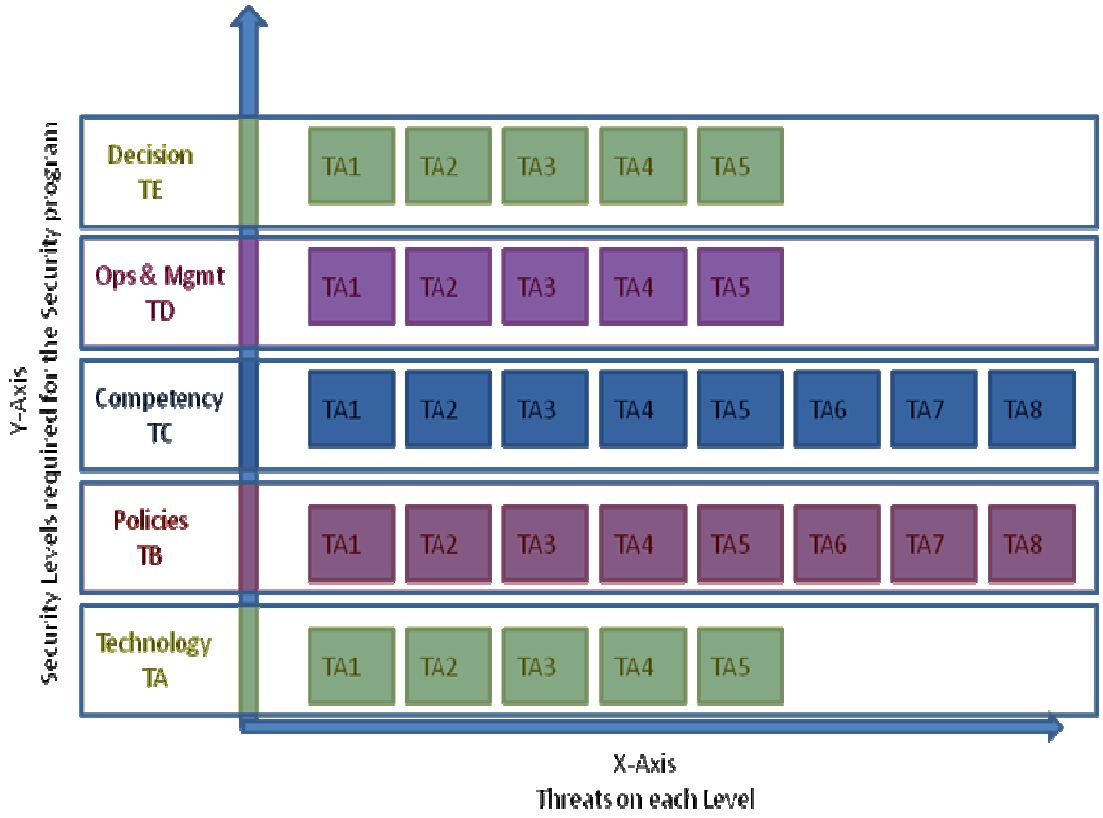


Figure 17: e-University threats analysis

Table 14: Application of multi threats concept on e-university

Level	Requirement	Threats
Technology **(TA)**	• Networking Infrastructure • Security Infrastructure Special application for e-university business requirements such as setting curriculum, posting classes, scheduling, accepting applications, workflow for admission, etc	• Viruses • Denial of Services • SYN Flood or Network based attacks • Application/OS flaws • Wrong Scheduling or admission due to intentional or unintentional error**.**
Policy **(TB)**	• The IT and security policy on what to post and how to use the e-university infrastructure by supporting staff or public users. A good example is how users can post a course through approval workflow, how students can apply and how applications get approved or rejected	• Self defeated policies which allow intruders to gain access. • Inapplicable and undoable policies which can't be used in the organisation. The organisation will have the perception of having a policy in place but at the same time the policy can't be practiced. • Disconnected procedures from policies. Procedures must spell out the policies and if they are in place but not aligned to the security policy, they may become an indirect threat. Procedures may encourage wrong practices violating the security policy. • Unclear IT policies
Competency **(TC)**	• Operational Knowledge: for the supporting staff. • Users Knowledge: for the users of the Infrastructure • Security Knowledge: How to protect the infrastructure	• Incapable staff managing the sensitive infrastructure • Relying on third parties in every aspect of operational needs. • non-unpadded and incapable security practitioners • having less hacking knowledge than the students who are the key users to the service.

Operational **(TD)**	• Operational Procedures on how to manage the infrastructure • Security Procedures for how to protect the infrastructure and how to respond to a threat	• Unpractical operational procedures. • No backup procedures. • No change management. • No security procedures
Decision **(TE)**	• When to launch the service • How to select the appropriate infrastructure • When to shut down the service if a threat is confirmed • Who has higher priority, security or business requirements?	• Launching the service during a peak of attacks on the Internet. • Selecting a weak application which has no security features due to cost reduction. • Launching the service due to business requirements without giving security ample time to mitigate any risk.

Since most of the e-services require more than a single step to launch, the approach discussed in this section and illustrated in Table 15 can be applicable to government authority and its affiliates offering similar e-services. The method of analysis is not limited to e-government services only. A column of numeric threats' values can be added if a quantified analysis is needed to give each e-service a value from threats perspective. The threats analysis can be based on what's available for the e-service and what's missing in order to make it more secure. In addition, the above table can be used as a checklist for each e-service and can determine the priority of launch for each e-service.

Adopting the above method in analyzing threats related to e-services will lead to the development of a comprehensive risk analysis to address all threats related to all levels and aspects. The need for new models was highlighted by many researchers to address all aspects of security (Schumacher, H. J. and Gosh, S., 1998). The key part in developing different models is to identify the threats of each level and how to set the proper countermeasure all linked in one security model.

A checklist for planning a launch of any new e-service is illustrated in **Table 15** where each layer supporting the e-services have some security measures to be placed, a list of threats affecting the layer, and a weighting rate on each threat. This table can be used to calculate the total value of the threats by the average of all layers threats level.

Table 15: e-services lunching checklists

Security Level	Requirement	Recognized Threats	Weight of each Threat Total of each level = 100
Technology TA	RA1--------- RA5---------- RA2--------- RA6---------- RA3--------- RA7---------- RA4--------- RA8----------	TA1--------- TA5---------- TA2--------- TA6---------- TA3--------- TA7---------- TA4--------- TA8----------	WTA1--------- WTA5--------- WTA2--------- WTA6--------- WTA3--------- WTA7--------- WTA4--------- WTA8---------
Security Policy TB	RB1--------- RB5---------- RB2--------- RB6---------- RB3--------- RB7---------- RB4--------- RB8----------	TB1--------- TB5---------- TB2--------- TB6---------- TB3--------- TB7---------- TB4--------- TB8----------	WTB1--------- WTB5--------- WTB2--------- WTB6--------- WTB3--------- WTB7--------- WTB4--------- WTB8---------
Security Competency TC	RC1--------- RC5---------- RC2--------- RC6---------- RC3--------- RC7---------- RC4--------- RC8----------	TC1--------- TC5---------- TC2--------- TC6---------- TC3--------- TC7---------- TC4--------- TC8----------	WTC1--------- WTC5--------- WTC2--------- WTC6--------- WTC3--------- WTC7--------- WTC4--------- WTC8---------
Security Operation and Management TD	RD1--------- RD5---------- RD2--------- RD6---------- RD3--------- RD7---------- RD4--------- RD8----------	TD1--------- TD5---------- TD2--------- TD6---------- TD3--------- TD7---------- TD4--------- TD8----------	WTD1--------- WTD5--------- WTD2--------- WTD6--------- WTD3--------- WTD7--------- WTD4--------- WTD8---------
Decision TE	RE1--------- RE5---------- RE2--------- RE6---------- RE3--------- RE7---------- RE4--------- RE8----------	TE1--------- TE5---------- TE2--------- TE6---------- TE3--------- TE7---------- TE4--------- TE8----------	WTE1--------- WTE5--------- WTE2--------- WTE6--------- WTE3--------- WTE7--------- WTE4--------- WTE8---------
Total Value of Threat			Average of each level/Number of Levels

This new approach of identifying the total value of threats and analyzing all threats related to the e-service integrates the key concepts from the models reported earlier.

Adding the policies, competencies, operation and management, and the decision levels allows the security practitioner to consider a comprehensive range of threats prior to launching any e-service. The decision level of the security programme is a major decision to launch a service or not. It also affects the other levels or layers by enforcing a security

policy, change of a technology, develop a new competency, and modify the security operation and management procedure.

4.3. The layers of new e-government security model

Having more than one dimension or layer of any model gives the model a robust structure and a better success rate in preventing organisations from various categories of threats related to a single or multiple e-services. Each layer will mitigate group of threats related to an e-services. The technology layer for example will address all the technological threats while the policy and competency layers will address the threats on an e-service related to the human aspect. The challenge is how to construct or build the academic support for the different layers/dimensions required to be in one model. A literature review and an extensive research were conducted in order to prove the necessity of the layers discussed in this chapter. The research continued to find out the sub layers of each layer needed in any information security system or programme. The purpose of the research is to establish any sub layer which may be used in the future in constructing a comprehensive model which will consist of multiple layers that complement each other. There are five areas the author argues that contribute in building strong security architecture and system **(Figure 18)**. It can be noticed that each area is a broad concept of the information security field and can be broken to smaller subsets which collectively contribute to the positive effect of the security programme of any organisation. The five layers were selected based on the author's industrial experience and reported in academic literature on their importance as a part of any strong security programme. The layers as depicted in **Figure 19** are, the technology layer, the policy layer, the competency layer, the operational and management layer, and the decision layer. The layers were constructed from the bottom to the top based on the importance of the layers, the frequency of their implementation in organisations, and how they complement each other.

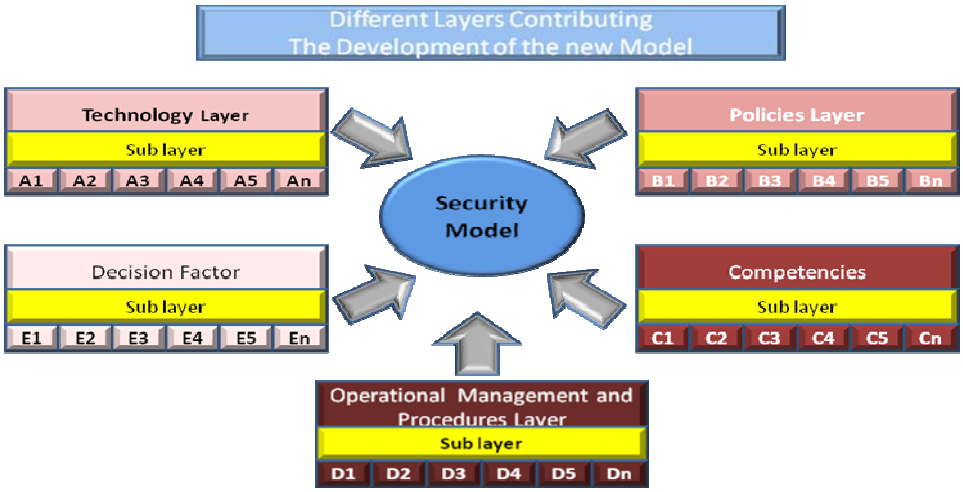


Figure 18: The different five layers building the new security model

The idea of the new model is to come up with a comprehensive method in reviewing the security needs and requirements for any e-enabled organisation in order to allow or not to allow the interchange of information with other e-organisations. This information sharing or interchanging can be part of an e-business or an e-government process. To ease the visualization from a non technical user point of view, the new conceptual model is expressed in a pyramid representation as illustrated in **Figure 19.**

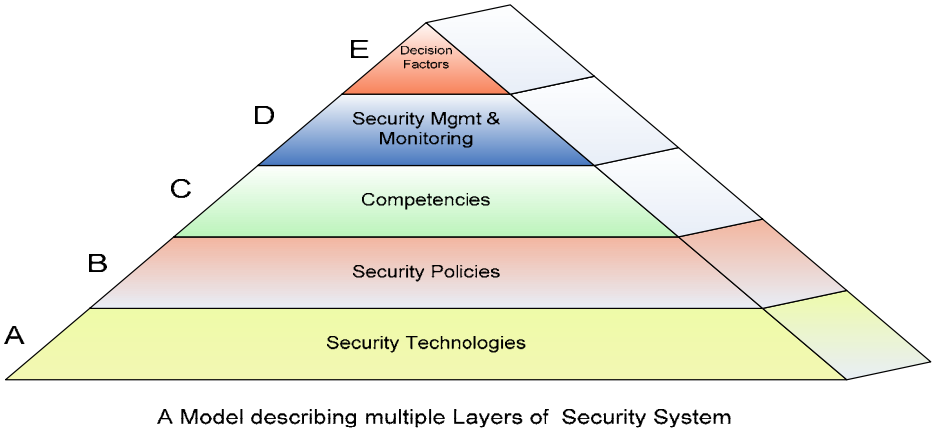


Figure 19: Multi layers model

Since each layer has more than one sub layer and to make the structure coherent and more understandable, the model evolved into a matrix oriented structure (**Figure 20)** where each layer was divided into multiple sub layers. The division of these layers into sub layers (referred as cells) gives the new model a flexibility to expand into n-number of cells based on the need of the organisation.

Supporting literature address the need of technologies, policies, awareness, and the right management decision in order to come up with a strong security programme. The key goal of the scope of work of this research is how to position the main security aspects in a single model to represent security architecture with multiple layers and cells that complement each other in order to reach a better level of security for any organisation. The structure of the model with the five main aspects of security (technology, policy, competency, operation and management, decision factors) is applicable to any organisation with a possibility of changing the sub layers based on the security trends in the market and the organisationneeds. Moreover, the number of the layers might change based on other researches or literature reviews which will be done in the future. The concept of having x-number of layers with y-numbers of cells in each layer and the combination of all to come up with a better level of security is what the author considers as "new model" and a "new approach".

4.4. Selection criteria of the new model sub layers

The following criteria used for the selection of any sub layer in the model:

1. The sub layer must address a security requirement in the government department.
2. The sub layer must be recognized and implemented by a minimum of five (5) of the security vendors and service providers.
3. The sub layer must be reviewed and approved by a government security committee consisting of members representing over 70% of the total number of the government departments.
4. The sub layer must not conflict or be redundant of other sub layers in the new model.
5. The sub layer must have at least two other sub layers to support it but a security policy sub layer must be one of the two.

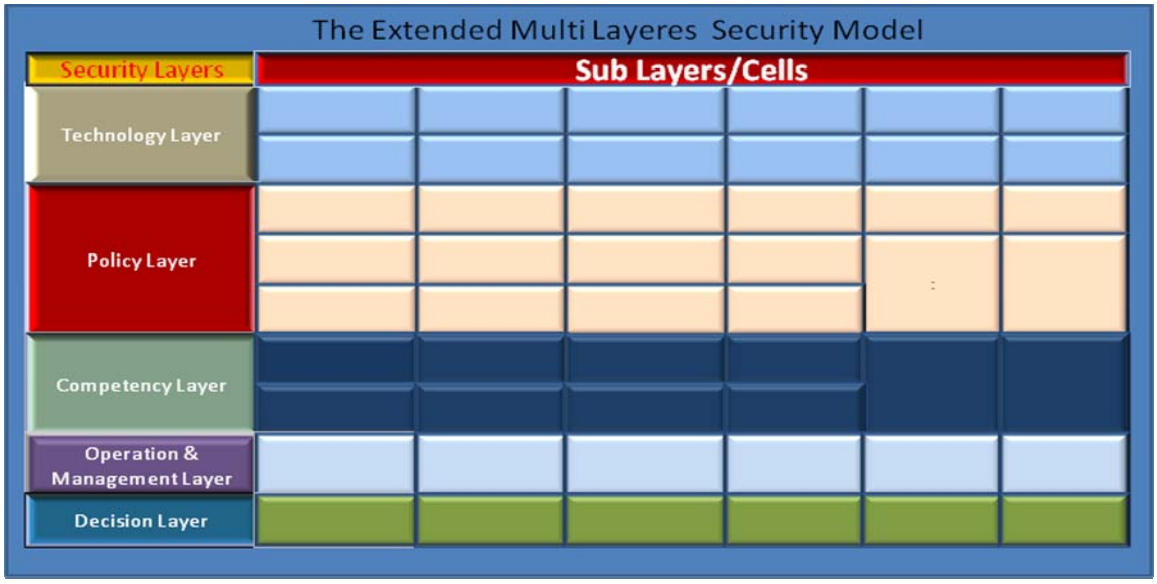


Figure 20: The matrix oriented model

4.5. The security technologies layer

In many journals and articles, authors tend to define security technologies very well. The approach of providing an extensive knowledge on security technologies can be part of the awareness strategy but not enough to justify the inclusion of the security technologies in the organisation. A brief description is provided on the need of these technologies in any organisation and how to use them. As part of the research work conducted for this thesis, all security technologies known in the security field were considered as the initial stage. A categorization was made to combine the security technologies into groups where each group represents a security measure. For example, there are many types of firewalls available in the market. Some of them are operating in the application layer while others are in the network and transport layers (stateful inspection filtering) of the networking OSI seven layers (physical, data link, network, transport, session, presentation, application). Regardless of the modus operandi of the firewalls, they all can be categorized as logical access control which can represent a single sub layer of the new model. The same analogy was performed to the other technologies which led to 12 sub layers required to build a strong technology layer. The categorization was derived from the literature reviewed for this layer. The main sub layers found out of the review process are:

4.5.1. Access Control

Access control is a mechanism of controlling entry to any perimeter or a boundary. The control might be through prevention of unauthorized entries, monitoring authorized entries, or limiting entries through predefined rules and roles. As per the latest CSI computer crime and security survey, insider abuse network access or email has a deeper impact (59% of the survey respondents) more than viruses spread (52% of the survey respondents) (Richardson, R., 2007). Organisations will need to place access control where entry can't be provided to public and where assets are categorized to be mission critical to the organisation. The assets can be in format of systems, information resources in any manifestation or an environment where confidential discussions can be held. All organisations will need some level of access control to its offices, computer centres, or even staff areas. An e-government model is as an example of an e-enabled organisation and will have a strong requirement of access control to the computer centres where governmental data are held, offices of the staff handling the e-government services, and even cables carrying the data between governmental departments.

4.5.2. Intrusion detection and prevention

Intrusion detection system (IDS) and prevention system (IPS) are becoming key elements of any security infrastructure to ensure the safety of systems and networks (Wheeler, P. and Fulp, E., 2007). Intrusion Detection and Prevention are technologies that rely on either statistical and signature databases or on the behaviour of the network through Artificial Intelligence (AI) agents. Both technologies sent alerts to the authorized staff whenever there is an attack symptom. The accuracy of the IDS is measured on how to reduce the false positives and false negatives alerts. False positives are legitimate user behaviour that is detected by IDS as a malicious act while false negatives are intrusive behaviour interpreted by the IDS as normal behaviour (Biermann, E., Cloete, E. and Venter, L. M., 2001). Organisations providing external access to information resources or even connected to the Internet will find the technology of IDS or IPS imperative in order to be alert on attacks or possible attempts of intrusion. Many organisations nowadays realize that having a host

based IDS and monitoring activities are imperative. The monitoring procedure is pushed all the way to the auditing logs of the system (Cole, E., 2002).

4.5.3. Anti-virus & malicious codes scanners

Since 1984 viruses were spreading in the internet causing users a great deal of inconvenience and lowering the trust on the Internet and the computer systems (Cohen, F. B., 1992). On the other hand, antivirus and malicious codes scanners are tools which perform a health check of the technical body of the organisation and prevent viruses from being transferred through multiple channels and can cause serious harm to the organisation. Even if the organisation is well protected through anti viruses systems, the infection might still take place through flaws in the operating system, or a service port which a worm is scanning for. Viruses are considered the highest threat for organisations nowadays (Doughty, K., 2003). Having antivirus systems distributed in the organisation will definitely lower the risk of serious damage or loss to the information resources. Completing the antivirus solution with users alertness will prevent the spread of computer viruses (Qasem, I. R., Yaghi, H. M. and Hubbell, J. N., 1990). Due to the need of exchanging files and information between the e-government departments, the lack of having a proper antivirus solution with a full synchronization of viruses updates, the probability of having an e-government department getting infected with viruses from another department due to unsecure file exchange over the Internet is high.

4.5.4. Authentication and passwords

The demand of protecting the privacy and the integrity of corporate information has been increasing recently (Yixin, J., Chuang, L. and Zhangxi, T., 2003). Since information systems are the heart of any organisation and the mean of users access to the e-services, authenticating the identity of the user is one of the fundamental controls an organisation needs to put in place (Zviran, M. and Haqa, W., J., 1990). It was stated by Zviran that having simple passwords is a risk as they can easily be guessed. A good mechanism of elevating the level of security was referred as the 3-factors security by Kurtz (Kurtz, R. L. and Vines, R. D., 2002). The concept of the 3-factors security is simple. Users get

authenticated through their identification which can be something that they know and keep as a secret (first factor) or something that they have (second factor) or something that is part of them (third factor). The first factor is usually a password which a user will know and hide. The second factor is a token that a user will have always. The third factor can be part of the user's body use as a mean of authentication such as eye-iris, retina, fingerprint, face geometry, etc. Combination the three factors together the authentication becomes more accurate and hard to be breached. "Authentication is the process of positively verifying the identity of a user in a computer system" (O'Gorman, L., 2003), It definitely plays a major role in elevating the trust of users in the computer system and the services launched over the Internet and it needs to be part of the government departments security architecture or model.

4.5.5. Files integrity checks

Securing information resources from external or internal attacks doesn't stop at preventing unauthorized access or exposure to information. Most of the time security breaches happen with motive of a cyber crime. The motive might be stealing information, destroying data, or hiding facts which we know as unauthorized alteration of data. Data modification of a government department or any organisation might result a great loss for organisations relay on data storage (Tomonori, F. and Masanori, O., 2003). The perpetrators can be internal such as storage device admin staff or external attackers as Tomonori stated. The attack tactics can be direct attempts of intrusion or planting undetected viruses to achieve the objective. The mission of the viruses or the malicious codes is to copy information and send it directly to the attacker. Some viruses can be embedded deeply in the system and remain undetected for a long time (Cohen, F. B., 1992). Having undetected viruses jeopardize the integrity of the government information stored data in a standard format within files in systems (Mckosky, R. A., 1990). These files are kept in either one system or distributed among group of systems. Providing availability and confidentiality for these files can be achieved through well known and standard security measures. The challenge really gets raised when integrity is one of the main security factors required in any organisation. Integrity check is not commonly used and sometimes is overlooked by

security practitioners due to the lack of good tools and mechanism in the organisation. Different tools can be used to ensure the data integrity such as digital signatures, certificates or hashing mechanism (Jaeger, T. and Rubin, A. D., 1996). E-governments rely on transacting data with high integrity. A breach in the integrity of the citizens' data can cause a direct disaster if the data is related to medical, personal, or application to governmental service.

4.5.6. Cryptography

Cryptography is the art of hiding information from those who are not authorized to view it (McClure, S., Scambray, J. and Kurtz, G., 2002). The need of cryptography got raised when the world discovered the man-in-middle attack from hackers and cyber-terrorist. Transacting data over the Internet in clear text is becoming a source of fear for many individuals, companies, and countries. The art of cryptography doesn't provide only with confidentiality but also with authentication when public key cryptography systems are applied. E-commerce which is a main pillar in any e-government relies heavily on cryptography. It is known in the security field that cryptography solves problems that involve secrecy, authentication and integrity by using it in different methods (Schneier, B., 1996).

In today's virtual world, most of the e-services involve financial transactions, business and private information sharing, and high level of trust between data exchange participants. Cryptography contributes highly in the elevation of trust of any e-service operation.

4.5.7. Virtual private network (VPN)

The acronym of VPN is becoming very popular in the business world. Executives require it in their laptops and during their business trips. They understand the need of it since it adds more convenience to them through direct and secure connection to the corporate information resources. "Global accesses, marketing research, selling, data collecting and supporting customers are but a few of the requests placed upon ISPs by their business customers" (Brown, S., 2001). VPN will play a major role in providing the staff working in

supporting the e-government a mean of extending support to the infrastructure virtually, extend the work environment to the homes, and make the government information resources accessible to authorized users.

4.5.8. Vulnerability scanning tools

Vulnerability scanners are becoming a must have in any security department trying to be in the proactive arena. Knowing the vulnerabilities in any system, network, or application can add value to the security programme for the organisation. Scanning the vulnerability needs to happen from two directions; the internal and the external (Richardson, R., 2007). E-governments will need to have scanners and tools for scanning the vulnerabilities and a team to analyze the output of these scanners. Having ethical hackers within the organisation can be considered as a form of having human based vulnerability scanners.

4.5.9. Digital signature and digital certificates

"A signature or multiple signatures on the paper guarantee its authenticity" (Atreya, M., Hammond, B., Paine, S., Starrett, P. and Wu, S., 2002). The digital signature is a mechanism to provide an authentication on a transaction to provide its legality and authentication. It may be used for payment authorization, acknowledgment of receiving a service or for any verification of information related to the customer. E-governments and with no doubt will need the digital signature to obtain authenticity, verification, or authorization from the customers. Digital Certificates on the other hand are mechanisms and are issued by trusted third parties known as Certificate Authorities (CAs) (Tiwana, A., 1999). A lot of technologist use the two terms interchangeably while they both have different meaning and purpose of usage. The main purpose of this technology is to become a main method of use in the electronic transactions in e-government services without being forgeable (King, C. M., Dalton, C. E. and Osmanoglu, T. E., 2001).

4.5.10. Biometrics

Biometrics is the most sophisticated tools providing logical and physical access control to information resources. Biometrics contribution to the science of security was invaluable.

The evolution of biometrics made it stable, solid and almost hard to be penetrated. It uses biological traits of the human being where no duplicate can appear. It prevents impersonation by matching the database of traits to the traits owners. The usage of biometrics in e-governments can vary from accessing critical systems to accessing physical restricted areas such as computer centres. Biometrics are used in payment systems to prevent fraudulent claims (Tipton, H. F. and Krause, M., 2000).

4.5.11. Logical access control (Firewalls)

From the ancient world, the term firewalls meant tough to penetrate and high security. It meant setting the toughest blockage before attackers so no by bypassing can occur, no direct penetration, and only those who are allowed can pass through. This analogy led to the invention of a technology using strong policies to block traffic into the network. Only allowed traffic goes through and traffic can be in the form of web access, applications direct access, applications to database exchange of data, or even simple email exchange to an external site. Having an organisation connected to the Internet without a firewall can be a challenge to find nowadays (Goncalves, M., Nov 18, 1999). The need of firewalls is now taught in professional course, academic course, or practical hands on sessions. Organisations sometimes fall in the misperception of considering firewalls are the only devices required to secure information resources. The introduction of applications and network layers firewalls confused organisations on the concept of firewalls usage. Firewalls are logical access control mechanism allowing and blocking entries to the organisation network by setting policies. Firewalls using IP and Ports to control the entry are considered in the network and transport layer of the OSI while firewalls using proxies to block or allow services are categorized as applications layer. Which one an organisation requires is a long debate which is out of the scope of this thesis. The comparison is between performance verses high level security. It is also between boundary and applications firewalls. An e-government with multiple applications will need applications layers firewalls to protect the systems infrastructure and boundary firewalls to protect the access of users from the different government departments and the Internet.

4.5.12. Security protocols

Security protocols can be categorizes as either network layer or application layer ones (Huth, M. R. A., 2001). Protocols such as IPSec and SSL act as a proactive mechanism in providing security to information. Security protocols play an imperative task in encrypting data during its transaction from a point to another.

The technologies proposed to construct the sub layers of the technologies layer are shown in **Table 16**. These technologies were selected based on literature review, industrial practices, and a direct derivation of the author and others experience in the field.

Table 16: Technology layer

Technology Layer				
A1: Access Control	A2: Intrusion Detection Prevention	A3: Anti-Virus & Malicious Codes Signature	A4: Authentication and Passwords	A5: Files Integrity Checks
A6: Cryptography	A7: VPN	A8: Vulnerability Scanning Tools	A9: Digital Signature and Certificate	A10: Biometrics
A11: Logical Access Control (firewall)	A12: Security Protocols			

Venter presented in his paper a good table indicating the all resources covering the information security technologies. Some technologies mentioned were not covered by the above matrix and may be added to support the technologies layer (Venter, H. S. and Ellof, J. H. P., 2003).

There are some technologies mentioned under different names which the author group into the model based on the real function used in practice. The access control referred to in the table shown in **Table 17** is the physical security access control while firewalls are referred as logical access control.

4.6. Security policies layer

Why any organisation needs a security policy? This question was answered long time ago when many businesses realized that technologies along can't serve the purpose of having a well structured security programme. Hare stated that "Policy is essential for the people in the organisation to know what they are to do" (Hare, R. M., 1952). Some of the reasons mentioned by Hare for having a security policy are compliance, maintaining shareholder confidence, and demonstrating the capability of the organisation on both establishing and maintaining objectives.

Many security experts believe that system security, product security, community security, and corporate information security policies are always the main concern of most of the security policies developers. Security policies can vary from a few policies to thousands of policies and sub policies covering all detailed aspect of protection, prevention, confidentiality, integrity and availability. Arguments between security policies developers were always raised on how detailed the policy should be. Wood stated that security policies are methods for building blocks of every successful information programme (Wood, C. C., 1999). Wood described a two-dimensional model of checking the level of coverage of all policies mentioned in the policy document. One of the pillars of the model is audience and the other one is control category or "Policy" (Moeller, R. R., 1981). The policy pillar can vary from one to as many policies are required for the organisation. The audience pillar is usually limited to five or six categories. Using this analogy, the author determined limited number of policies required for e-governments. These policies might increase due to new needs from e-governments or an occurrence to a new threat. The school of thought Wood is leading is to have different sizes of security policies based on the needs of the organisation. Another school of thought on developing security policies suggested that policies should not exceed ten pages maximum (Pelitier, T. R., 1998).

The number of security policies can vary based on the needs of the organisation and the area security is meant to guard against a well defined threat. In this layer the author selected a few policies to construct the sub layer. These policies can increase and has no limit. The

model will still hold as the idea is to have the right combination of policies with the other layers in the model and can hold irrespective of the number of the policies' cells in the layer.

The policies selected to form the cells of the layer are password management, log-in process, logs handling, computer viruses, intellectual property rights, data privacy, privilege control, data confidentiality, data integrity, Internet connectivity, administrative policies, encryption policies, HR security policies, third party policies, physical security policies, and operation security policies. The policies selected for the model are shown in **Table 17.**

Table 17: Policy layer

Security Policy Layer				
B1: Password Management	B2: Log-in Process	B3: Logs Handling	B4: Computer Viruses	B5: Intellectual Property Rights
B6: Data Privacy	B7: Privilege Control	B8: Data Confidentiality	B9: Data Integrity	B10: Internet Connectivity
B11: Administrative Policies	B12: Encryption Policies	B13: HR Security Policies	B14: Third Party Policies	B15: Physical Security Policies
B16: Operation Security Policies				

4.7. Security competencies layer

Due to the proliferation of the Internet and the usage of the citizens of the government wide e-services, government departments must invest on the human capital of the information security departments. Having a competent security team within the organisation will solidify the security infrastructure. Other researchers in the field of information security argued that the security competency must also be extended to the users of the e-services and not be restricted to the IT or information security departments. Siponen (Siponen, M. T., 2001) stated, "The Internet seems to make the fundamental dilemma of computer security. The dilemma arises from the fact that security-unaware users have a need for security but no expertise in such matters". In his paper, Siponen defined five dimensions

for the information security awareness. Only one dimension was related to the organisational while the other four were externals (Siponen, M. T., 2001). Whether the organisation decides to extend the awareness programme to the users or to limit it to its staff, the information security awareness programme should cover the baseline topics of the security knowledge such as (Al-Hamdani, W., A., 2007) security operation and management, security architecture and development, ethical hacking, security policies development, computer forensics, cryptography, security programming, law and regulations, security implementation and configuration, and security analysis. The author recommends other competencies for the security practitioners such as analytical thinking and complex problems solving, network troubleshooting, and cybercriminals psychology analysis which can be part of the computer forensic or security analysis competency. The competencies listed below **(Table 18)** will assist the government department enhancing the control of security and narrow the gap of the knowledge between the different government security departments. It will contribute in elevating the trust on the security programmes between the government departments and will increase the usability of the e-services by the citizens due to the strong confidence in the security level of the government departments.

Table 18: Competency layer

Security Competency Layer				
C1: Security Operation and Management	C2: Security Architecture and development	C3: Ethical Hacking	C4: Security Policies Development	C5: Computer Forensics
C6: Cryptography	C7: Security Programming	C8: Laws and Regulations	C9: Security Implementation and Configuration	C10: Security Analysis

Education and training are the tools of building the required knowledge base for security to all staff working in providing e-government services, internal users, and public users. Barnett stated in his report, ”people must get training and education foundations to enable them to work effectively in a variety of situations and stay current with both information systems technology and computer security threat, tools, techniques, solutions and risk containment” (Barnett, F., 1996). The focus in Barnet’s paper was on the essence of

providing security education to students. He argued that knowledge on designing, building, testing and operating computer security countermeasures will assist students to understand the security field in depth and will prepare them with the appropriate knowledge required in the industry. Considering students are a subset of the e-government services users, similar knowledge will be applied to the set of users defined S(users)= ((employees, security practitioners, users in the country, users out of the country, perpetrators).

The knowledge of how to protect the e-government services will be the sole responsibility of the security practitioners involved directly with the e-government security department as direct employees or suppliers, consultants, or third parties to the e-government. The e-government authority must allow their security staff to get the maximum knowledge on various security areas such as hacking, computer forensics, etc. These competencies can be acquainted through attending conferences and training courses. It is recommended that the e-government authorities allow their security staff to get updated on the security knowledge through freeing 10-15% of their time. This excess time will be utilized on attending conferences or higher educational courses (Barnett, F., 1996). Not considering the security awareness as a core element of the overall security programme is one of the 10 deadly sins noted by Von (Von, S., B. and Von, S., R., 2004).

Perry stated in his article that having low skills, low training, low integrity, and insufficient people is considered as a high risk on the competency of people continuum (Perry, W. E., 1982).

4.8. Security operations and management layer

Having the appropriate security technologies, policies, and knowledge will not provide the organisation solid and comprehensive security architecture. The National Institute of Standards and Technology (NIST) categorized the security controls into three categories; technical, operational, and management: technical controls as the security products and processes an organisation is placing to protect the IT infrastructure. The operational controls are the mechanisms which will ensure the proper security operation and prevent

any operational misconduct. The management controls are related to the usage policies management and the disaster recovery tasks management (Baker, W. H. and Wallace, L., 2007). Security is about vigilant monitoring and management of critical assets and information resources. Management and operational tools are a must to have in order to enable the security practitioner to perform the task and achieve the best objectives.

The most important aspect of this layer is how the organisation runs its operation. The operational policies and procedures are the rules and regulations where the security operational staff will follow in performing the tasks expected from them. Not considering the internal best practices for operational and management procedures is considered a deadly sin an organisation will commit (Von, S., B. and Von, S., R., 2004). These operational policies and procedures will spell out the security policy approved in the organisation and shall have strong reference to it.

Running security operation with primitive management tools is a tedious and daunting task. Having the appropriate tools such as the management agents, correlation engine, data warehouse and data mining will ease the process and will allow the operational staff to contribute better in the analysis and response to attacks. The concept of security operation and monitoring got more popular in the security field after the Microsoft incident in 2000 when a hacker penetrated its corporate network. The system administrators reviewed the logs after they discovered many accounts created in the system. The concept of protection alone will not serve the organisation to reach the accepted security level. It has to be protection, detection and response together in order to reach the maximum security benefits (Schneier, B., 2001). The sub layers indicated in **Table 19** are the proposed tools and functions needed to accomplish the security monitoring and management. The author believes that having this layer complements the other layers in the security model and makes them more tied in the inter-functional requirements and processes.

Table 19: Operations and management layer

4.9. Decision

Reaching the right decision for launching or not launching an e-service will have a direct impact on the success or failure of the e-service. Taking one direction or another can affect the overall model in selecting policies, technologies and hiring the right staff to run the security programme. Schneier stated that the top five reported problems were viruses/worms, employee misconduct, denial-of-service attacks, loss of customer data, and amateur hackers. This made many organisations to consider putting the position of security in the top level of their organisational hierarchy (Schneier, B., 2004). Schneier also illustrated that it is easy to calculate the security expenditures while calculating the ROI is quite hard. From the author's industrial experience, failing in presenting the ROI or the quantified values of information security made many organisations reluctant from selecting the appropriate programme, or hiring the right person for the right job. Network and security administrators use fear, uncertainty and denial (FUD) to justify the need of security. This approach usually works in Small and Medium Enterprises (SMEs) but not in big enterprises where the chief officers are well educated on security and the needs of the organisation.

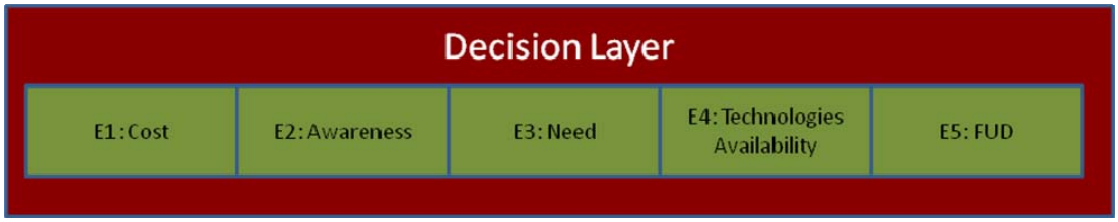
"Insufficient budget is the number-one obstacle to effective information security, followed closely by "resources priorities" according to a new survey of information security representatives at 1400 organisations in 66 countries (Risk Advisory Services Group, 2006) The numbers indicated in **Table 20** reflect the direction of information security expenditures in most organisation as per the 2006 survey:

Table 20: Security expenditures

Area Of Expenditure	Percentage of Expenditure
Security Technology	**83%**
Business Continuity	**68%**
Processes	**48%**
Consultants	**34%**
Staffs	**33%**
Employee Awareness	**15%**
Training	**13%**
Other	**2%**

As shown in the above table awareness, technologies and having the appropriate staff are what construct the right combination of the security programme of any organisation. The author presented other factors listed in **Table 21** from his experience in the field of information security. These factors play major role on whether a security programme can be successful or not. The cost verses the need of security; the awareness of technologies verses the availability of these technologies and above all, the physiological effect of FUD over the decision. Each factor has a direct or indirect effect the other sub factors in the same layer as well as the other sub factors in other layers of the model. The cost of security technologies is a good illustrative point to the impact of the decision layer on other layers of the security programme. Considering the cost constraints of any organisation, having the best technology, right competency, end-to-end operation and management infrastructure, and the right security policies will be evaluated thoroughly. Having the combination of all or some is also related to the cost limitation which derives the decision of the management of the organisation. Awareness is another factor which derives the decision. Having the right awareness on technologies to select, policies to apply, required competencies, and the right level of management and monitoring will have an impact on which direction the organisation can take.

Table 21: Decision layer



The model evolution

Figure 21 depicts the evolution of the model to a matrix format having sub layers and giving a description of each sub layer. The author found many literature on building security model to evaluate the network security based on a structure of security pillars and attributes such as the one proposed by Gosh called the NRM model (Schumacher, H. J. and Gosh, S. ,1998). Other models were presented for illustrative purposes only. Since the layers of the multi layered model are connected and complement each other in terms of functionalities and objectives, the author has evolved the model to a form where each cell has a value and a need of integration with the other cells of the model. The model the author is proposing will be used for further research for calculating the combinations of all possibilities the matrix can have to score the highest security rate. Having all combinations will not be possible due to the interference of the decision factors which are placed to reflect the real world scenario in many if not all organisations. Placing the layers in the model in the order reflected was not based on consecutive reasons, nor was it based on importance of each layer. The author placed the layers based on the industrial experience as security technologies are more common and accepted than the security policies. The other layers can be in any other order with no effect on the overall Model **(Figure 22)**.

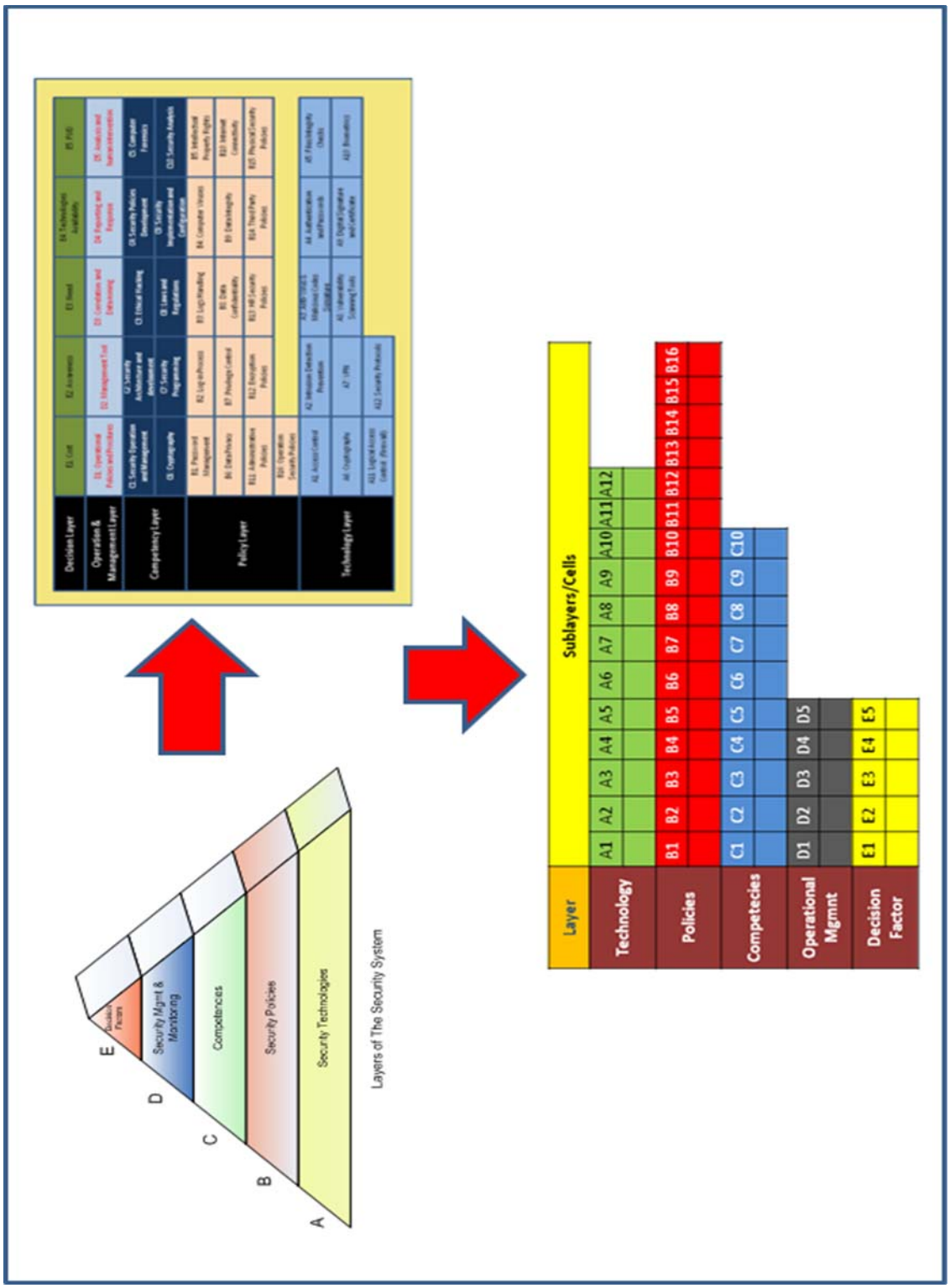


Figure 21: The evolution of the new model

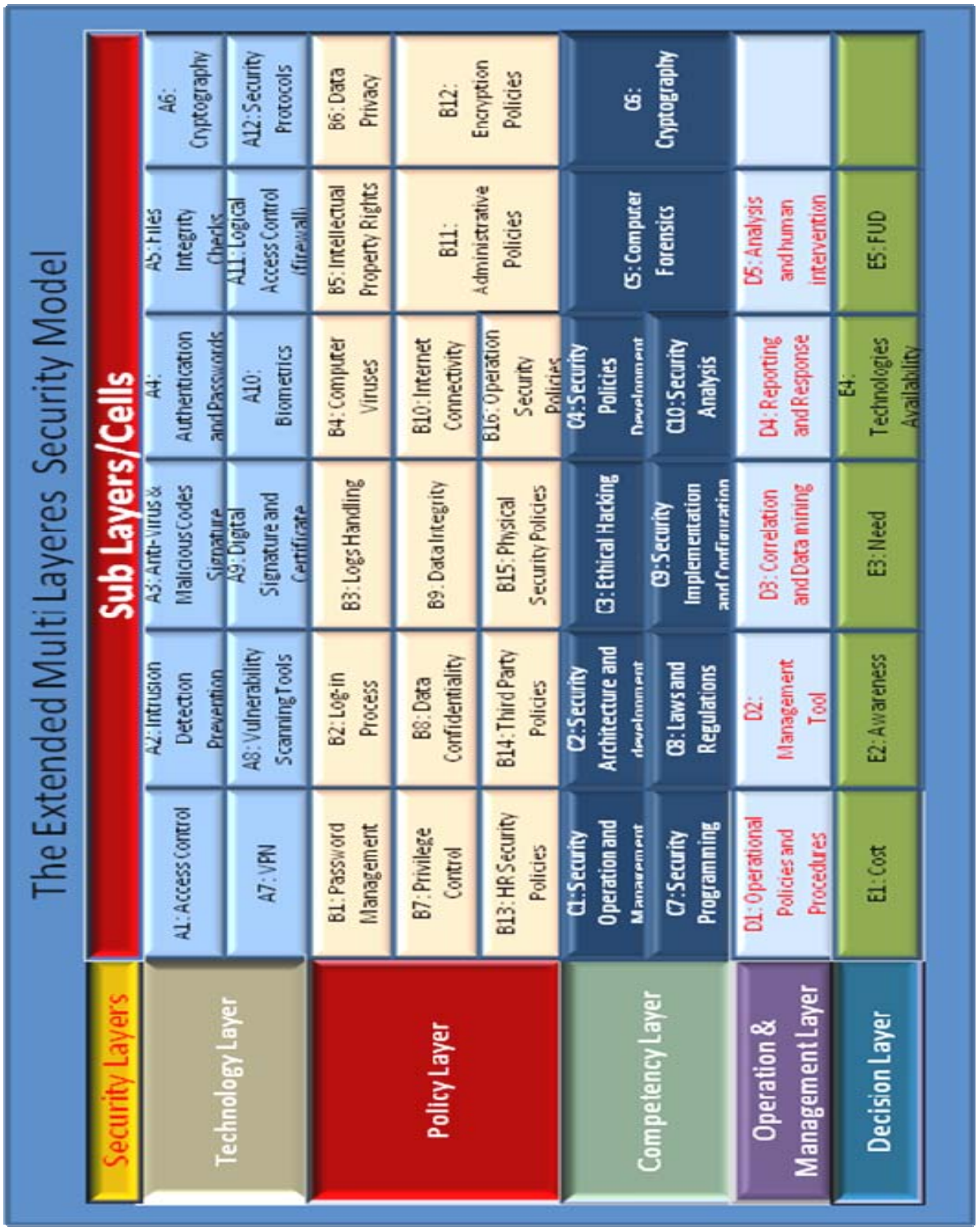


Figure 22: The matrix orientation of the model

This model derived from literature analysis is to be tested in the case study of the DEG authority. The new model will be used as a reference to identify the security layers applicable to the different e-services categories. In addition, a rating process will be applied on the different layers and sub layers by a group of selected security practitioners in order to confirm the applicability of the layers/sub layers proposed in the new model.

Chapter five: Case study of Dubai e-government security requirements

5.1. Introduction

This chapter aims to provide the reader the questionnaire (A) results analysis and the key findings from the answers provided by 19 participants who are IT decision makers and hold senior positions in the government or semi-government departments. This is out of a total of 26 government departments and represented 73% of possible organisation participants in Dubai. The questionnaire had 3 main sections as described in section 5.1.3; the first section was about general questions related to the e-government different types of services, the second section was about the internal threats, and the third section was about the external threats on the online services. The questionnaire established the Dubai perception of relationship, internal and external threats with the technological, human aspects, lack of policies, weak security competencies, or wrong decisions. The analysis will show how the scope of the model which addresses the different types of threats appropriate for Dubai government.

5.2. Questionnaire design

A high level questionnaire was designed for the management of the e-government authority and the government departments which are providing e-services to the public, interacting with the e-government authority and sharing information with other government departments. The questionnaire was designed in a way to assist the management of the government departments or those who are in charge of the e-government initiative within the department to identify threats, needs, and risks related to the online/e-services' implication to allow inter department information sharing. A copy of the questionnaire is in **Appendix A**.

5.2.1. Purpose of the research

The questionnaire starts with general questions related to the e-government e-services. The general questions address the types of services the government department offers such as information publishing, interactive services (one way or two ways), or transactional e-services. A government department may offer all types of e-services which will make it susceptible to more threats. The second section of the questionnaire addresses the internal threats which are related to the e-government authority or any government department affiliating with it. A list of well known threats is listed for the management to select from in order to get focused answers related to the thesis presented in this document. The third section of this questionnaire is related to the expectations, threats, and needs raised by an e-government authority or government department from trading/exchanging information with other government departments. The purpose of the research is to validate the needs of the e-government authority and government departments' management of information security in order to exchange or share information with the public or other departments.

5.2.2. Target interviewee

The e-government initiative is run by two main teams; the management of the e-government initiative and the technical team supporting the online services. Taking the opinion of one team rather than the other will not give a holistic view on the need of a new security model for the e-government. The technical team will cover the technical aspects only and the management team will only focus on the management aspects. It was found from a practical perspective that two questionnaires are needed for the two groups of audiences; the management and the technical. The types of threats on the online services will be identified by the management of the e-government and its affiliates. In this chapter, the survey results for the management questionnaire (questionnaire-A) are presented and analyzed. The participants of this questionnaire were either in the management level or hold a decision making role when it comes to launching online services or setting a strategy for them.

5.2.3. Different sections

There are three main sections of the management questionnaire:

- The **first section** addresses general questions related to the e-government types of services which they are classified as per the UN as:
  - Information Publishing
  - One way Interactive Services
  - Two ways Interactive Services

A question related to the current information security programme offered within the e-government or the government department was addressed in the questionnaire. Different possible practices offered the security programme were covered as part of section one of the questionnaire. The idea of highlighting the different practices was to correlate the types of threats (external or internal) with the different practices of the security covered by the security programme.

- The **second section** covers the internal threats related to the online services. A list of all twelve threats which might be caused internally was listed to ease the selection for the management of the government department. Some of the threats listed might be caused by technological flaws while others can be related to human factors.

  Questions were related to the reason of the level of threats severity, the areas of the security assessment must cover, and to the frequency of the security programme review.
- The **third section** was related to the external threats of the e-government and its affiliates. A list of twelve threats was put for selection.

All questions were inserted into a spreadsheet to record the results of the questionnaire. This method assisted in conducting the analysis faster.

5.2.4. Format of questions in questionnaire A

The format of the questions was mixed between close-ended and open-ended questions. Having the mixture in the format allows the participants to select the appropriate answers

faster and to add new points and answers if it is needed. It gave the questionnaire a great level of flexibility.

5.2.5. Questionnaire pilot

A sample of seven different respondents was selected based on the diversity of their roles within their organisations. The objective of having a pilot questionnaire was to test the easiness of the survey process, clarity of the questions, and to get an overview on the different possible answers which may occur in the larger population.

A preliminary analysis was conducted using the pilot survey results to get a sense of the direction of the results. Unfortunately, the pilot survey results were not giving a clear indication of any direction yet the following points were noticed:

- Some questions were not answered due to lack of clarity or to the sensitivity of the answers.
- Some respondents limited their answers to their experience without taking the effort of thinking about the other scenarios which they may have not encountered.

5.2.6. Selection of pilot interviewees

The interviewees of the pilot survey were selected based on the following criteria:

- The involvement of the interviewee in the security programme of their governmental department.
- The involvement of the interviewee with some or all the e-government online services.
- The strong background in the field of information security.

Table 22: Pilot interviewees

Role	Frequency	Percent
IT security Manager/Specialist	3	42.85
Director of Venture Development and Alliance	1	14.28
Director of Information Security	1	14.28
Manager of e-services/e-government	1	14.28
Professor of MIS/American University of Sharjah (expert of the e-commerce field)	1	14.28
Total	7	100%

5.2.7. Feedback

A feedback form was designed for questionnaire A and was sent to the interviewees to fill in order to capture all observations and apply the necessary changes prior to the final questionnaire circulation. This approach was agreed on during the design process of the questionnaire and the objective was to discover loopholes or major flaws in the questionnaire in order to make it stronger and more effective.

Most of the feedback was related to the questions being in academic format and to the length of the questionnaire. There was no negative feedback on the strength of the questions or their clarity. Some minor observations were given about the list of answers given being limited.

5.2.8. Changes done to incorporate pilot feedback

Some minor changes were incorporated to the questionnaire which was related to the list of answers given. In addition, some corrections of spelling, grammatical and logical flow were applied.

5.3. Main questionnaire survey

A total of 19 managers and leaders of the government departments affiliated with DEG authority participated in the "Security Management" survey. As the title states the survey was on the decision makers and management of the government departments. In addition, it highlighted the issues the management of a government department will concern.

5.3.1. The main questionnaire participants

The following table indicates the roles of the participants who answered the main questionnaire. Most of the participants moved to higher positions and to different roles in different semi government or government departments but still hold decision making roles when it comes to the e-government.

Table 23: Participants types to questionnaire A

Role	No. of Participants	Percent
IT security Manager/Specialist	3	15.8%
Director of Venture Development and Alliance	1	5.3%
Director of Information Security	1	5.3%
Manager of e-services/e-government	1	5.3%
Professor of MIS/American University of Sharjah (expert of the e-commerce field)	1	5.3%
COO of RTA	1	5.3%
CIO of Dubai Civil Aviation	1	5.3%
CIO of Dubai Municipality	1	5.3%
High Rank in Dubai Police	1	5.3%
Director of DEG Authority	1	5.3%
High position of Immigration	3	15.8%
Director level of different government departments	4	21.1%

5.3.2. When questionnaires were collected

The collection process of the questionnaires was not time stamped as some questionnaires arrived much before others. The reason of the delay was due to the time required to understand the organisation structure of some of the government departments and find the appropriate participant to the questionnaire. There were many cases when questionnaires floated from a department to another in order to find the right person who can answer the questions based on the interaction with DEG authority.

5.3.3. Who collected data?

All questionnaires were sent to the author of this document directly through email in order to ensure their validity and to check whether all questions are properly answered or not.

5.3.4. Process of collection

The process of collection was based on using the email as agreed by all participants. The questionnaire was sent to each participant on the official email address with a request to fill the questionnaire stating the purpose of the research and committing that the data will only be used for research purpose only. The participants confirmed back through email and responses were received subsequently.

5.4. Analysis

5.4.1. The spread of government e-services:

The e-government e-services analysis indicates a low spread of the four categorizations. A total of 4 respondents (21%) stated that they use information publishing type of e-services. Only 5% of the respondents are either using one or two way interactive services. A total of 3 respondents (16%) are using transactional services and 11 respondents (58%) stated that they use a combination of all e-services.

5.4.2. Status of Security services

In the existing or planned security practices in the e-government, the results indicated a strong need of human related policies and the need of strong encryption mechanism to protect the confidentiality of information.

The results of the survey **(Figure 23)** identified that 17 respondents (89%) indicated that information classification policies and procedures are existing in most of the government departments affiliated to the e-government authority. Only 11 respondents (58%) stressed on the need of encryption of classified information related to the government departments, 12 respondents (63%) indicated an existence of access control to enforce the concepts of separation of duties and need to know is in place, Also 12 respondents(63%) highlighted that the current security programme covers security operation management and monitoring, 11 respondents (58%) indicated the existing of network security measures such as firewalls, IDS/IPS, VPN, etc, while only 10 respondents (53%) indicated the need of strong authentication for the staff of the e-government authority.

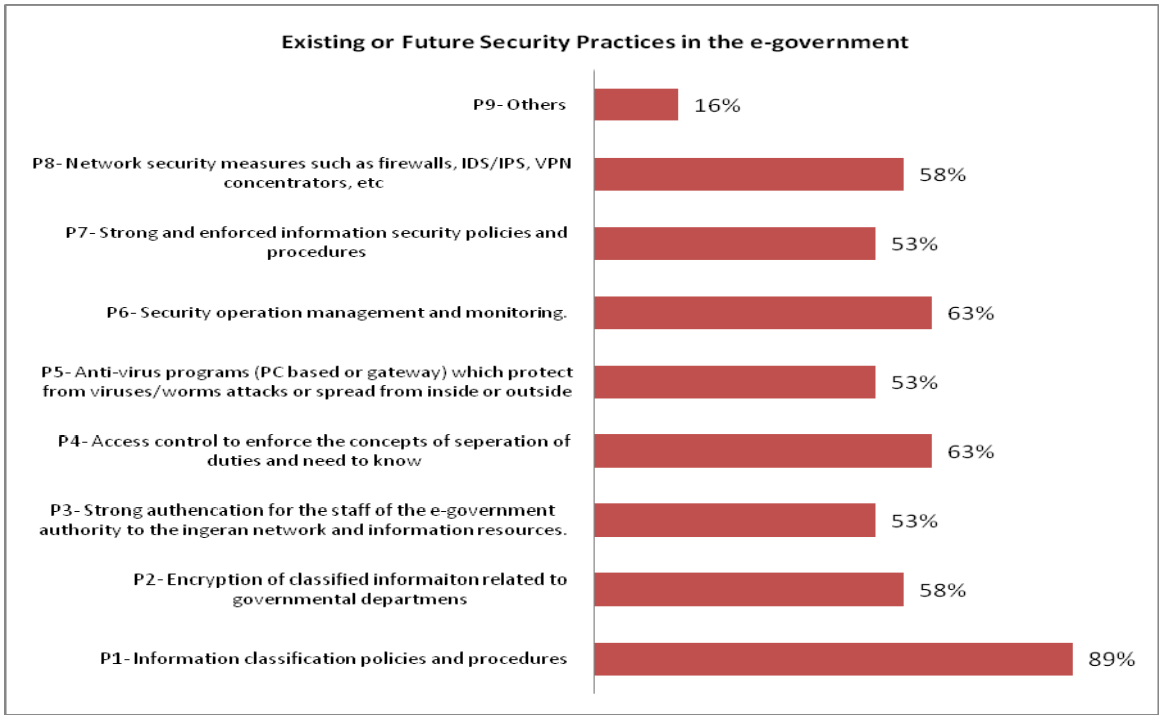


Figure 23: Future security practices in DEG authority

5.4.3. Internal Threats on e-government Infrastructure:

The survey results indicate that human related threats, failure of classified data and the lack of appropriate security operational management are considered the highest the respondents consider **(Figure 24)**.

The 16 respondents (84%) considered having disgruntled employees with access to non-authorized information resources is the highest internal threat their organisation might have. The second highest threat was related as indicated by 11 respondents (58%) is the lack of security and operational competency due to the introduction of new e-services or new technologies supporting these new services. A total of 9 respondents (47%) stated that the exposure of classified data to unauthorized staff due to a failure of encryption system can be considered as a strong internal threat. On the contrary, the threats related to the use of classified data by either industrial spies or information dealers were indicated to be low as only 7 respondents (37%) stated leakage of information or espionage related to the privacy of the citizen or public users is threat, 4 respondents (21%) highlighted the threat of industrial spies and 8 respondents (42%) indicated the threat of information dealers looking for classified and sensitive information of public citizens. This might be related to the lack of correlation of the respondents between the failure of encryption system which represents failure information confidentiality and the easiness of accessing unprotected classified information by industrial spies of information dealers.

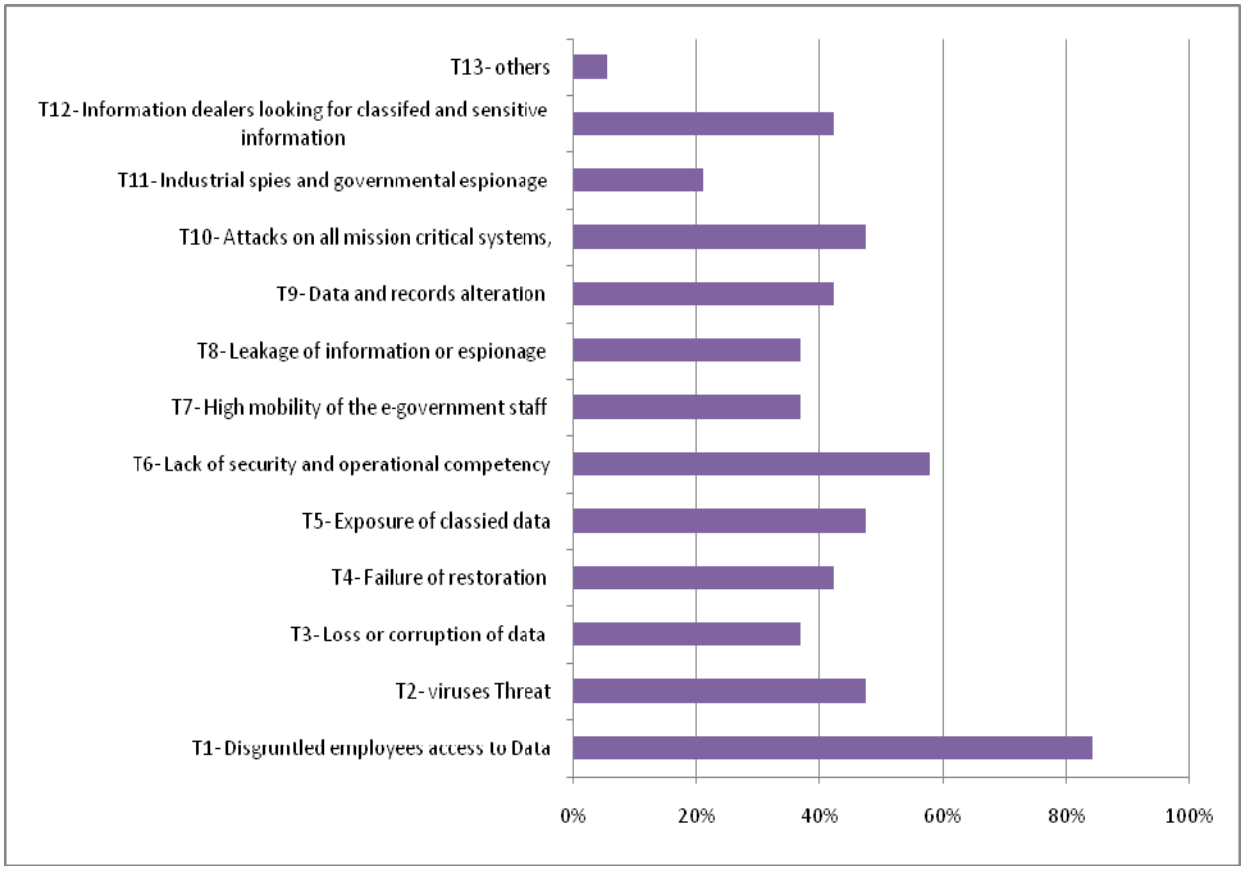


Figure 24: Internal Threats on e-government Infrastructure

5.4.4. Reasons for severe impact of threats:

A total of 12 respondents (63%) stated that the reasons for the severe impact of threats are related to the following **(Figure 25):**

- Lack of security knowledge in how to handle an incident (competency related threat).
- Lack of proactive security systems which can reduce the impact and contain the risk (operational and technological threats)
- Lack of a strong security operational and management systems which assist in the vigilant monitoring of the infrastructure (operation related threat).

A total of 11 respondents (58%) stated a severe impact threats might be due to weak security and IT infrastructure which is vulnerable to any level of attacks or security threats. Only 9 respondents (47%) stated that the severe impact of the threats might be due to the

high dependency on the security systems in running the business operation. The direct link between the internal e-government infrastructures to the external parties interacting with it was not found as a possible cause of a severe impact for threats as it was stated only by 4 respondents (21%).

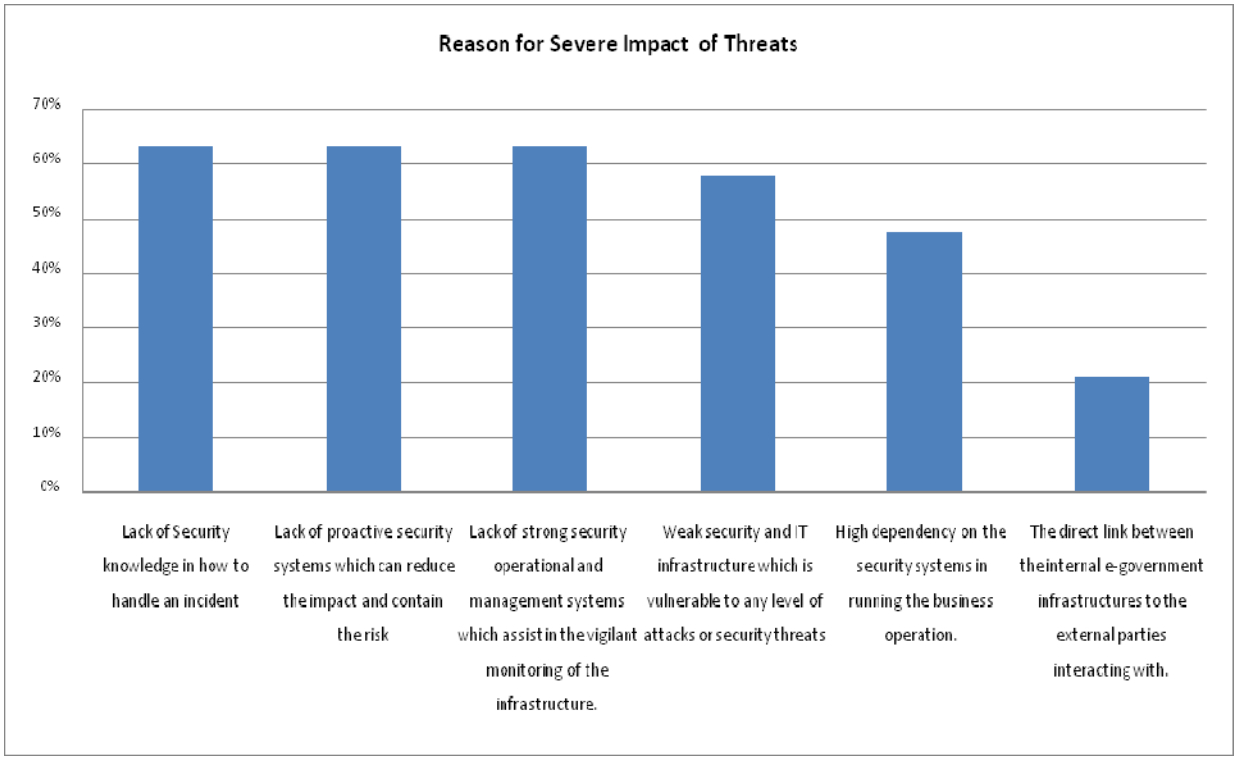


Figure 25: Reasons for severe impact of threats

5.4.5. Area of security assessment for the e-government:

The survey **(Figure 26)** identified that the majority of the respondents strongly believe on the need of assessment for the e-government on:

- Technologies used as stated by 14 respondents (74%)
- Policies applied as stated by 15 respondents (79%)
- Security operational procedures; 14 respondents (74%)

Only 11 respondents (58%) identified the need of assessment on the security and IT competencies available in the e-government whilst 10 respondents (53%) stated that an assessment will need to be conducted on the decision factors.

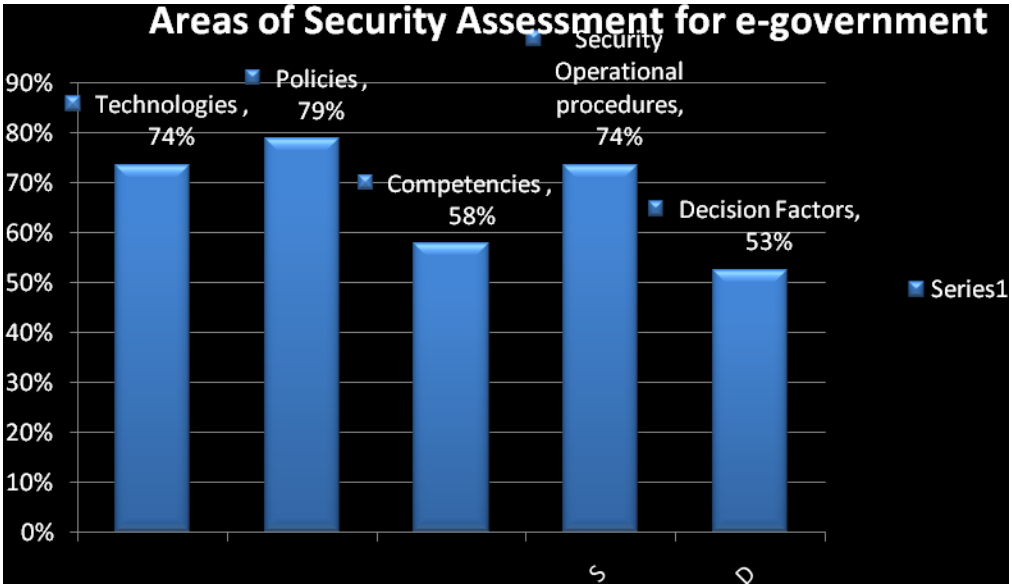


Figure 26: E-government areas of security assessment

5.4.6. Frequency for the security programme:

The survey results **(Figure 27)** indicate that the security programme of the e-government authority is not consistently reviewed by the affiliated government departments which might be the cause of the low trust in sharing the information. A total of 3 respondents (16%) only stated that the security programme of the e-government authority is monthly reviewed whilst 3 respondents (16%) stated that it is annually reviewed. On the contrary 3 respondents (16%) indicated that the programme is never reviewed. Only 1 respondent (5%) stated that a semi-annual review is conducted while 2 respondents stated it is quarterly reviewed.

The inconsistent answers indicate that the security programme of the e-government authority might be reviewed by some but not all affiliated government departments which will cause low level trust and will have a direct impact on the information sharing objective. It also leads to the need of having a common security programme between all interacting government departments in order to maintain a consistent assessment across all of them.

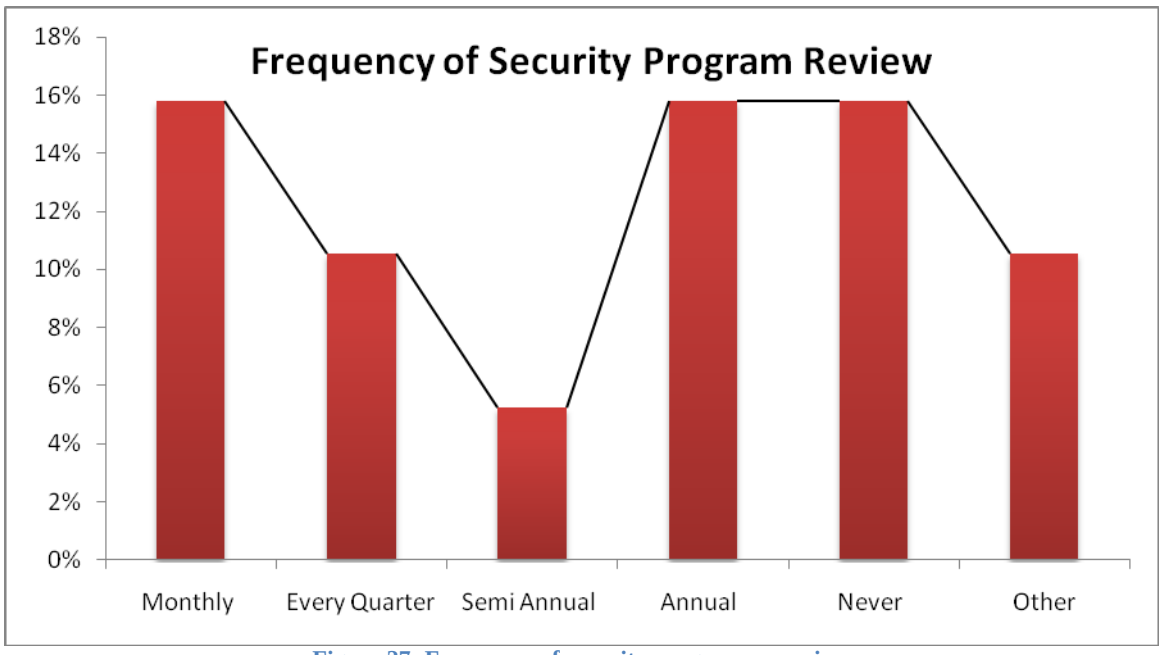


Figure 27: Frequency of security programme review

5.4.7. Security knowledge in e-government

The survey results **(Figure 28)** highlight that only 7 respondents (37%) confirmed the knowledge of the security staff on the security programme while 9 respondents (47%) negated that. Three respondents didn't answer this question (16%).

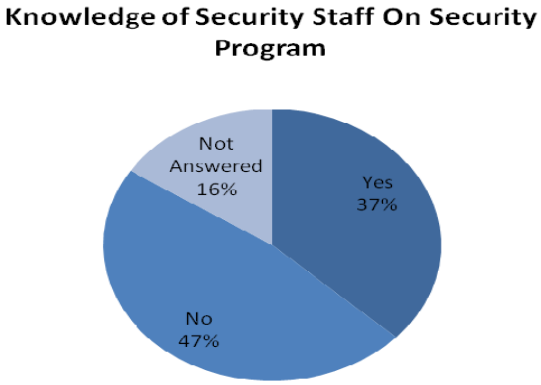


Figure 28: Knowledge of security staff

5.4.8. Security programme and business processes

Is the security programme linked directly to the business processes of the e-government authority and integrated with the services launching processes?

32% of the respondents confirmed with yes while only 26% negated that. A good percentage of 21% indicated that it might be in the future. A high percentage of respondents (21%) didn't answer the question **(Figure 29)**.

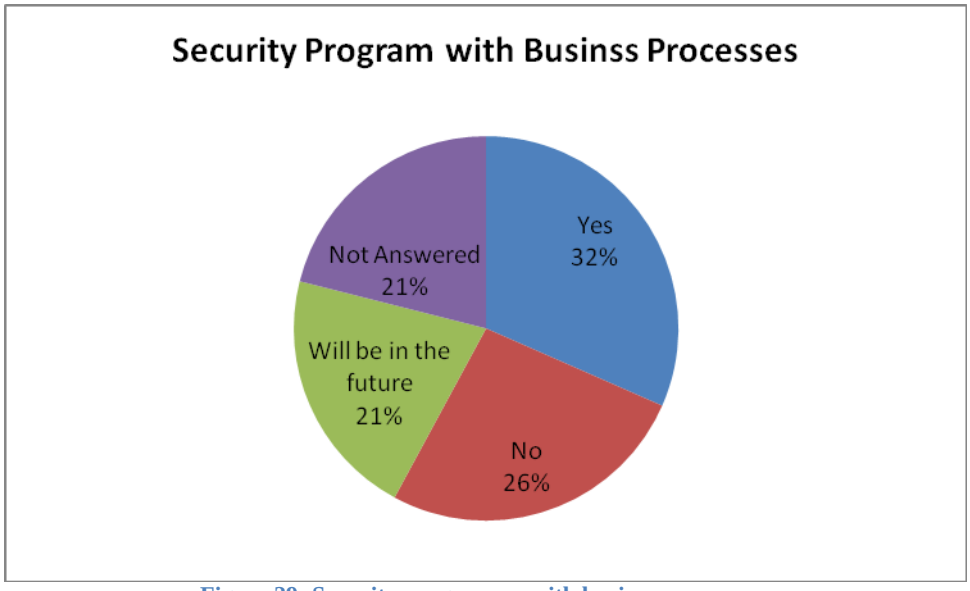


Figure 29: Security programme with business processes

5.4.9. Analysis of the external security related questions:

The definition of the e-government authority:

The purpose of this question was to draw a correlation between the perception on the e-government authority and the need of information sharing by the affiliated government departments. From the survey conducted **(Figure 30)**, 10 respondents (53%) confirmed that the e-government authority acts as a common gateway for all governmental services. Only 4 respondents (21%) stated that it is a relay and a workflow engine of governmental e-services offered by different government departments. The 5 respondents (26%) stated that it is an e-catalogue to all e-services offered by different governmental departments. Another 5 respondents (26%) stated that the e-government authority acts as a point of consolidation

for shared services of all e-government departments. Only 3 respondents (16%) indicated that the e-government authority is nothing but a portal while another group of 3 respondents (16%) stated that the authority is only part of an e-initiative for all the government departments.

The different definitions and perceptions of the e-government authority by the respondents of the survey might be the root cause of the low level of information sharing; integration of e-services or backend systems, and enforcement common security policies, programmes and assessment models.

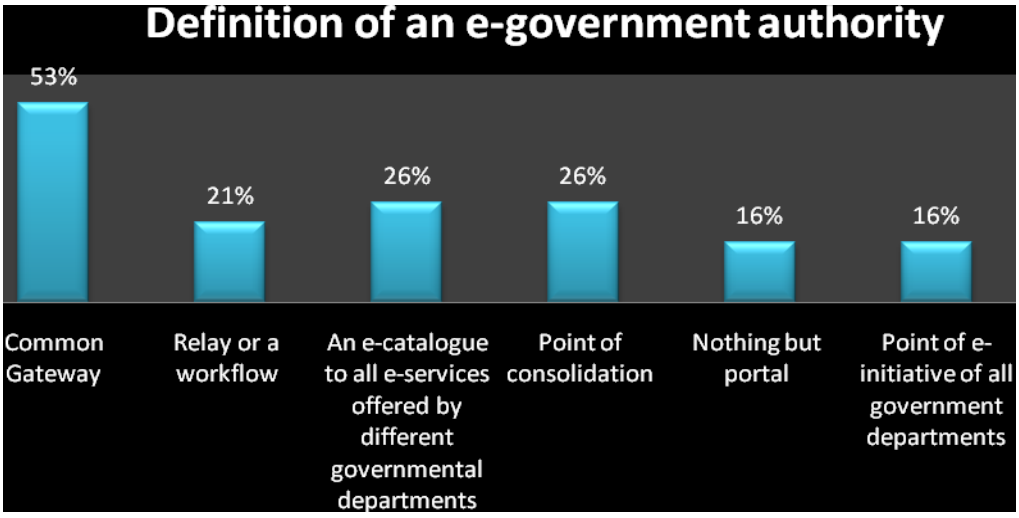


Figure 30: E-government definition

A total of 8 respondents (42%) indicated that the number of users of the e-services their organisations offer is 1000 to 10000. Only 3 respondents (16%) indicated that the number of their users vary from 10,000 to 100,000. An indication of only 21% (4 respondents) has shown that the number of their e-services users will exceed 100,000 whilst 3 respondents (16%) stated that the exact number can't be determined **(Figure 31)**.

The number of e-services users will be directly related to the type of online service the e-government department's offer and to the interest of the public users of these services. The categorization of the e-services the respondents' government departments has shown that 21% of the services are information publishing and 58% is a combination of all online

services categories (information publishing, one or two ways interactive, or transactional). The purpose of this question was to draw a correlation to the number of public users of the e-services and the high probability of external threats.

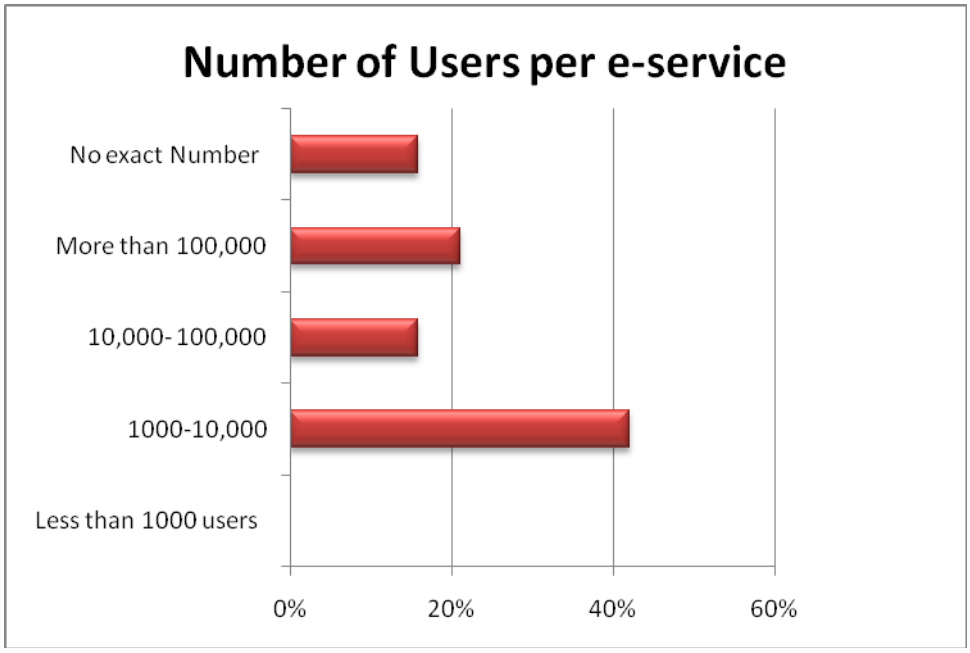


Figure 31: Number of users per e-service

5.4.10. Integrated services:

The survey results **(Figure 32)** show that only 7 respondents (37%) confirmed that they have integrated e-services or processes. A single respondent stated (5%) that more than 10 services are integrated. The 6 respondents (32%) stated that all the e-services offered by their department are integrated. Only 3 respondents (16%) indicated that none of the e-services are integrated. Only 10% of the respondents didn't answer the question.

The purpose of this question is to reflect the level of integration between the e-services which will lead to the need of having a common security programme for the integrated services.

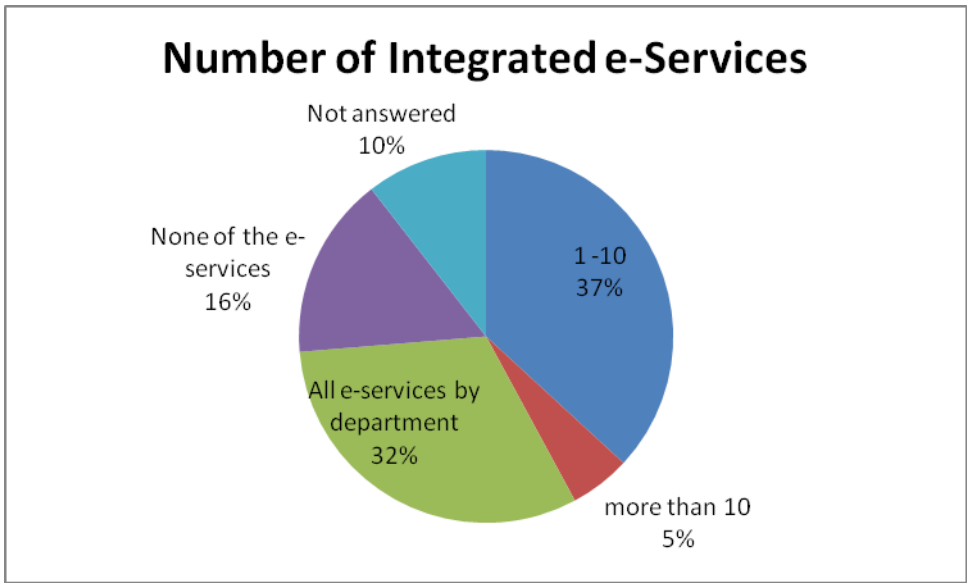


Figure 32: Number of integrated e-services

The majority of the e-government online services are mixed of public and corporate users as stated by 13 respondents (68%). Only two groups of 3 respondents (16%) indicated that the users are either public/residents of the country or corporate users.

A total of 9 respondents (47%) stated as there is no need of any computer literacy for the users of the e-services as long as the knowledge of using the web is there. Only 4 respondents (21%) highlighted that there is a need of computer literacy whilst another group of 4 respondents (21%) indicated that the computer literacy will be required to acquaint users with how to use the e-services at the beginning only. The 2 respondents (11%) highlighted that this need can't be determined at this stage.

The purpose of the above question was to draw a correlation between the need of awareness and computer literacy and the threats which might be raised by misconducts from uneducated users.

5.4.11. Number of e-services offered:

A total of 7 respondents (37%) stated that their government departments offer less than 10 e-services. The 5 respondents (26%) stated that their departments offer from 10 to 100 e-services whist another group of 5 respondents (26%) highlighted that between 100 to 1000 e-services are offered **(Figure 33).**

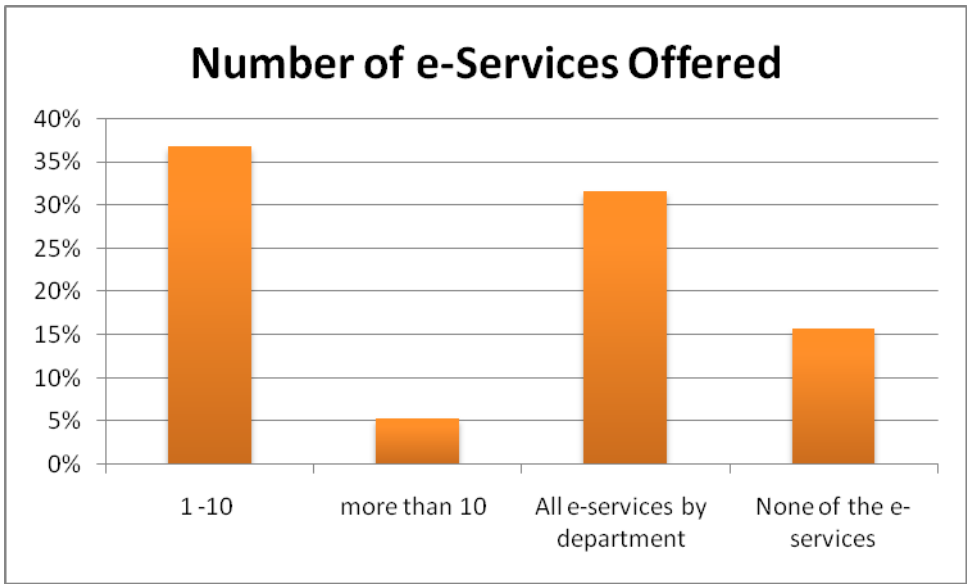


Figure 33: Number of e-services offered

5.4.12. External threats analysis:

The table below **(Table 24)** illustrates the related external threats and fear factors from dealing with the external customers (government or individuals related to the e-services offered as identified by the respondents of the survey:

Table 24: External threats

Threat	No. Of Respdn	%	Category of the Threat
Declassification and mishandling of information flowed between e-government authority and other departments or individual customers	11	58%	(C)
Man in the Middle attacks and interception with may expose the classified information from the e-government to the other departments or individual customer	6	32%	(T)
Denial of Services due to intentional actions (attacks) or unintentional actions (operational problem)	13	68%	(T)
Attacks generated from e-government external users whether from other departments or citizens interacting, transacting, or exchanging information with the e-government authority	7	37%	(T)
Viruses coming from the government departments which are not having good anti-virus infrastructure	12	63%	(T)
Rerouted attacks through penetrated e-government departments by external hackers or attackers	9	47%	(T)
Financial frauds due to impersonations of authorized users, systems flaws, or non repudiation	6	32%	(T) &(C)
Mis-configuration of any IT infrastructure element which may lead to leakage of information, wrong assignment of e-services, fraud, or corruption of data	13	68%	(C)
Disruption of complete cycle of an e-service due to latency of the network, low bandwidth, or bad integration	8	42%	(T) l
Information Alternation or unauthorized modification	9	47%	(T) & (C)
Physical Security breach which may cause of a total destruction of the IT infrastructure	6	32%	(P)
Other reasons	3	16%	Combination of All

T: Technological C: Competency P: Policies

As indicated in the table above, the majority of the respondents selected threats and fear factors which can be classified as technological in nature. 6 respondents (32%) selected man in the middle attacks as an external threat, 13 respondents (68%) selected denial of service attacks, 7 respondents (37%) stated that attacks might come from external users who may be part of other government departments and 12 respondents (63%) selected viruses coming from other departments are considered as a high external threat. The 9 respondents (47%) stated that rerouted attacks through another penetrated e-government departments are external attacks. In addition, financial frauds was considered by 6

respondents (32%) only, disruption of complete cycle of an e-service due to network latency or bad integration was selected by 8 respondents (42%) and the breach of data integrity was stated by 9 respondents (47%).

Competencies related threats scored high percentages as 11 respondents (58%) stated that declassification and mishandling of information flowed between e-government authority and other departments or individual customers is a high external threat. In addition, 13 respondents (68%) selected miscofiguration of any IT infrastructure element which may lead to leakage of information, wrong assignment of e-services, fraud, or corruption of data as a strong external threat.

A total of 6 respondents (32%) stated that a breach of the physical security which may cause a total destruction of the IT infrastructure is considered an external threat.
Only 3 respondents felt that there might be other external threats to the e-services **(Figure 34)**.

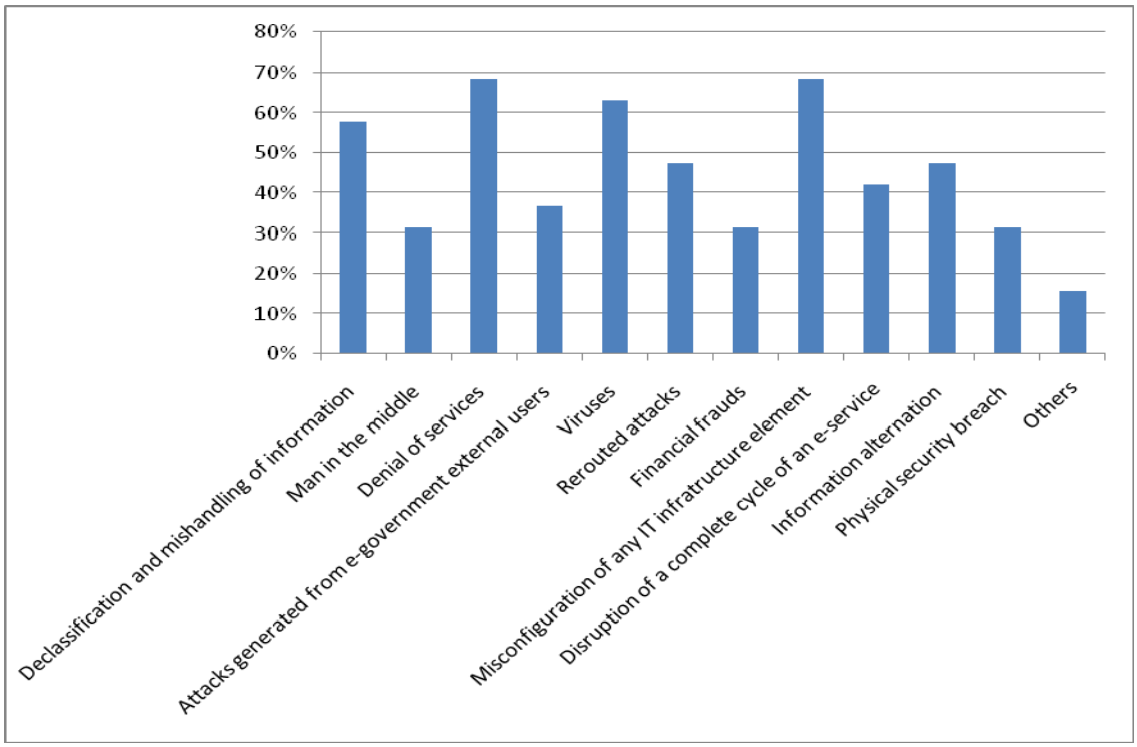


Figure 34: External threats

5.4.13. High probability of Threats

The survey results identified **(Figure 35)** a total of 13 respondents (68%) stated that the high probability of threats coming from external government department is due to the lack of auditing of government security. A total of 10 respondents (53%) related that to the lack of rules and regulations. Only 5 respondents (26%) linked that to the different perception of how security systems/programmes must be built with any governmental department or e-government authority. Six respondents (32%) indicated that the high probability of having external threats coming from another government department is due to security being a low concern by government department or the e-government authority. A total of 13 respondents (68%) confirmed that it is related to the lack of security model or model which can be applied on the e-government and its affiliated government departments and citizens.

It is clearly observed that the majority of the respondents stated that the high probability of external threats coming from another government department is due to either lack of auditing on the government security level and systems or to the lack of a common model and model which can be applied across the government departments in Dubai who adopted the e-government initiative.

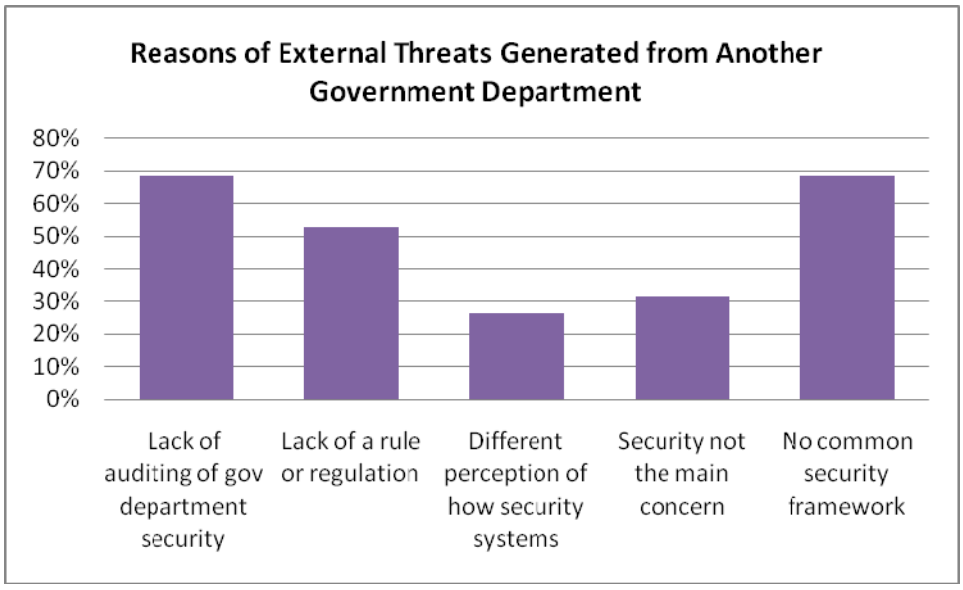


Figure 35: Reasons of external threats

5.4.14. Key security problems:

A total of 15 respondents (79%) **(Figure 36)** stated that lacking strong security policies is a key security problem faced by most if not all government departments. Only 8 respondents (42%) stated that security issues related to the information and security technologies implemented in the government departments are common problems across the government departments. The 12 respondents (63%) stated that lacking competent and security practitioners is a key security problem, whilst another group of 12 respondents (63%) indicated that the lack of vigilant monitoring a common problem. Taking the wrong decision regarding implementation of security technologies, enforcement of security policies, and hiring the right staff for the right security jobs was identified by only 3 respondents (16%). A good percentage of 58% (11 respondents) was voted for security not being carefully studied carefully and deeply. A single respondent (5%) selected other reasons but didn't specify.

The highest key security problems identified were related to the lack of policies, competencies, and good operational management and procedures.

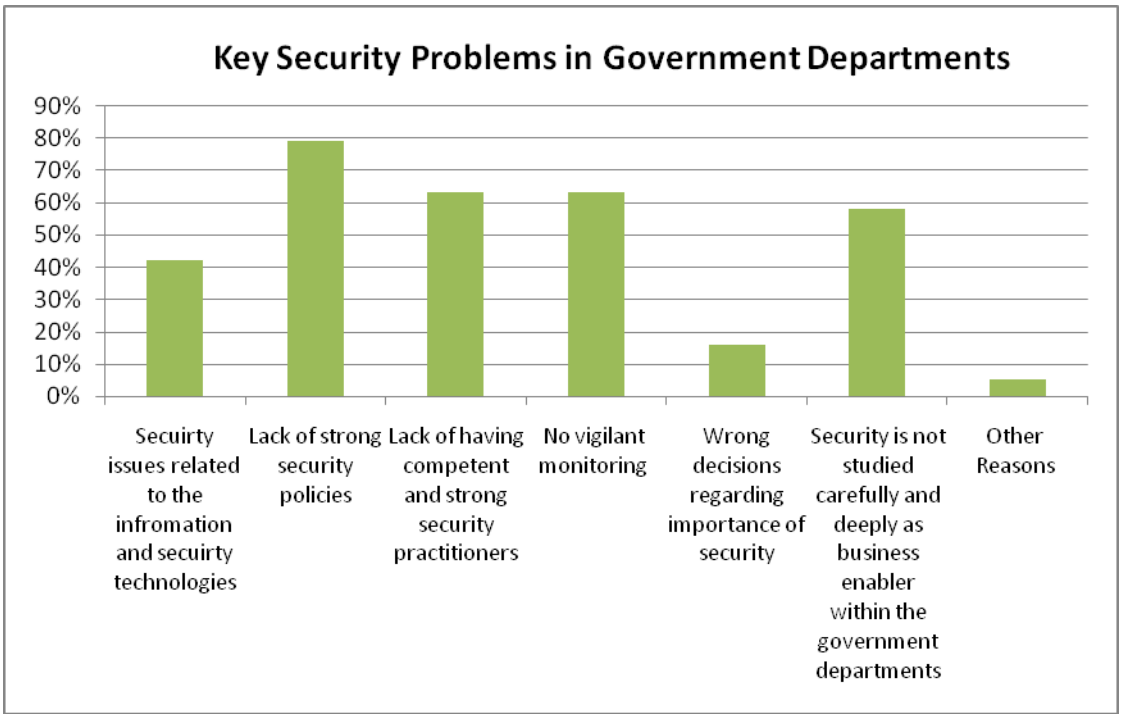


Figure 36: Key security problems in government departments

5.4.15. Requirements of government department:

A total of 11 respondents (58%) **(Figure 37)** indicated that a review of applied security policy is expected before sharing information. The review of the security architecture and infrastructure implemented with the governmental department was selected by 11 respondents (58%). Only 8 respondents (42%) highlighted that the list of security practitioners and their qualifications will need to be reviewed before sharing information between departments. This is directly related to the competencies category. The 10 respondents (53%) stated that a proof of strong security operational procedures within the government department will need to be demonstrated for any information sharing. Only 8 respondents (16%) required the security certification to be in place such as ISO 17799 whilst 3 respondents (16%) required a copy of the business continuity plan and the disaster recovery plan (BCP/DRP) for any information sharing.

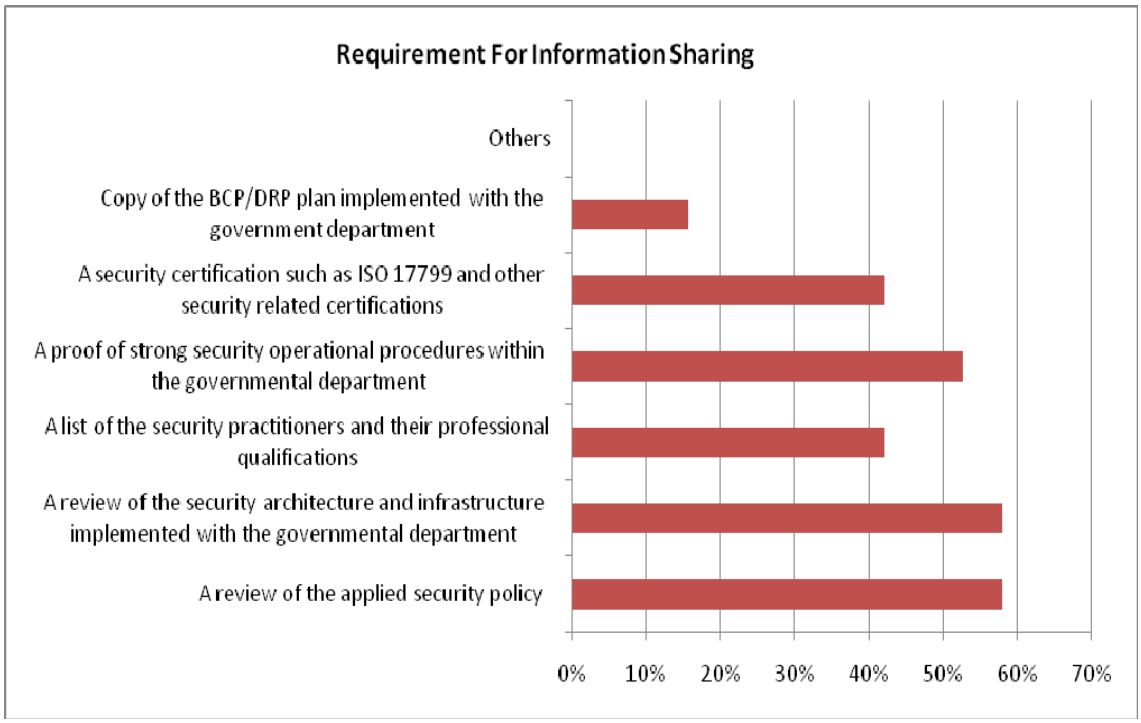


Figure 37: Requirement for information sharing

5.4.16. Security programme awareness:

A total of 13 respondents (68%) **(Figure 38)** stated that they won't feel comfortable dealing with other government departments or citizens without knowing the security level applied in their infrastructure. Only 3 respondents (16%) stated yes while 2 respondents (11%) stated that such knowledge is not necessary to conduct any interaction with government departments or citizens. Only 5% of the respondents didn't answer this question.

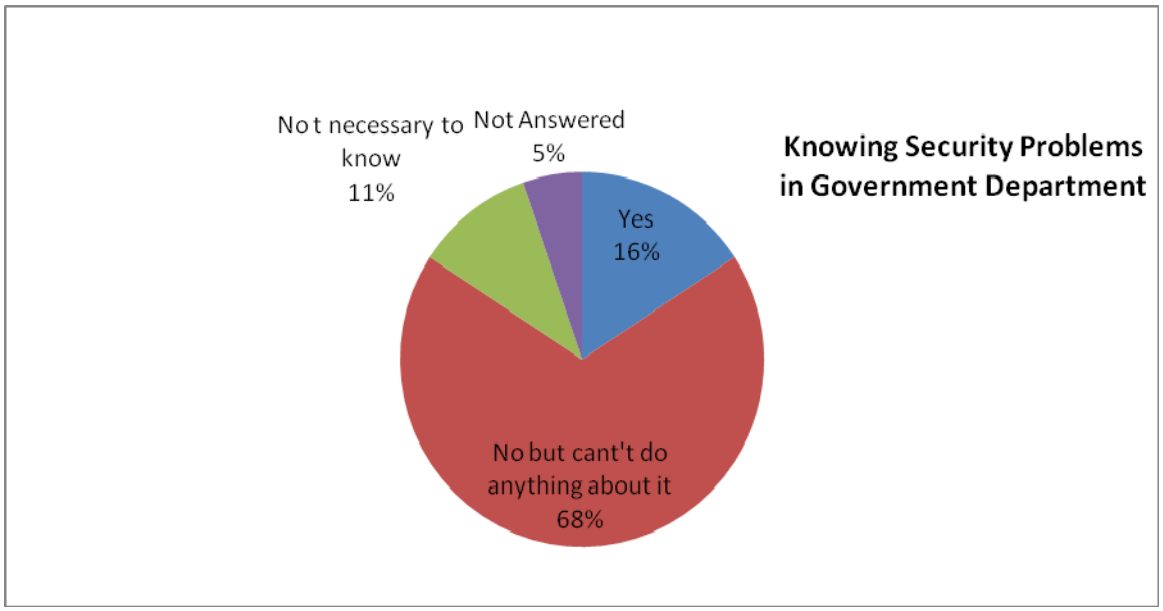


Figure 38: Other Departments Security Level

5.4.17. Ways for implementing security measures:

A total of 15 respondents (79%) **(Figure 39)** stated that developing awareness programmes for the public users is the best approach. Only 2 respondents (11%) suggested installing security programmes in the citizen PCs. A group of 4 respondents (21%) suggested restricting access of e-government authority or any governmental department except from special terminals and kiosks. Another 4 respondents (21%) stated that running manual authentication in parallel to all e-services authentication might a good security measure for the citizens accessing e-government services. Applying biometrics was suggested by 5 respondents (26%) and a single respondent (5%) suggested implementing the security policies will be a good security measure for citizens.

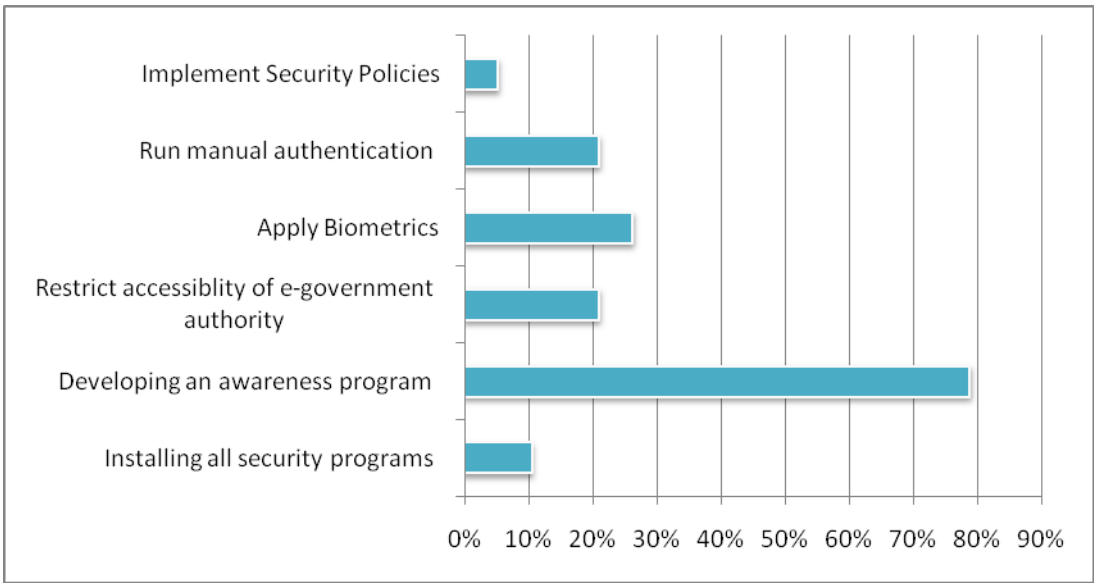


Figure 39: Methods of enhancing security level

5.5. Summary of key findings:

- The majority of the respondents to the survey provided the combination of e-services (58%) and only 21% provided the information publishing e-services.

- Disgruntled employees having access to unauthorized information resources were identified as the highest internal threat (84%). This threat might have a strong impact only if a weak security policy is practiced. Other security threats related to the exposure of classified data to unauthorized staff (47%). The lack of security operational competency was also highlighted as a high internal security threat (58%). This indeed was found in line with the high percentage given to the strong need of information security policies and procedures in the government departments (89%) and to the requirement of having access control to enforce the concepts of separation of duties and need to know (63%). The security operation management and monitoring was also identified as must to have (53%).
- It has been noticed that there is a direct link between the low percentage of the number of information publishing e-service and the fear of internal threats related to

exposure of classified data due to failure of encryption (47%) and the threat of information dealers looking for sensitive information (42%). Although these threats were internal threats they might be key factors blocking the organisation to publish any information over the Internet or forcing the organisation to be more contained. The low percentage of the interactive (one or two ways) and the transactional e-services 5% and 16% respectively can be related to the high percentage of fear of disgruntled employees (84%) and the lack of security operational competency due to the launch of new services (58%). This indeed cause a delay in launching services as developing competencies might require time, cost, and resources.

- Comparing the external threats with the spread of government e-service, it was observed that the top three external threats were having denial of services attack (68%), viruses spread from the government departments (63%), or mis-configuration of any IT infrastructure element (68%). The top external threats selected will have an impact of the spread of the e-government services in general and might be the reason behind the low percentage of the spread of the one way and two way interactive services.

- The top three reasons for the internal threats severe impact were identified as the lack of security knowledge (63%), lack of proactive security systems (63%), lack of strong security operational and management (63%). On the other hand, the lack of security competencies was rated as the third most demanded area for the security assessment (58%) while the security operation and technologies were equally rated the second (74%).

- The interactive and transactional e-services will require heavy integration of the business processes as applicants will need to apply, interact, and follow up the e-services from the time of application to the closure of the process. The majority of the respondents (32%) indicated that the security programme will need to be linked directly to the business processes and must be integrated with the services launching

processes. This highlights that if the security programme is not linked to the business processes, the services launching process will be affected and therefore, less interactive and transactional e-services will be launched by the authority. The results of the interactive and transactional e-services (5-16%) confirmed this point and showed that more integration of the security programme and the business processes of the e-services are required.

- Respondents indicated clearly that the areas which will need to be assessed as part of the security programme for the e-government and its affiliates are technologies (74%), policies (79%), competencies (58%), security operational procedures (74%), and decision factors (53%).

- Respondents indicated that integrated services and processes exist between the e-government authority and its affiliates which will increase the probability of risk and raise the need of having a common security assessment model which will tackle different types of threats related to any e-services.

- The highest percentage of identified external threat was given to miscofiguration of any IT infrastructure element which may lead to leakage of information, wrong assignment of e-services, fraud, or corruption of data.

- Online services are having different types of internal and external threats. Most respondents confirmed that a high probability of having a threat coming from another government department will be due to the lack of auditing of government departments and the lack of a common and comprehensive security model. This confirms the need of having a commonly accepted model for the e-government authority and its affiliates.

- A high percentage (79%) was given to the lack of strong security policies as a key issue which might be faced by most if not all security departments, followed by the

lack of competent security practitioners (63%) and the lack of vigilant monitoring (63%).

- There are key activities which will need to be conducted prior to information sharing. These activities are:
    - The review of the applied security policies in the other government department before sharing information (58%).
    - A comprehensive review of the security architecture and infrastructure implemented within the other government department (58%).
    - A proof of strong security operational procedures with the government department (53%)

5.6. Chapter summary

From the analysis conducted on the results of the survey, it can be conclude that online services or e-services have internal and external threats. These threats can be categorized as technological, competencies related, policies related, or operational. Taking the combination of the internal and external threats with the different categories of them, it can be derived that an online service will have a set of threats (external and internal) and a set of different categories of threats (technological, competencies, policies, and operation). This will lead into a need of a comprehensive model to tackle all types of threats. **(Figure 40)**

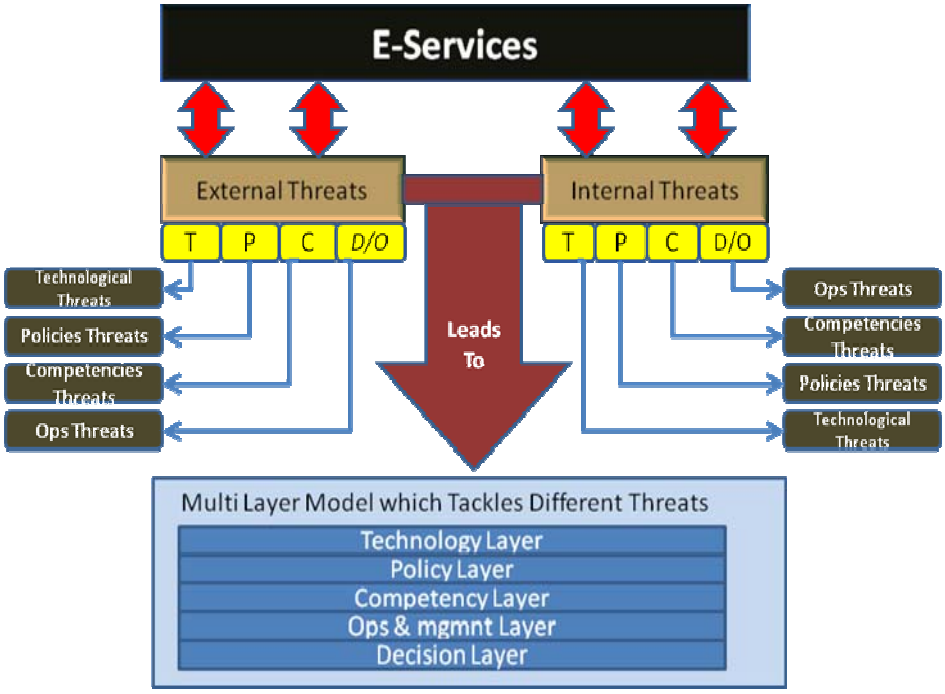


Figure 40: The drivers of the multi layer model

The nineteen participants of the Dubai government departments represent the majority of the government departments (73%) participating in the e-government initiative. Most of the respondents are currently holding executive levels positions in their organisations which make them the right population for this type of questionnaire. The responses were fair reflection of the reality of the situation and avoiding exaggerations for most of the questions addressed. The decentralized e-government strategy has caused the lack of synergetic security programmes which could have been shared and implemented across the 26 government department in Dubai.

The major threats (external or internal) selected by the participants of questionnaire A were:

Table 25: Top threats selected by participations

Internal Threats		
Threat No.	Threat Type	Description/Analysis
1	Disgruntled employee	This threat will definitely cause a low trust between the government departments as having the possibility of a disgruntled employee will cause threat 4 and 5
2	Lack of Security and operational competency	This threat will weaken the security infrastructure of the government department
3	Viruses	Viruses are a major threat in Dubai organisations in general
4	Attacks from within the government departments	Will have a serious effect if threat no. 1 exists
5	Exposure of classified data	Related to Threat no. 1
External Threat		
1	Denial of service	This will affect the availability of the government e-services
2	Mis-configuration of any IT infrastructure devices	This will be affecting the operation of the government department
3	Viruses	A major threat in Dubai in general
4	Rerouted attacks from other government departments	Will be a strong threat if the internal threat of the disgruntled employee
5	Information alteration or unauthorized modified of information	Can exist from external perpetrator or internal

Chapter six: Dubai e-government security model

6.1. Introduction

This chapter aims to address the objectives of developing questionnaire B and the steps followed to distribute the survey, collect the data, and analysis the data. The questionnaire was developed for security professionals and practitioners to solicit their industrial experience in building the detail of the new model. In addition, a comparison between the initial proposed model and the new one based on the findings and results of the survey is addressed.

6.2. Questionnaire design

Questionnaire B was developed to target security professionals and practitioners and to be used as a tool for capturing and analyzing their views. The objective of the questionnaire was to highlight the internal and external threats on different e-services categories (information publishing, one way interactive, and two way interactive and transactional e-services) and to identify the reasons which might cause a severe impact of these threats. Prior to distributing the survey, a thorough analysis was conducted on what might cause negative impacts of threats (internal or external), different types of threats which can be listed for the participants to select from, the sections of the survey which will need to cover different aspects of security related to e-government online services, and the correlation which can be drawn between different answers of the questionnaire's sections. The incorporated threats list in the questionnaires were derived from the literature review conducted. Some are from the author's industrial experience in the field of information security.

6.2.1. Questionnaire aim

The aim of the questionnaire was to get confirmation from the top security practitioners in Dubai on all the layers proposed in the model, sub layers suggested, and the level of their importance for the e-government authority. This technical survey included a correlation part for all the layers/sub layers with the different categories of the e-government e-services. The correlation questions assist the author to derive the final model representation and confirm the sub layers suggested in it.

6.2.2. Target interviewee

Since there is a limited number of highly qualified security practitioners who have strong background of the security field and known with their credibility in building bullet proof security programmes and architectures, the 16 participants for this type of a survey give a strong confidence that the number set a credible population. The participants for the survey were highly recognized security practitioners in Dubai and in charge of the security/IT infrastructure of a government department affiliated with the e-government authority or indirectly in contact with it. The qualifications of the participants varies from being certified in the information security or having a long experience in the field of IT or information security.

6.2.3. Questionnaire content

Questionnaire B contained around 69 closed questions in 7 sections:

Section 1: e-government questions:

The objective of this section was to identify the challenges the e-government authority and its affiliates are facing. This section has 3 sub sections which are addressing the following:

- e-government portfolio of services:

Diverse questions were included in this section to identify the challenges an e-government department is facing, the contribution of a new model might add in the information sharing,

needs of a new model, and the categorizes/maturity level of the e-services the participant e-government department offers (information publishing, one way interactive, two way interactive, and transactional e-services).

- Internal threats list:

A list of the general internal threats were listed for the participants to select from and an option for them to add other threats which may have not been covered in the list. The threats mentioned in the list were derived for both the literature reviews conducted through the research and the experience of the author. In addition, a table which draws the relation between the e-services with the threats associated was constructed and presented in this section in order to assist the participant to correlate threats with different e-services categories.

- External threats list:

Similar to the internal threats, a list of all external threats was presented for the participant to select from with an option to list other. The process of coming with this list is similar to the internal threats. A table of external threats associated with different e-services categories was constructed. In addition, a key question was presented in the end of this section asking about the causes of the severe impact of any threat (external or internal). The objective was to discover different reasons which may be technological, policies related, competencies deficiencies, or operational issues.

Section 2: Information security technology:

Information security technologies play a major role in comprehensive security model or system. Unfortunately, the lack of the hybrid security technologies force organisations to implement different ones and try to integrate them. Since all technologies can't be implemented in the organisation due to cost related issues and other reasons, a list of the most popular technologies was presented to the participants to select from. The selection was based on:

- The current technologies implemented in the organisation architecture.

- The importance and being sufficient to provide protection to the organisation.

The participants were asked to assign percentages on the technologies presented in this section in order to know which technologies are rated high and can be part of the first layer of the model. In addition the challenges related to the security technologies faced in the participants' organisations were listed for selection.

A key question was asked in this section which is related to the possibility of having all security technologies in one layer or not. The objective of this question is to gather a consensus on having all the technologies in one layer by group of security practitioners and professionals.

Section 3: Information security policies:

The objective of this section is to identify the key security policies required for a comprehensive security system or model and to assign a percentage on each policy based on its importance. The participants were asked whether having a second layer for security policies in any security model will assist in enhancing the security level of any organisation. The objective was to establish the need of the second layer in the new model presented in this thesis by the security practitioners who are from the region and have interacted with the e-government online services in Dubai.

Two key questions were asked in this section related to the need of applying security policies between organisations willing to share information and having a checklist of all policies need to be implemented is a good method of assessment of the level of security.

Section 4: Competencies:

Security competencies are key success factors of any security programme in the organisation. The importance of security competencies will be noticed when security projects are managed effectively during the implementation. The operational security competency will be required after the implementation of any security infrastructure to maintain the security procedures. The participants/practitioners were asked to select from a

list of security competencies in order to draw a clear picture on the type of competencies required for the e-government authority and its affiliates. In addition, the security practitioners were asked about their professional opinion on the importance of the competency layer in the new model.

Section 5: Information security management and monitoring:

Information security management and monitoring is a frequently discussed subject in the security conferences and seminars such as RSA, NetSec, Blackhat and ISC2 security workshops and seminars. Many experts and practitioners emphasise the importance of security management and monitoring as a key success factor of any security programme/system implemented in the organisation. A survey was taken on the following key points in order to confirm the alignment of thoughts when it comes to this area:

- The level of importance for the information security management and monitoring.
- The link between the strength of security management and monitoring and the level of the security in any organisation.
- The area of coverage for the security management and monitoring and whether all technologies need management and monitoring or not.

The strength of security management and monitoring is measured based on:

- Number of incidents handled
- Existence of the standard security operational procedures
- Infrastructure supporting this function
- Response time to incidents
- Correlation of data collected from all security devices

Participants of this questionnaire were asked to select from the above in order to identify the most common areas for measuring security management and monitoring.

The following list presents the common areas which build a good security management and monitoring programme which the participants were asked to select from:

- Operational policies and procedures
- Management tools
- Correlation and data management
- Reporting and response
- Analysis and human intervention

By completing this section, the security management and monitoring layer will be defined as part of the model and the sub layer cells will be selected by industrial practitioners of the field.

Section 6: Decision factor:

The decision factor of any security programme plays a major role in determining the technologies, policies, competencies, and the level of security monitoring and management. How the e-government authority and its affiliates reach decisions related to the security programme is what this section is designed to discover. Direct questions were addressed to the participants in order to determining how the decision is reached for any security technology, policy, competency, and operational procedure. The list below highlights some of the elements which will contribute in building the decision for any security programme:

- Cost factor
- Background on the security subject
- Need or want
- Availability of competencies/technologies and ease of implementation
- Any other reason the participant might feel to be valid

There are some factors which may change the decision of any security technology, policy, or implementation such as:

- Not having enough information on the subject
- Failure to justify the ROI

- Lack of competencies required for new technologies implemented
- The high cost of implementation, training, and transition from the old security infrastructure to new security infrastructure
- Major and core business processes change which will be introduced by the new security programme

These factors were addressed in this section for the participants to identify and select from. In addition, the impact of any decision on the technologies and policies implemented was checked by addressing direct questions to the participants to analyze their feedback.

To emphasise on the decision factor in any security model, this section of the survey checked whether the participants are aware of any model or methodology which addresses the importance of the decision in any security programme. The objective was to identify any new model or methodology in order to examine and analyze.

Section 7: Correlation questions:

A correlation table was set for all the five categories of e-services and the different layers of the new security model. The participants were asked to select from the list of technologies, policies, competencies, operational and management practices, and decision factors abbreviated as A(x), B(x), C(x), D(x), and E(x). Based on this selection, a percentage is calculated for each category of e-service and a correlation analysis will be done as part of the finding and analysis section. The participants were asked to select based on their industrial experience with the different categories of the e-services in Dubai e-government.

The selections were as the followings:

Security technologies (A):

Table 26: Selected security technologies

A1 Access control	A2 Intrusion Detection and prevention	A3 Anti-virus & malicious and prevention	A4 Authentication & passwords	A5 Files integrity & checks
A6 Cryptography	A7 VPN	A8 Vulnerability scanning tools	A9 Digital signature and certificates	A10 Biometrics
A11 Logical Access Control (firewalls)		A12 Security protocols		

Security policies (B):

Table 27: Selected security policies

B1 Password Management	B2 Log-in Process	B3 Logs Handling	B4 Computer viruses
B5 Intellectual Property Rights	B6 Data Privacy	B7 Privilege Control	B8 Data confidentiality
B9 Data integrity	B10 Internet Connectivity	B11 Administrative Policies	B12 Encryption Policies
B13 HR Security Policies	B14 Third Party Polices	B15 Physical Security Policies	B16 Operation Security Policies

Security competencies (C):

Table 28: Selected security competencies

C1 Security Operation and Management	C2 Security Architecture and development	C3 Ethical Hacking	C4 Security Policies and development
C5 Computer Forensics	C6 Cryptography	C7 Security Programming	C8 Laws and Regulations
C9 Security Implementation and Configuration		C10 Security Analysis	

Security operations and management (D):

Table 29: Selected security ops and mgmt

D1 Operational Policies and Procedures	D2 Management Tools	D3 Correlation and data mining	D4 Reporting and Response	D5 Analysis and human intervention

Decision Factors (E):

Table 30: Selected decision factor

E1 **Cost**	E2 Awareness	E3 **Need**	E4 Technologies Availability	**E5 FUD**

6.2.3.1. Survey questions:

The survey contained closed ended questions which were designed to give the participants a selection from lists presented for each section and key questions. The lists items as aforementioned were selected based on research and literature reviews conducted and based on the industrial experience of the author. In addition, the participants were given an option to add other ideas, factors, or security hints by filling the field "others" which was presented in each list.

6.3. Questionnaire pilot

A pilot questionnaire was designed for questionnaire B to test the length of the questions, style, and level of technicality. The pilot questionnaire was sent to seven (7) security practitioners and the feedbacks which came from the pilot didn't indicate any issues related to the length or the structure of the questions. However, during the analysis of the actual questionnaire, many questions were not answered somehow in the expected way which might be due to the way the questions were presented. This was noticed in the technology and security policies where participants were asked to put percentages right next to each items in each layer. Some participants have put low percentages thinking that all the numbers shall be accumulated to a 100% while others understood the question in the right way and assigned each item an percentage from 0-100% independently from the others.

6.3.1. Pilot interviewees

The selection of interviewees of this questionnaire was based on the need of having qualified security practitioners who agreed to participate in the pilot and give the preliminary feedback on questionnaire. The criteria of selection for the security practitioners was based on the direct and or indirect involvement in the e-government initiation, the strong background of the practitioner in the e-government security topic, and the number of years, certification, and background level of the security practitioners. Most of the security participants who participated in this process have had direct or indirect experience with the e-government, governmental departments, or online services offered in the country.

6.3.2. Feedback

The feedback forms came back after the pilot with some corrective comments summarized in the following points:

- The language of some of the questions was weak or didn't reflect the right objective of the question
- Some questions were vague and didn't make sense

- The questions were relevant and good but sometimes are missing the government department context.

Some of the positive comments are summarized as follows:

- The questions are contributing to the knowledge body of the information security field.
- Length of the questions is suitable for information security practitioners and IT executives.
- To test the value of the questionnaire from research and scientific view, five questions were asked addressing the following areas:
    - Coverage of the information security domain: Average of 80%
    - Analytical thinking behind each question: Average of 80%
    - Knowledge contribution in each question: Average of 80%
    - Raising or highlighting issues which are related to the security of government: Average of 85%
    - Scientific quality of each question: Average of 90%

The above areas indicate that the questionnaire was well designed and also was used as a tool to address security issues and assisted in giving better view of the different aspect of information security.

6.3.3. Changes done to incorporate pilot feedback

All comments were considered and changes were made to the questionnaire language, clearance of the questions, length, and the analytical part of them. The questionnaires were given to some colleagues who are well known of having strong critique and a thorough review was conducted on every question. The amended questionnaire was then sent to the other participants who didn't comment on the length, clearance, or the scientific value of the questions.

6.4. Main questionnaire survey

A total of 16 security practitioners and IT managers/executives, participated in "Questionnaire B" survey which was designed to be technical and more related to the information security industrial experience. The questionnaire was sent as an attachment over email. The role and profiles of the security practitioners who participated were changed as some of them took new roles within their organisations while others left their organisations and moved other governmental departments. From a research perspective, their contribution was still considered valuable to the research as they are considered the most knowledgeable of the information security field in the city of Dubai and the ones who interacted with the e-government online services.

6.4.1. When questionnaires were collected

Each participant was given a period of 3 weeks to send his response. Extensive follow up was conducted through phone calls, emails, text message, and personal interactions just to get the questionnaires on time. Some of the questionnaires came after 2 months from the sent date while others came in less than 3 weeks. The long time span for the collection process affected the analysis phase and created some data errors which could not be sent back to the participant to correct. Most of the participants are so busy and they are contributing in a way or another in the transformation of their departments/organisations which created a challenge for the research and data collection process.

6.4.2. Who collected them?

All questionnaires were sent to the author of this document directly through email in order to ensure their validity and to check whether all questions are properly answered or not.

6.4.3. Process of collection

The process of collection was based on using the email as agreed by all participants. There was no iterative process of collection as the participants took a long time for answering the questions except for those who answered less than 50% of the questions. Only two questionnaires were returned for incompletion.

6.5. Analysis

Challenge an e-government is facing in terms of information flow:

As per the survey results **(Figure 41)** 8 respondents (50%) stated that the challenges an e-government is facing in terms of information flow are related to the trust between the e-government body and the government departments. The 11 respondents (69%) indicated that it might be due to no common rule and or standard which control this flow of information. Technical challenges were identified by 8 respondents (50%) while 7 respondents (44%) stated that it is due to the absence of direct relation between the government departments and the e-government except on the services the e-government offers. Only 5 respondents (31%) stated that it is due to no assurance in data classification or declassification.

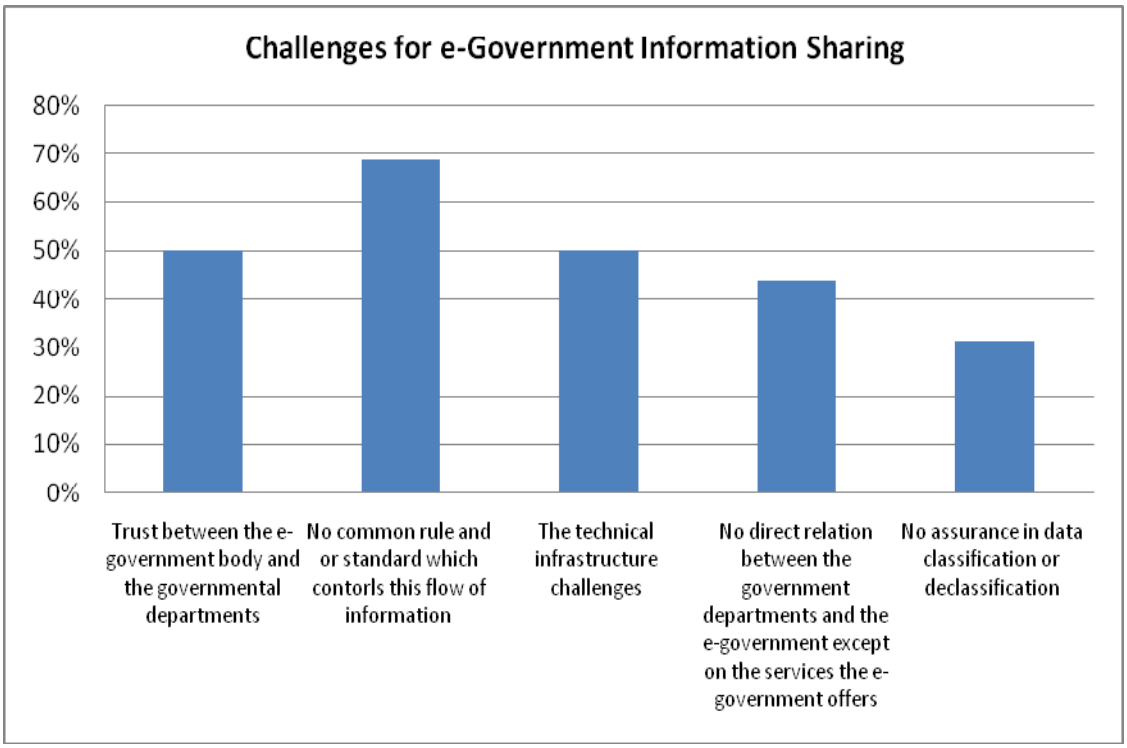


Figure 41: Challenges for e-government information sharing

Regarding the opinion of having a standard assessment model for the e-government in order to synchronize the level of security for intra or inter communication:

The results of the survey **(Figure 42)** identified 14 respondents (87.5%) confirming the need and only 2 respondents (112.5%) negating any need of standard assessment.

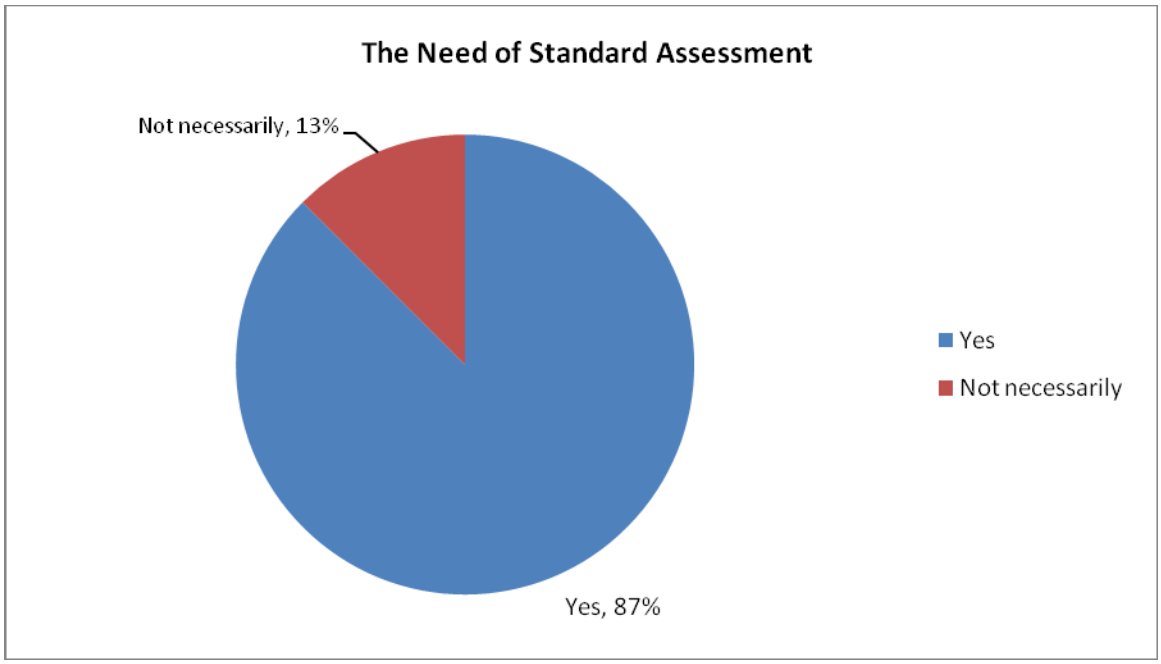


Figure 42: The need of standard assessment

The impact of the standard security assessment should be positive on the government departments and will encourage them to freely exchange information between themselves and the e-government authority:

A total of 14 respondents (87%) stated yes and only 2 respondents (13%) stated no.

Will the cybercrimes which already occurred for the e-government force the implementation of the standard security assessment model across the government departments?

A total of 14 respondents (88%) stated yes and a single respondent (6%) stated no.

Types of e-services the respondents' government departments offer:

The results of the survey **(Figure 43)** identified that 4 respondents (25%) stated that their organisations provide information publishing online service. This service is meant to assist the citizen to start the procedure and obtain an e-service or a catalogue of other e-services offered by the e-government. The 3 respondents (19%) selected the one way interactive e-service which is a downloadable from the government department portal. A transactional e-service where users can perform functional transactions through the government department portal was selected by only 3 respondents (19%). Only 7 respondents (44%) selected the combination of all e-services.

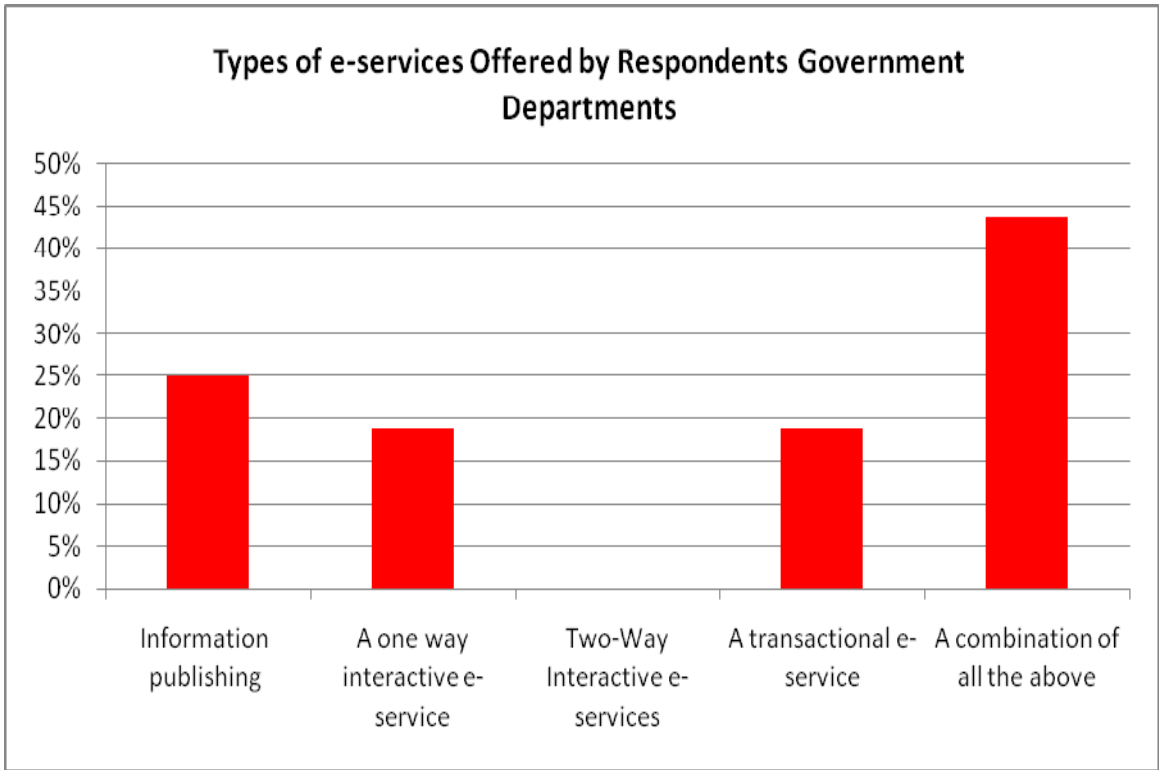


Figure 43: E-services offered government departments

6.5.1. Internal threats:

The following table indicates the internal threats identified by the survey participants:

Table 31: Internal threats

Threat	Resp	Perc
Disgruntled employees having access to non-authorized information resources.	14	88%
Viruses spread intentionally or unintentionally by e-government staff	11	69%
Loss or corruption of data caused to applications/OS malfunctions, database issues, etc.	8	50%
Failure of restoration after a major unplanned shutdown due to weak operational and recovery procedures.	6	38%
Exposure of classified data to unauthorized staff due to a failure of encryption system.	8	50%
Lack of security and operational competency due to the introduction of new e-services or new technologies supporting the new services.	14	88%
High mobility of the e-government staff which will increase the threat of accessibility	3	19%
Leakage of information or espionage related to the privacy of the citizen or public users through electronic transfer, physical leakage through medium handing over, or oral information exchange.	10	63%
Data and records alteration related to public users or governmental departments.	8	50%
Attacks on all mission critical systems, and processes from within the governmental departments.	6	38%
Industrial spies and governmental espionage conducted by internal terrorist and spies working within the governmental departments.	4	25%
Information dealers looking for classified and sensitive information of public users/citizens, or other governmental departments.	7	44%
Others	0	0

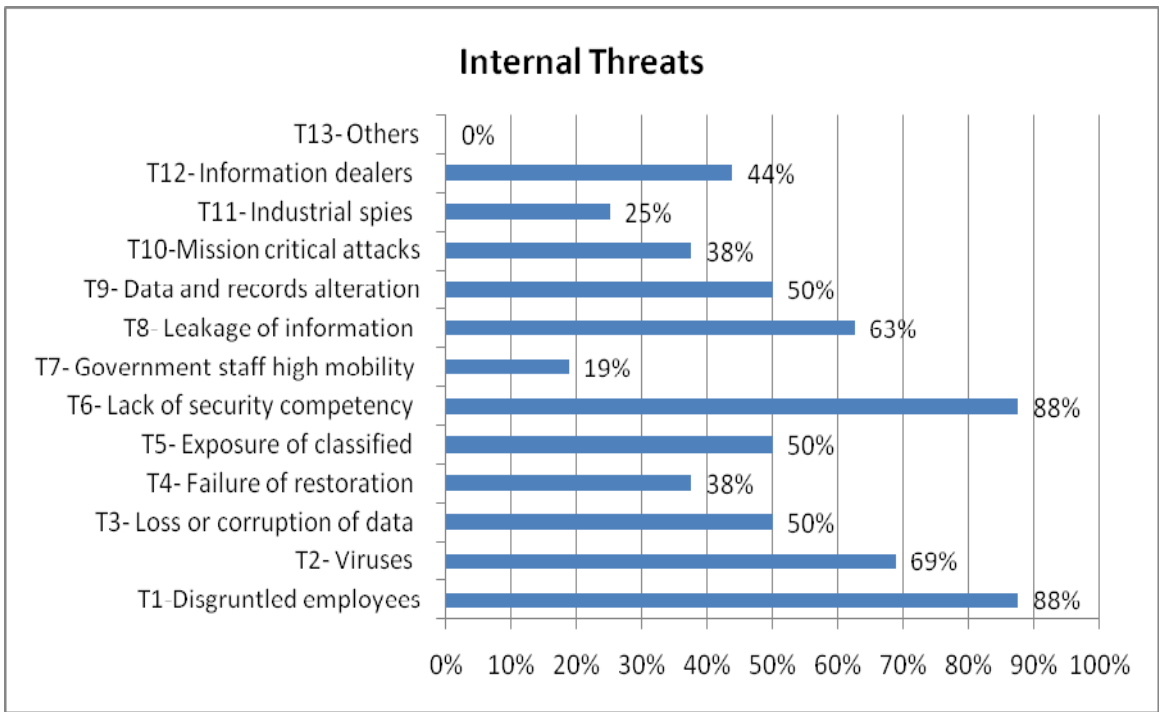


Figure 44: Internal threats

The following section discusses the internal threats related to different types of e-services offered by the e-government:

6.5.1.1. Internal threats on information publishing e-services:

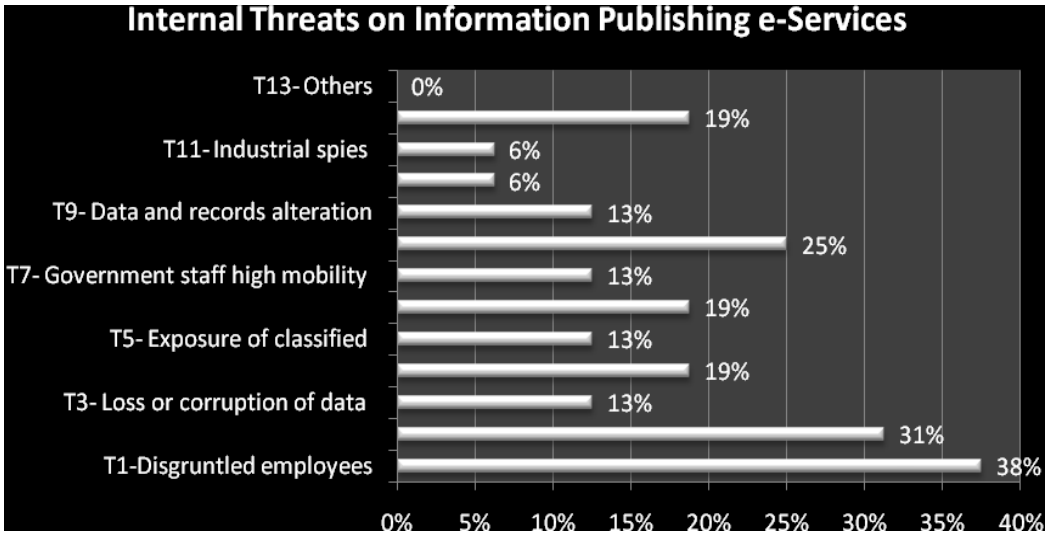


Figure 45: Internal threats-information publishing e-services

6.5.1.2. Internal threats on one way interactive e-services:

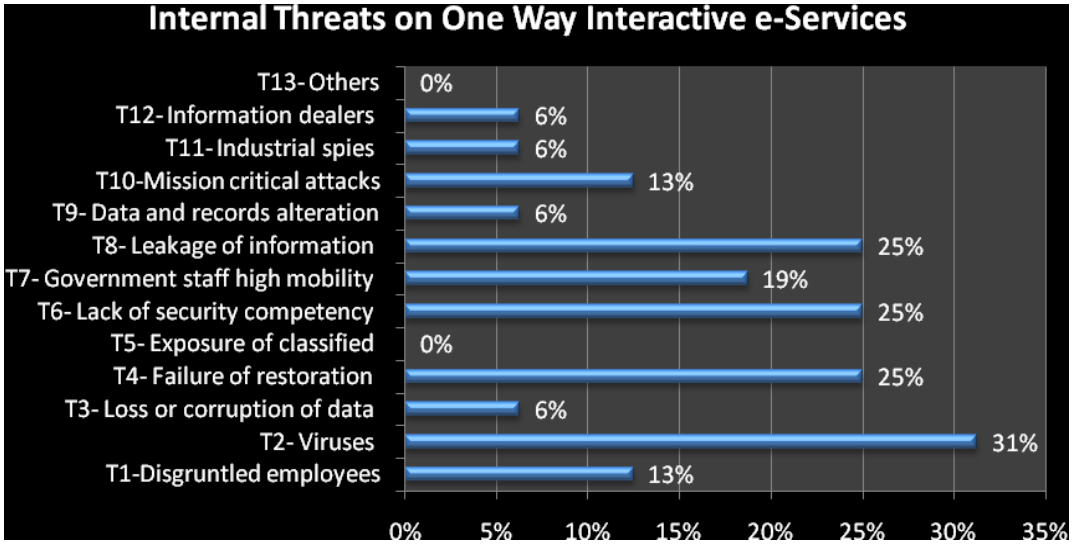


Figure 46: Internal threats-one way interactive e-services

6.5.1.3. Internal threats on two way interactive e-services:

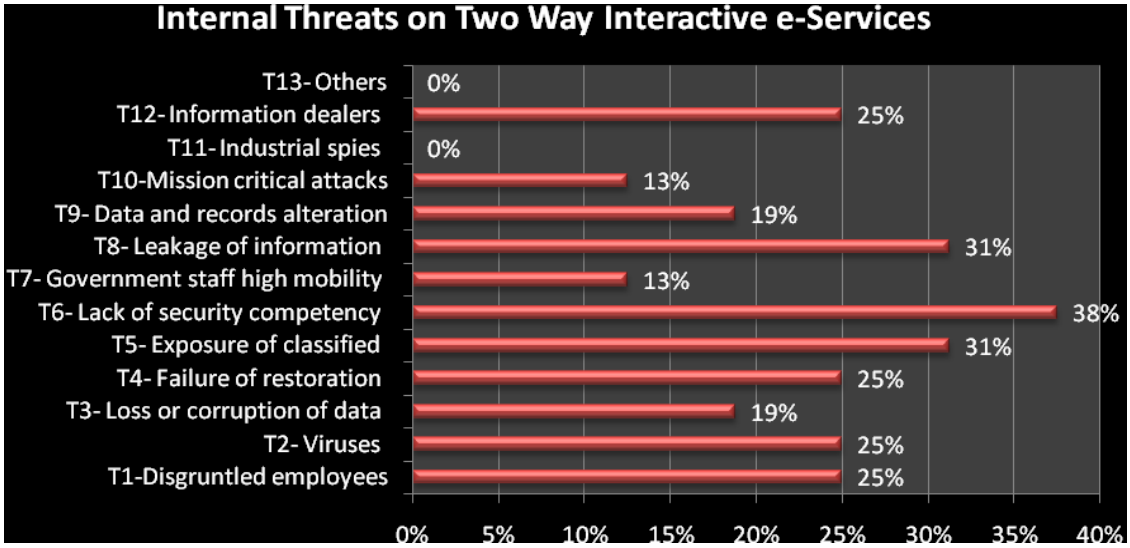


Figure 47: Internal threats-two way interactive e-services

6.5.1.4. *Internal threats on transactional e-services:*

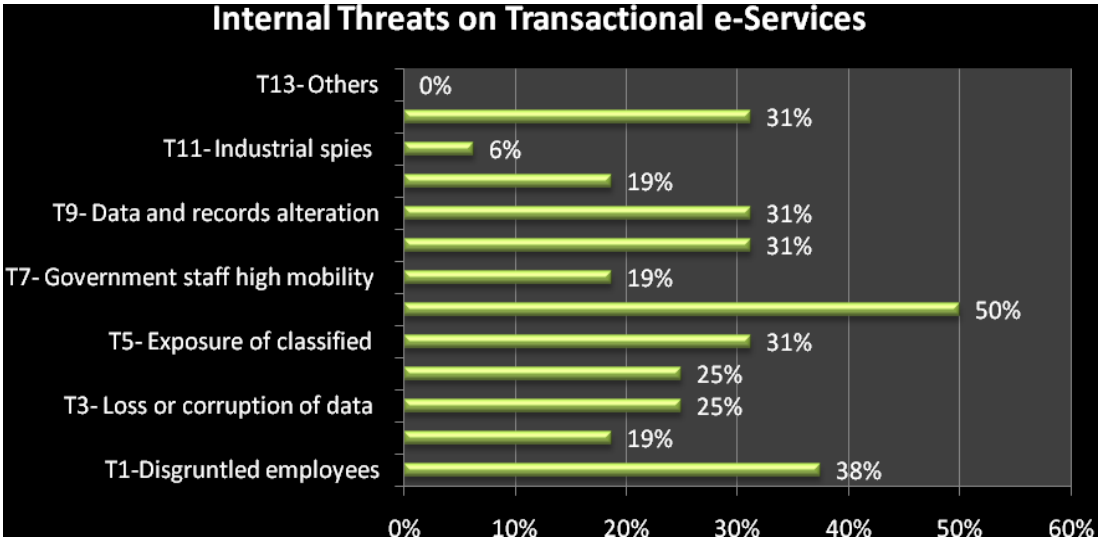


Figure 48: Internal threats-transactional e-services

6.5.2. *External threats:*

The following diagram indicates the external threats identified by the survey participants

External threats

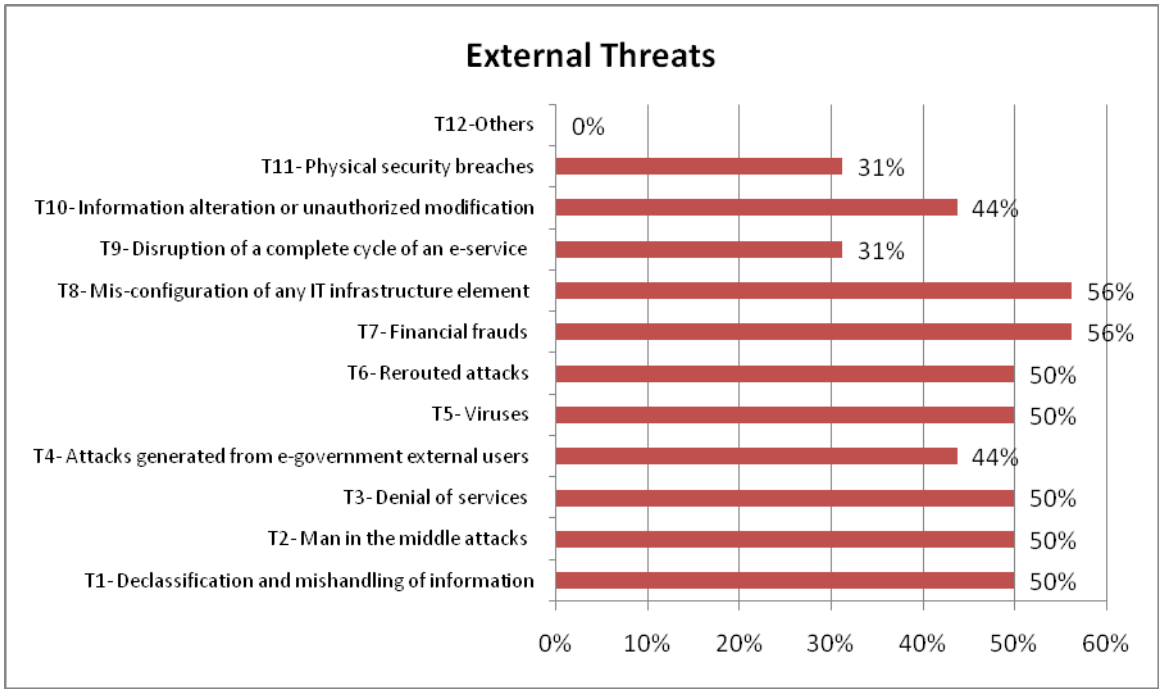


Figure 49: External threats

6.5.2.1. External threats on information publishing e-services:

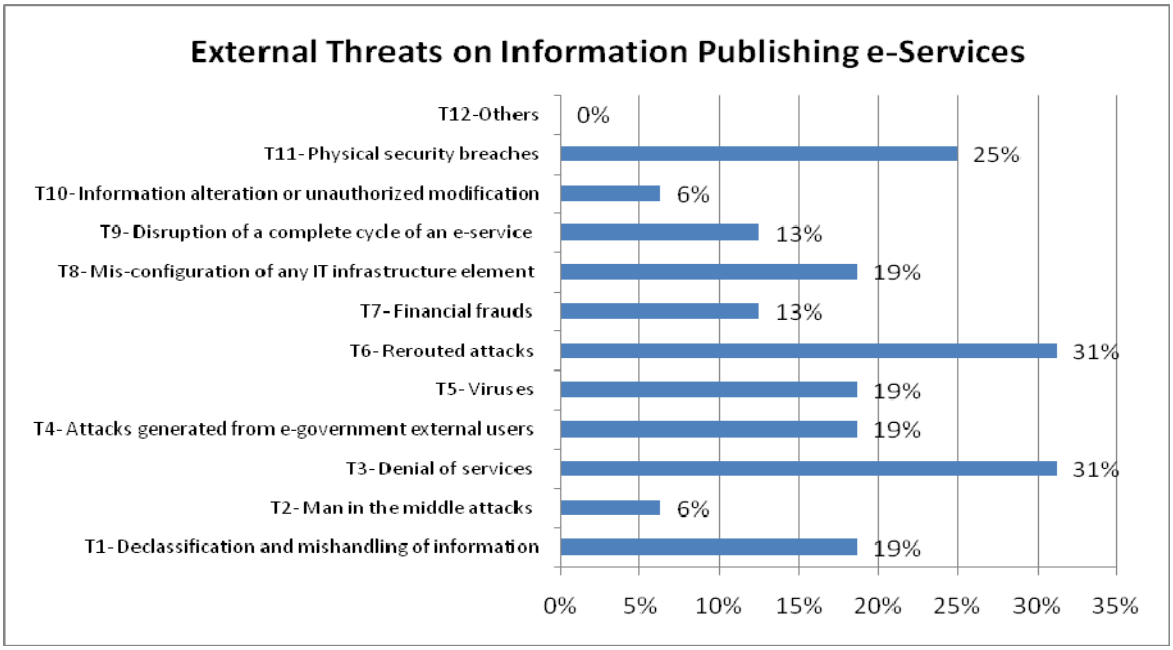


Figure 50: External threats-information publishing e-services

6.5.2.2. External Threats on One Way Interactive e-Services:

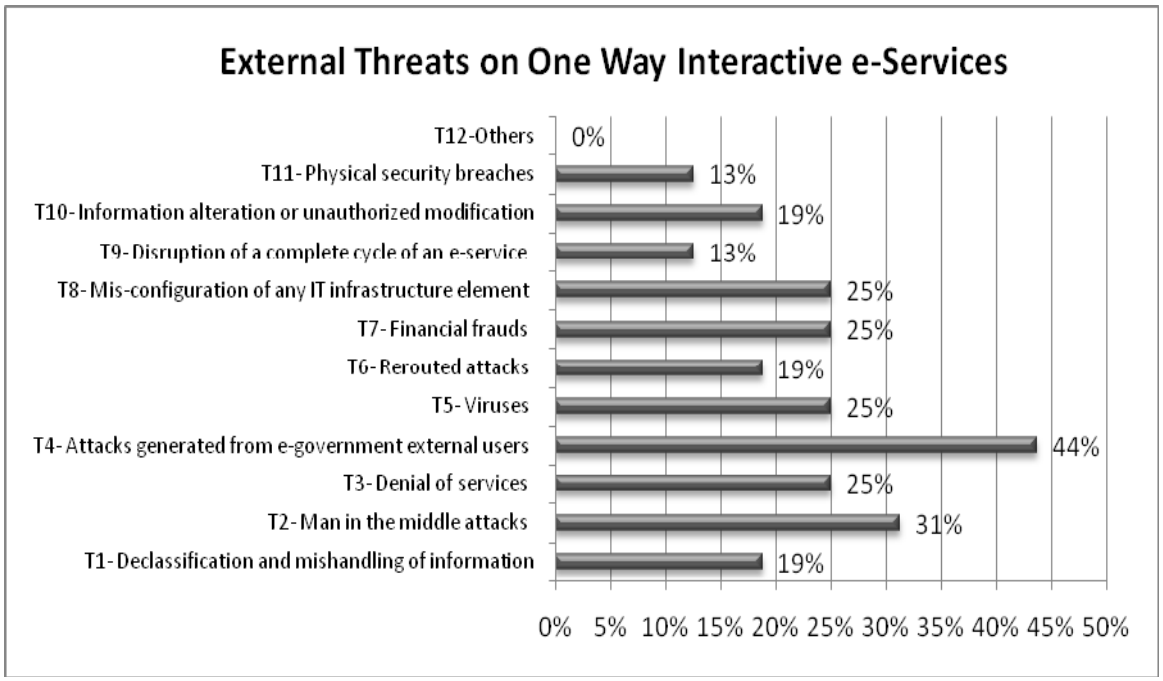


Figure 51: External threats- one way interactive e-services

6.5.2.3. External threats on two way interactive e-services:

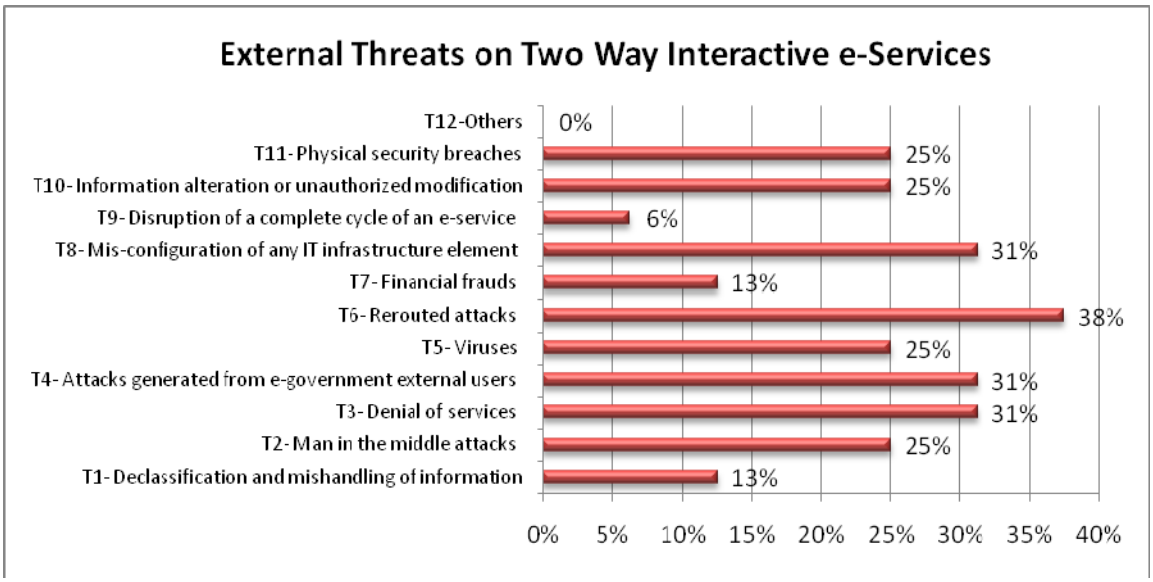


Figure 52: External threats-two-way interactive e-services

6.5.2.4. External threats on transactional e-services:

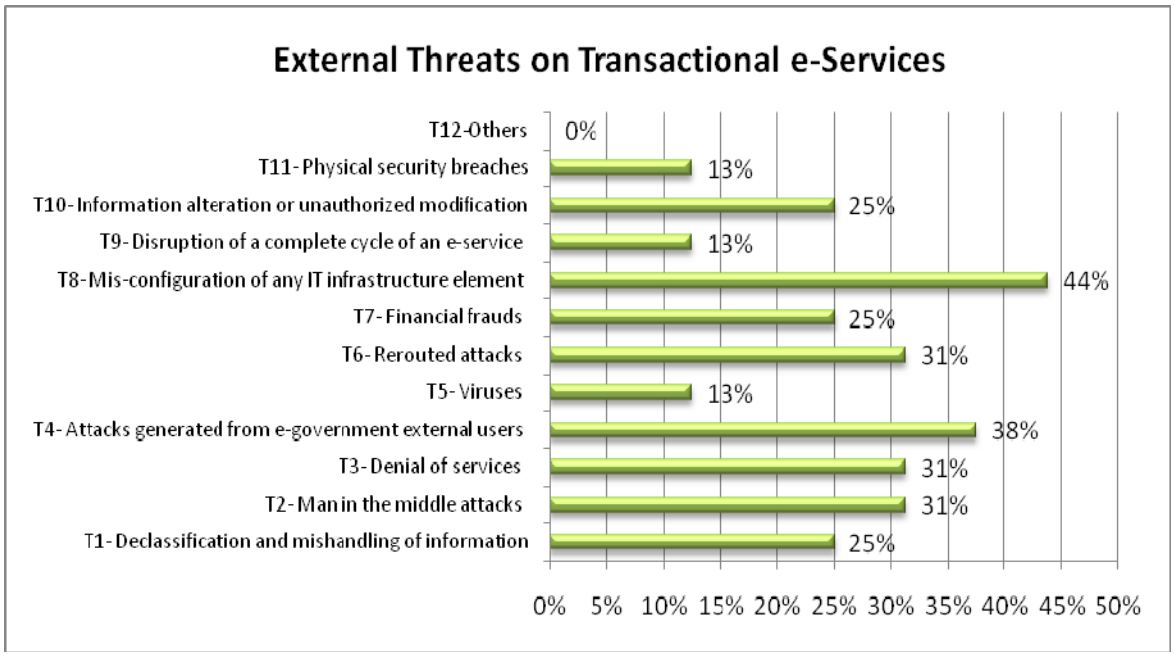


Figure 53: External threats-transactional e-services

6.5.3. *External and internal threats:*

The results of the survey **(Figure 54)** identified that 16 respondents (10%) stated that the severe impact of any threat whether it is external or internal will be due to the lack of security knowledge in how to handle an incident. Twelve (12) respondents (75%) selected the lack of proactive security systems which can reduce the impact and contain the risk, whilst 11 respondents (69%) selected the lack of strong security operational and management systems which assist in the vigilant monitoring of the infrastructure. Another 12 respondents (75%) stated that weak security and IT infrastructure which is vulnerable to any level of attacks or security threats will cause a severe impact of any threat. Only 4 respondents stated that it might be related to the high dependency on the security systems in running the business operation whilst only 2 respondents (13%) stated that it is due to the direct link between the internal e-government infrastructures to the external parties interacting with it.

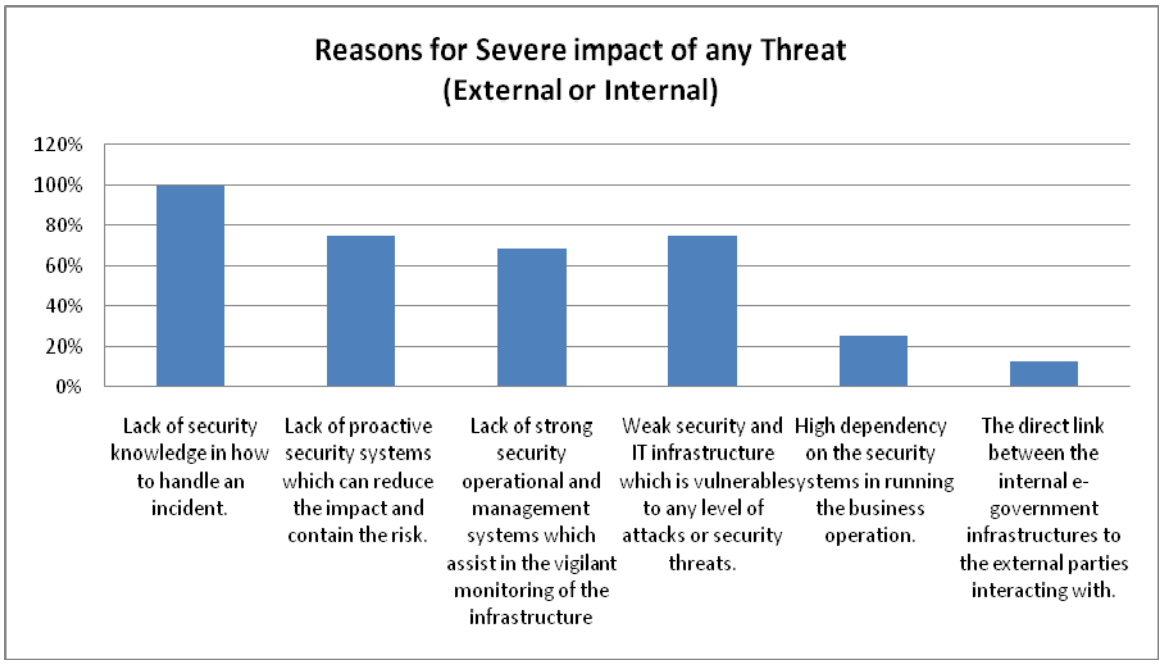


Figure 54: Severe impact of threats

6.5.4. Analysis on information security technology:

The results of the survey **(Figure 55)** identified 8 respondents (50%) confirming that all necessary security technologies are implemented in their organisation whilst 7 respondents (44%) are negating that. Only 2 respondents (13%) stated that some security technologies are implemented.

The implementation of the security architecture in the government departments **(Figure 55):**

- Access control (A1) and logical access control (firewalls) (A11) were rated the highest implemented security technologies in most organisations as it got a 100% selection of the survey respondents.
- Intrusion Detection and Prevention (A2), Anti-Virus and Malicious codes scanners (A3), Authentication and passwords (A4) were the second highest with 88% of the survey respondents' selection.
- 12 Respondents (75%) selected VPN whilst 7 respondents (44%) selected vulnerability scanning tools (A8), digital signature and digital certificates (A9).
- Only 6 respondents (38%) selected cryptography whilst 2 respondents (13%) selected file integrity checks.

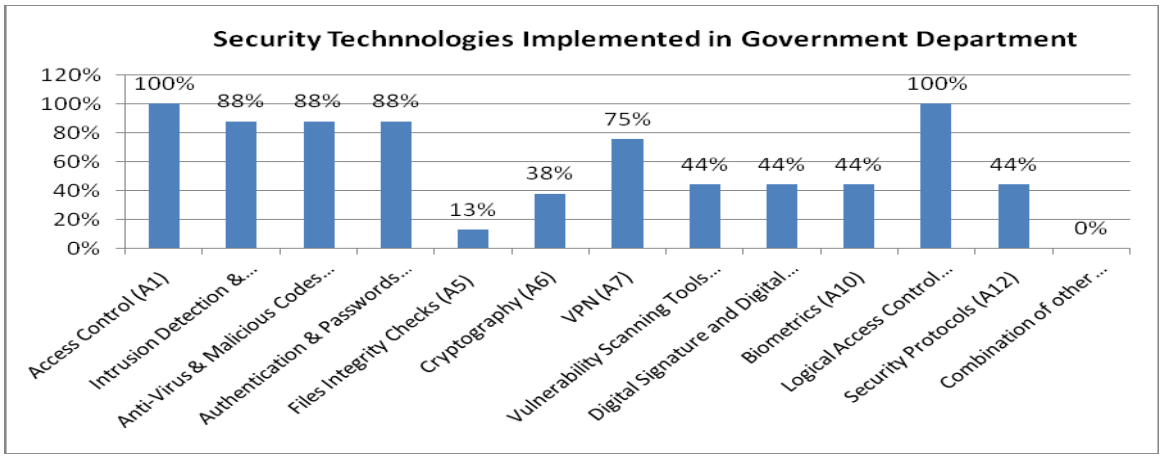


Figure 55: Security technologies implemented in government department

6.5.4.1. Cybercrime security counter measures

- It is strange that when it came to rate the sufficient technologies for the organisation which will provide enough protection the rates were different. Access control (A1) and logical access control (firewalls) (A11) which were selected as the highest technologies implemented in government departments dropped from 100% to 94%.
- Intrusion detection and prevention (A2), Anti-virus and malicious codes scanners (A3), and authentication and passwords (A4) dropped from 88% as implementation rate to 63% -75%.
- File integrity was having a low rate of implementation (13%) yet was given a higher rate as a sufficient security technology which will provide good protection (31%).
- In general most technologies were given good rate when selected as sufficient to provide protection. The key observation that there was no technology out of the list which was found insufficient.

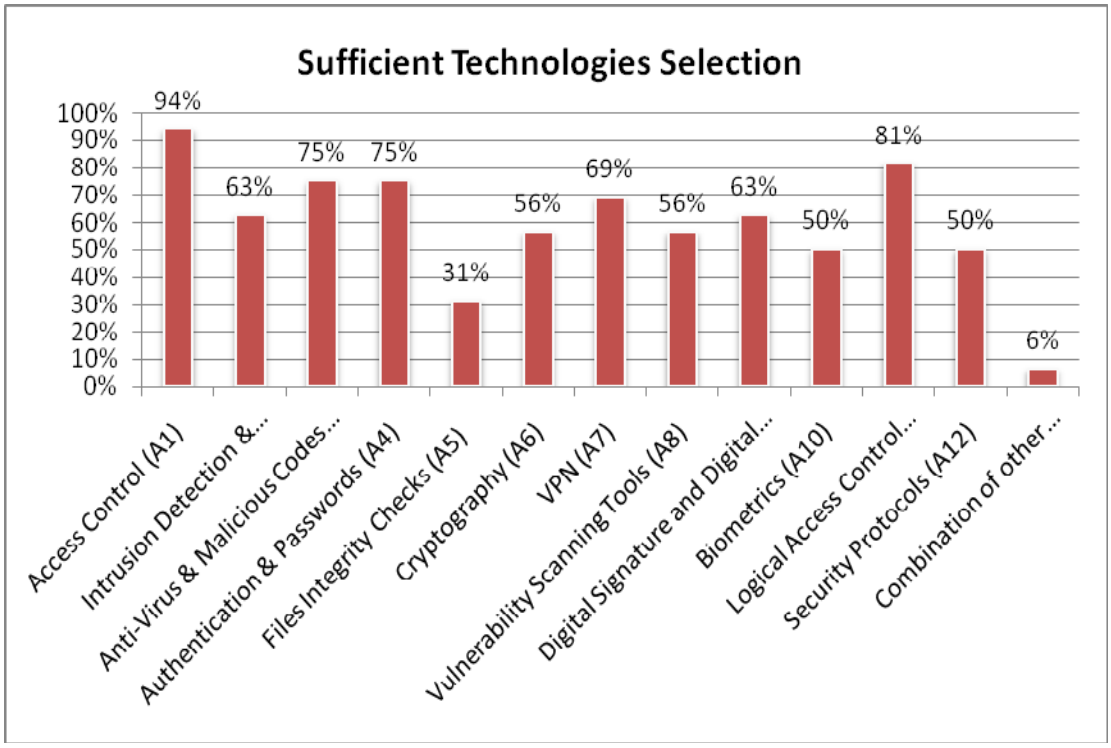


Figure 56: Sufficient security technologies

6.5.4.2. The unnecessary technologies for building a security system:

The results of the survey **(Figure 57)** identified 6 respondents (38%) stated that biometrics technology is not necessary, 4 respondents selected files integrity and checks, 2 respondents (13%) selected anti-virus, cryptography, vulnerability scanning and digital signature as unnecessary to build a security system. The selection might be based on the industrial experience of the respondents yet it does not show high rates as most of the technologies were found essential for building a security system.

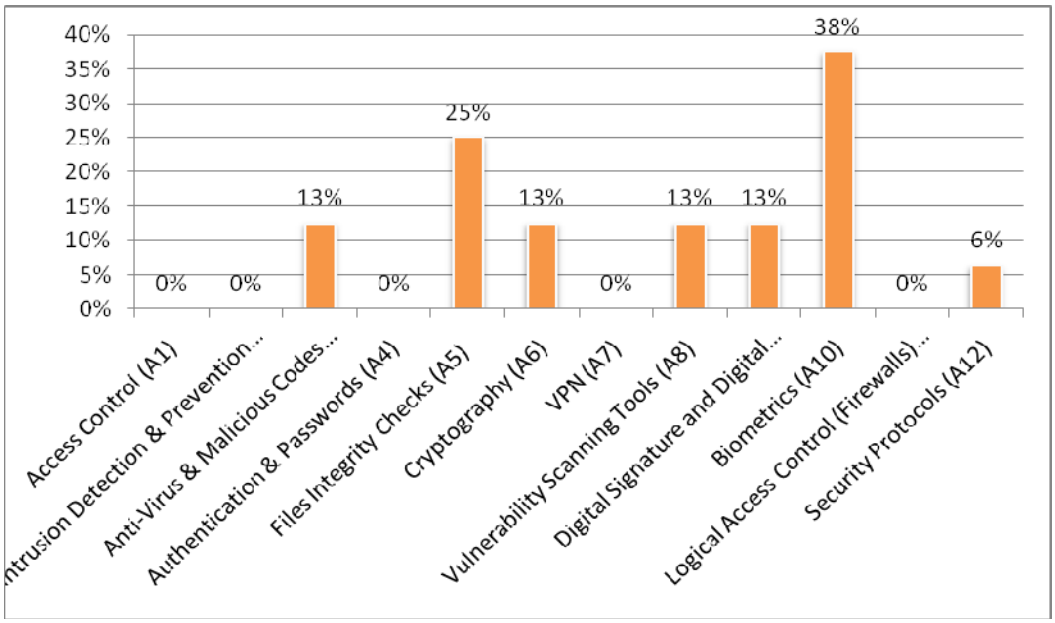


Figure 57: Security technologies

6.5.4.3. The coexistence of all security

- The results showed that 14 respondents (88%) stated that it is not necessary to have all technologies in one layer of a model whilst 2 respondents (13%) answered with yes.
- Rating the technological security level by the number of security technologies available in any organisation:
- A total of 7 respondents (44%) stated yes while 8 respondents (50%) answered with no.

6.5.4.4. Technologies importance:

Access Control (A1):

- 5 respondents (31%) have given the technology between 0–19%
- 1 respondent (6%) rated it between 20–39 %
- 1 respondent (6%) rated it between 40-59%
- 9 respondents (56%) rated it between 80-100%

Intrusion Detection & Prevention (A2):

- 4 respondents (25%) rated the technology between 0-19%
- 2 respondents (13%) rated it between 20-39%
- 1 respondent (6%) rated it between 40-59%
- 3 respondents (19%) rated between 60-79%
- 6 respondents (38%) rated between 80-100%

Anti-Virus & Malicious Codes Scanners (A3):

- 6 respondents (38%) rated the technology between 0-19%
- 1 respondent (6%) rated it between 20-39%
- 1 respondents (6%) rated between 60-79%
- 8 respondents (50%) rated between 80-100%

Authentication & Passwords (A4):

- 6 respondents (25%) rated the technology between 0-19%
- 1 respondents (6%) rated it between 20-39%
- 9 respondents (56%) rated between 80-100%

Files Integrity Checks (A5):

- 8 respondents (50%) rated the technology between 0-19%
- 3 respondents (19%) rated it between 20-39%
- 2 respondent (13%) rated it between 40-59%
- 4 respondents (25%) rated between 80-100%

Cryptography (A6):

- 7 respondents (44%) rated the technology between 0-19%
- 2 respondents (13%) rated it between 20-39%
- 3 respondent (19%) rated it between 40-59%
- 3 respondents (19%) rated between 60-79%
- 1 respondent (6%) rated between 80-100%

VPN (A7):

- 7 respondents (44%) rated the technology between 0-19%
- 2 respondents (13%) rated it between 20-39%
- 4 respondent (25%) rated it between 40-59%
- 1 respondent (6%) rated between 60-79%
- 2 respondents (13%) rated between 80-100%

Vulnerability Scanning Tools (A8):

- 5 respondents (31%) rated the technology between 0-19%
- 1 respondents (6%) rated it between 20-39%
- 1 respondent (6%) rated it between 40-59%
- 6 respondents (38%) rated between 60-79%
- 1 respondent (6%) rated between 80-100%

Digital Signature and Digital Certificates (A9):

- 7 respondents (44%) rated the technology between 0-19%
- 2 respondents (13%) rated it between 20-39%
- 4 respondent (25%) rated it between 40-59%
- 1 respondent (6%) rated between 60-79%
- 2 respondents (13%) rated between 80-100%

Biometrics (A10):

- 6 respondents (38%) rated the technology between 0-19%
- 2 respondents (13%) rated it between 20-39%
- 7 respondent (44%) rated it between 40-59%
- 1 respondent (6%) rated between 60-79%

Logical Access Control (Firewalls) (A11):

- 5 respondents (31%) rated the technology between 0-19%
- 2 respondents (13%) rated it between 20-39%
- 2 respondent (13%) rated it between 40-59%
- 1 respondent (6%) rated between 60-79%
- 6 respondents (38%) rated between 80-100%

Security Protocols (A12):

- 6 respondents (38%) rated the technology between 0-19%
- 2 respondents (13%) rated it between 20-39%
- 5 respondent (31%) rated it between 40-59%
- 2 respondents (13%) rated between 60-79%
- 1 respondents (6%) rated between 80-100%

6.5.4.5. *Security level between A and B*

Let's assume the scenario of organisations a and b exchanging business information over the internet on a frequent basis, do you feel both organisations must have the same level of security technology:

The results of the survey **(Figure 58)** identified 6 respondents (38%) stated yes while 5 respondents (31%) stated no. Only 2 respondents (13%) were not sure while 3 respondents (19%) selected to a certain level.

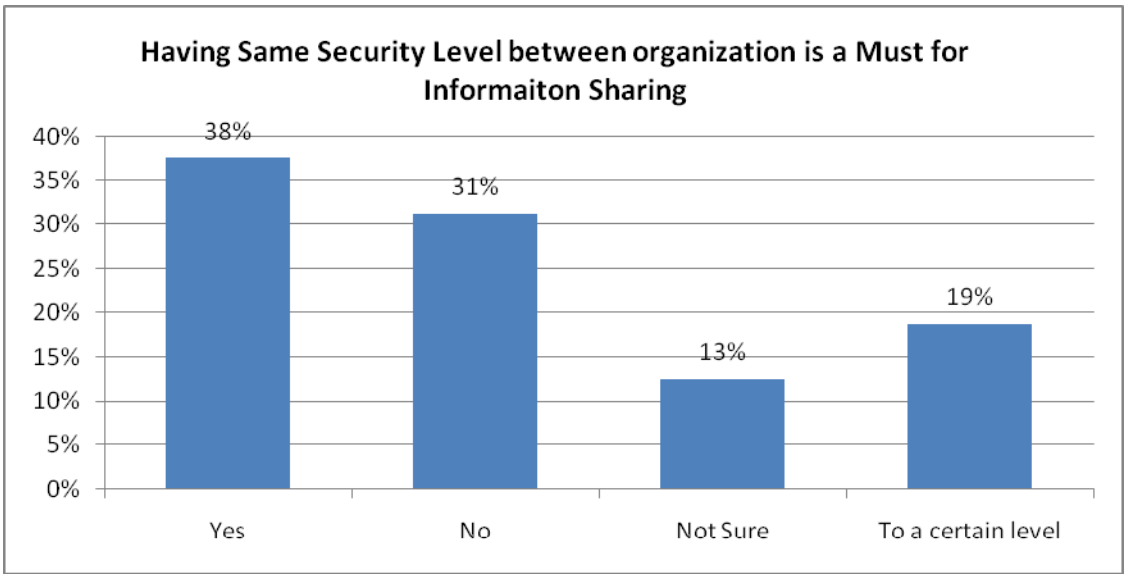


Figure 58: Security alignment between government departments

6.5.4.6. *Having multiple security measures in a single layer*

- A total of 13 respondents (81%) stated no while only 3 respondents (19%) stated yes.
- This highlights the importance of having other aspects than technologies in the security system. Technology layer can't be the only layer which will resolve all security issues.

6.5.4.7. *Technology challenges:*

The results of the survey **(Figure 59)** identified 8 respondents (50%) stated that it is due to the lack of competencies related to the technology applied. The 11 respondents (69%) selected the lack of the lack of security policies as the main reason, 10 respondents (63%) selected the lack of in-depth threat analysis done prior to any technology implementation, 10 respondents (63%) stated that it is due to the lack of management and monitoring, 9 respondents (56%) stated it is due to decision is always based on commercial aspects not technical/security requirements, 8 respondents (50%) selected the integration with other technologies, 5 respondents (31%) said it is due to placing the right technology in the wrong place and a single respondent highlighted that it might be due to other reasons.

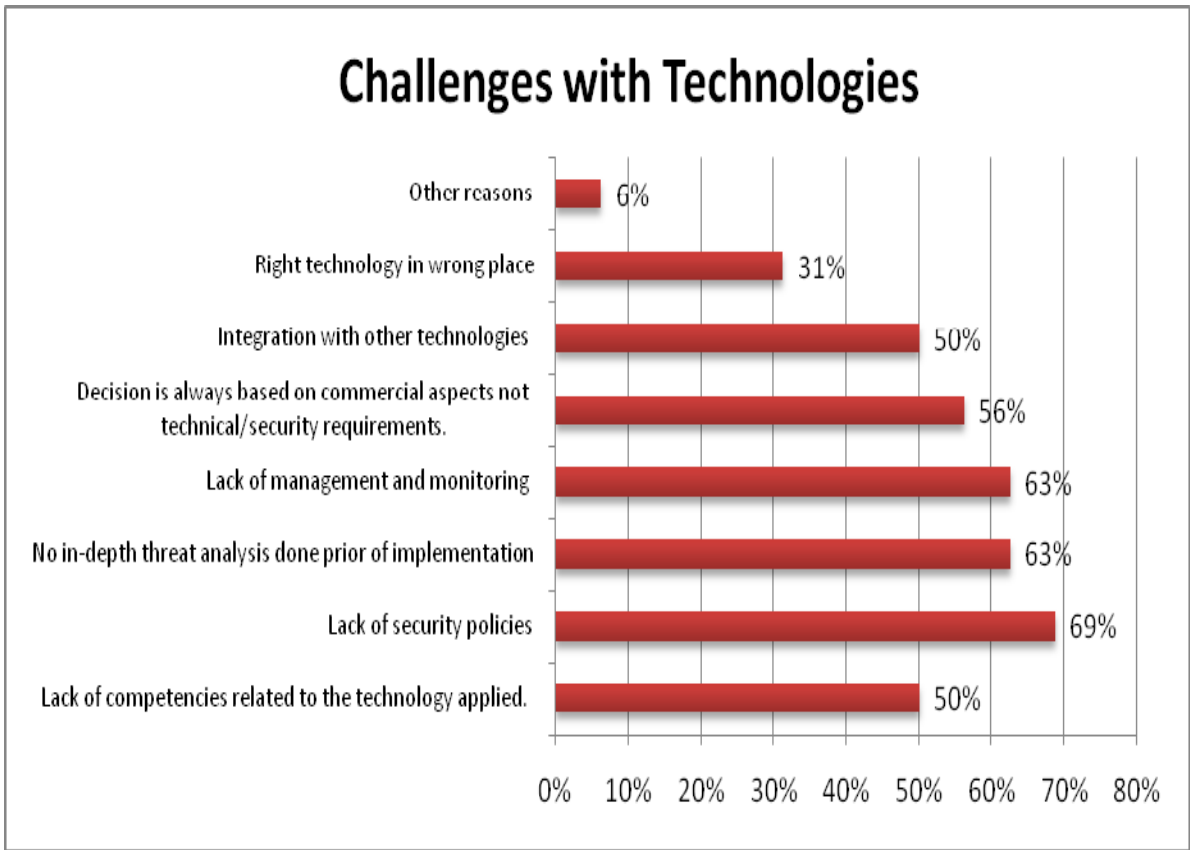


Figure 59: Challenges with Technologies

6.5.4.8. Information flow security condition:

- A total of 8 Respondents (50%) agreed while 8 respondents did not agree. This is a split in the professional opinions from the security practitioners.

6.5.4.9. Security model existence:

- A total of 3 respondents (19%) stated that they have come across a model while 5 respondents (31%) stated that they have not seen any model.

6.5.4.10. Security assessment requirement

- A total of 15 respondents (94%) **(Figure 60)** confirmed that such a model is required and only a single respondent negated.

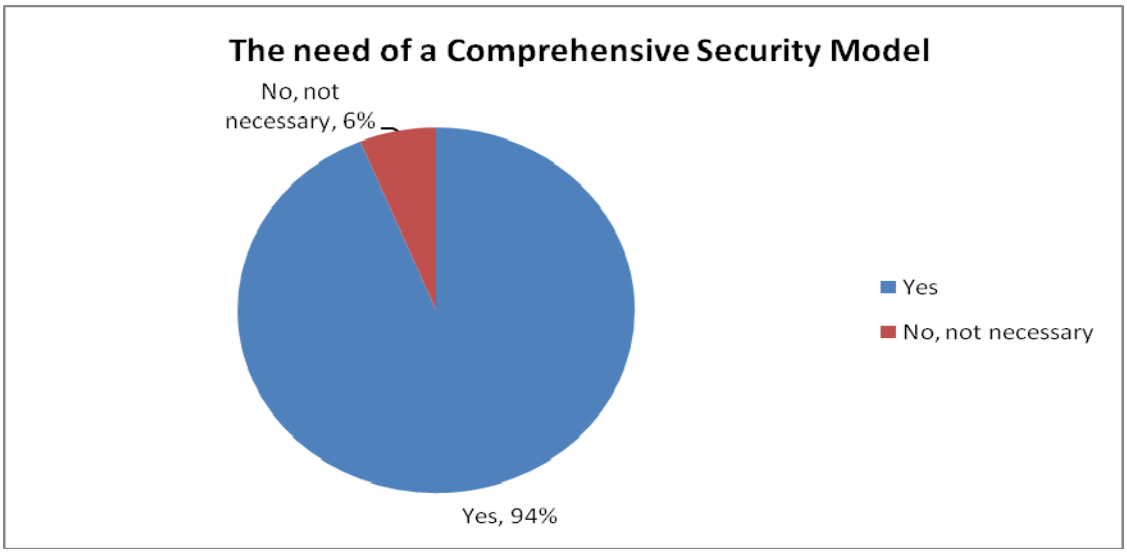


Figure 60: The need of a comprehensive security model

6.5.4.11. Factors of security breaches

- A total of 9 respondents (56%) **(Figure 61)** stated that it is due to the lack of security level matching (org A might be higher than org B in the security level). The reason of not having enough protection measures applied was selected by 13 respondents (81%) whilst 6 respondents (38%) stated it is due to the declassification of information from one side. The 12 respondents (75%) stated that it is due to technical security breaches or flaws. Over trusting the Internet by sending information or allowing communication in clear text

was selected by 13 respondents (81%) whilst 8 respondents (50%) stated that the reason will be due to no common security model/system applied in both organisations.

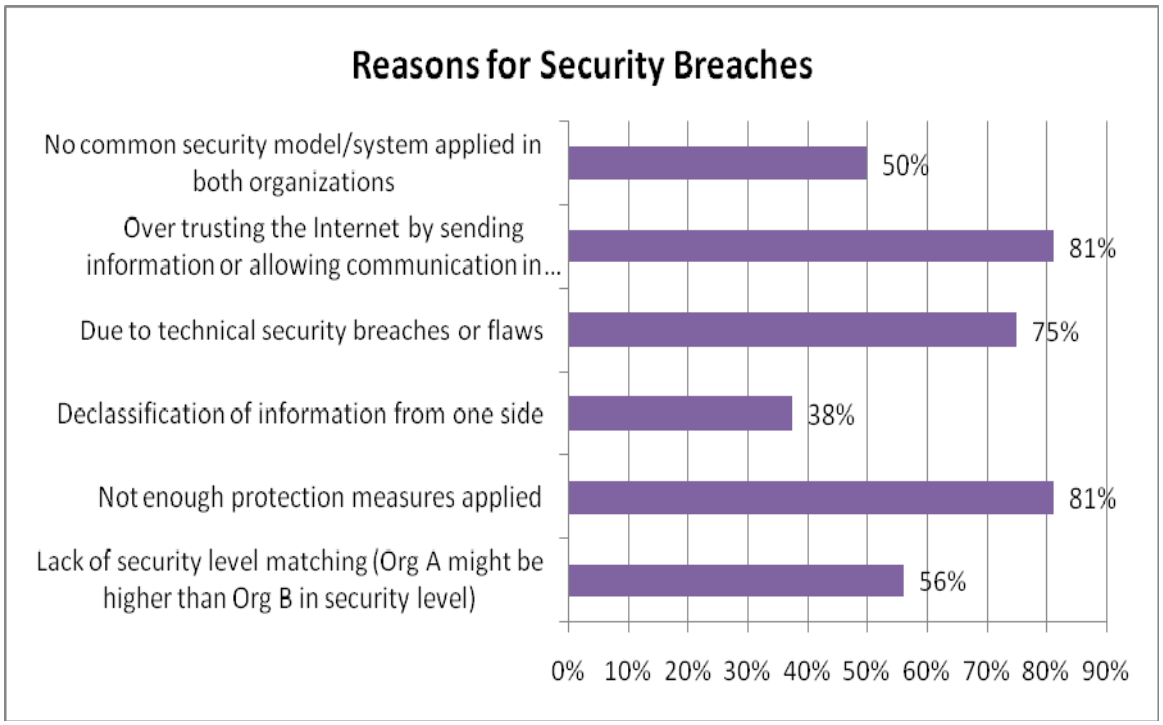


Figure 61: Reasons for Security Breaches

6.5.5. Analysis of information security policies

The importance of the security policy in relations to the full security system in any organisation was rated as:

- A total of 5 respondents (31%) stated that security policies are important while 6 respondents (38%) stated it is very important.
- 14 respondents (88%) stated that the degree of relation between the information security policy and the information security technology is complementary while 3 respondents (19%) stated that they are related.
- A total of 15 respondents (94%) agreed that the coexistence of both the technology layer and the policy layer in one model will assist the security system to be more effective. A single respondent didn't agree.

Importance rating for the security policies:

Password management (B1)

- 5 respondents (31%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 20-39%
- 3 respondents (19%) rated the policy between 60-79%
- 7 respondents (44%) rated the policy between 80-100%

Login process (B2)

- 9 respondents (31%) rated this policy between 0-19%
- 2 respondents (13%) rated the policy between 40-59%
- 2 respondents (13%) rated the policy between 60-79%
- 3 respondents (19%) rated the policy between 80-100%

Logs handling (B3)

- 4 respondents (25%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 20-39%
- 2 respondents (13%) rated the policy between 40-59%
- 4 respondents (25%) rated the policy between 60-79%
- 5 respondents (31%) rated the policy between 80-100%

Computer viruses (B4)

- 6 respondents (38%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 40-59%
- 8 respondents (50%) rated the policy between 80-100%

Intellectual property rights (B5)

- 11 respondents (69%) rated this policy between 0-19%
- 2 respondents (13%) rated the policy between 60-79%
- 3 respondents (19%) rated the policy between 80-100%

Data privacy (B6)

- 5 respondents (31%) rated this policy between 0-19%
- 2 respondents (13%) rated the policy between 40-59%
- 3 respondents (19%) rated the policy between 60-79%
- 6 respondents (38%) rated the policy between 80-100%

Privilege control (B7)

- 6 respondents (38%) rated this policy between 0-19%
- 1 respondents (6%) rated the policy between 40-59%
- 2 respondents (13%) rated the policy between 60-79%
- 7 respondents (44%) rated the policy between 80-100%

Data confidentiality (B8)

- 7 respondents (44%) rated this policy between 0-19%
- 2 respondents (13%) rated the policy between 60-79%
- 7 respondents (44%) rated the policy between 80-100%

Data integrity (B9)

- 8 respondents (50%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 20-39%
- 1 respondents (6%) rated the policy between 40-59%
- 2 respondents (13%) rated the policy between 60-79%
- 4 respondents (25%) rated the policy between 80-100%

Internet connectivity (B10)

- 7 respondents (44%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 20-39%
- 2 respondents (13%) rated the policy between 40-59%
- 4 respondents (25%) rated the policy between 60-79%
- 2 respondents (13%) rated the policy between 80-100%

Administrative policies (B11)

- 6 respondents (38%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 20-39%
- 2 respondents (13%) rated the policy between 40-59%
- 2 respondents (13%) rated the policy between 60-79%
- 5 respondents (31%) rated the policy between 80-100%

Encryption policies (B12)

- 8 respondents (50%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 20-39%
- 3 respondents (19%) rated the policy between 40-59%
- 3 respondents (19%) rated the policy between 60-79%
- 2 respondents (13%) rated the policy between 80-100%

HR security policies (B13)

- 6 respondents (38%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 20-39%
- 3 respondents (19%) rated the policy between 40-59%
- 1 respondent (6%) rated the policy between 60-79%
- 5 respondents (31%) rated the policy between 80-100%

Third party policies (B14)

- 7 respondents (44%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 20-39%
- 3 respondents (19%) rated the policy between 40-59%
- 2 respondents (13%) rated the policy between 60-79%
- 1 respondent (6%) rated the policy between 80-100%

Physical security policies (B15)

- 5 respondents (31%) rated this policy between 0-19%
- 1 respondent (6%) rated the policy between 20-39%
- 4 respondents (25%) rated the policy between 60-79%
- 6 respondents (38%) rated the policy between 80-100%

Operation security policies (B16)

- 2 respondents (13%) rated this policy between 0-19%
- 2 respondent (13%) rated the policy between 20-39%
- 3 respondents (19%) rated the policy between 40-59%
- 4 respondents (25%) rated the policy between 60-79%
- 6 respondents (38%) rated the policy between 80-100%

6.5.5.1. Security breaches and violation of security policies:

- A total of 13 respondents (81%) agreed that violation to the security policies will lead to security breaches whilst only 3 respondents (19%) didn't agree.

- A total of 16 respondents (100%) agreed that if two organisations are interacting with each other over the Internet, they must have enough assurance that they have applied the appropriate security policies in order to maintain the confidentiality, integrity and availability of the information.

- A total of 16 respondents (100%) agreed that having a checklist for the security policy implemented is a good method to assess the level of security for any organisation prior the exchange over the Internet is a good model to adopt.

6.5.6. Analysis of security competencies

- A total of 2 respondents (13%) stated that security competency is more important than the technical competency in the organisation, 6 respondents (38%) stated that security is as important as IT, and 8 respondents (50%) stated it is more important than IT.

- A total of 13 respondents (81%) confirmed that the lack of security competencies in the organisation will be the root cause of security breaches. Only 3 respondents (19%) stated that it is not linked.

- Having a standard or a method to assist the organisation to maintain a high level of security competencies was agreed by 9 respondents (56%) and disagreed by 9 respondents (56%).

- A total of 13 respondents (81%) confirmed that they have experienced a security incident due to the lack of the security competency whilst 3 respondents (19%) negated that.

- A total of 8 respondents (50%) confirmed that the outsourcing of security function in their organisation is due to the lack of competency while 8 respondents (50%) denied that.

6.5.6.1. Method of competency assessment:

- A total of 14 respondents (88%) stated that it is based on the total number of experience in the security field, 7 respondents (44%) stated that it is related to the number of security certifications in the department of security, 7 respondents (44%) stated it is related to the number of security trainings attended, and 9 respondents (56%) believed that it is the total number years in the IT field.

- Assessing the security competency in an organisation is a good method for identifying the level of security of an organisation. This method was agreed on (**Figure 62**) by 13 respondents (81%) whilst disagreed with by only 3 respondents (19%).

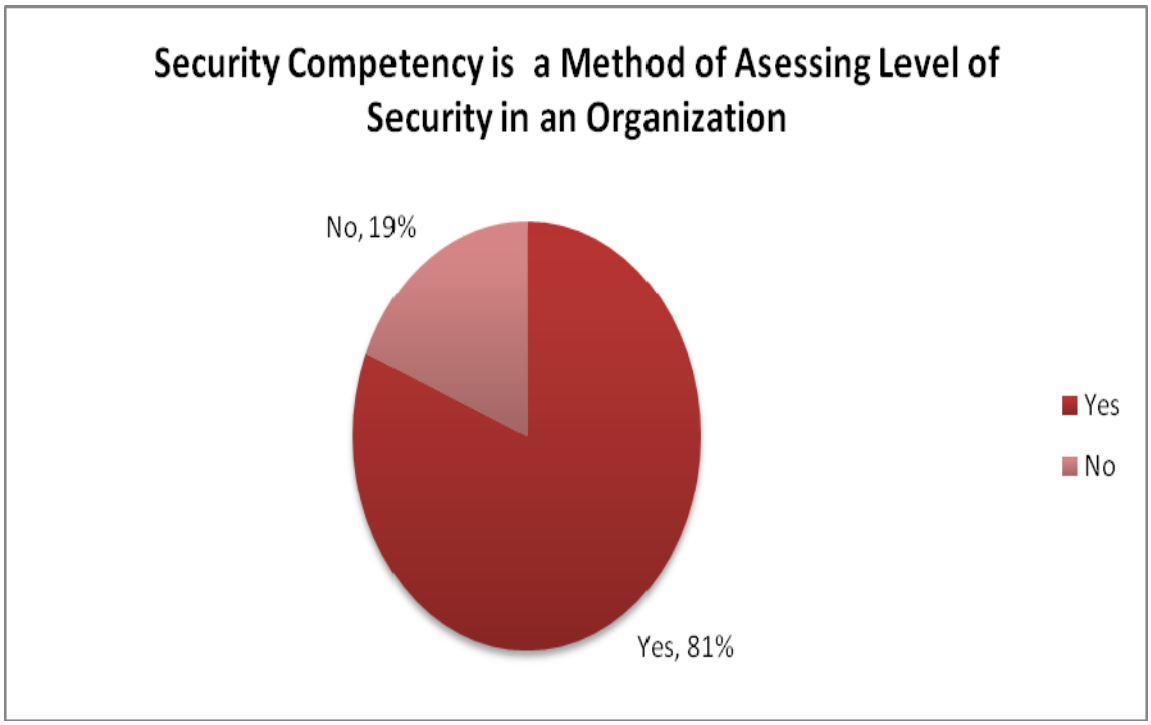


Figure 62: Security competencies as an assessment method

6.5.6.2. The mandatory security competencies required in any organisation

- A total of 16 respondents (100%) **(Figure 63)** agreed that security operation and management (C1) is a mandatory competency to have in any organisation. The 12 respondents (75%) stated that security architecture and development (C2) is a must to have whilst another 12 respondents (75%) stated its security policies development (C4). The security implementation and configuration (C9) competency was selected as the second highest competency required by 14 respondents (88%), 9 respondents (56%) stated that security analysis (C10) is important, 6 respondents (C8) stated it is laws and regulations, 5 respondents (C3) stated ethical hacking. Computer Forensics (C5) and cryptography (C6) competencies were selected by 4 respondents (25%) and only 3 respondents (19%) selected security programming.

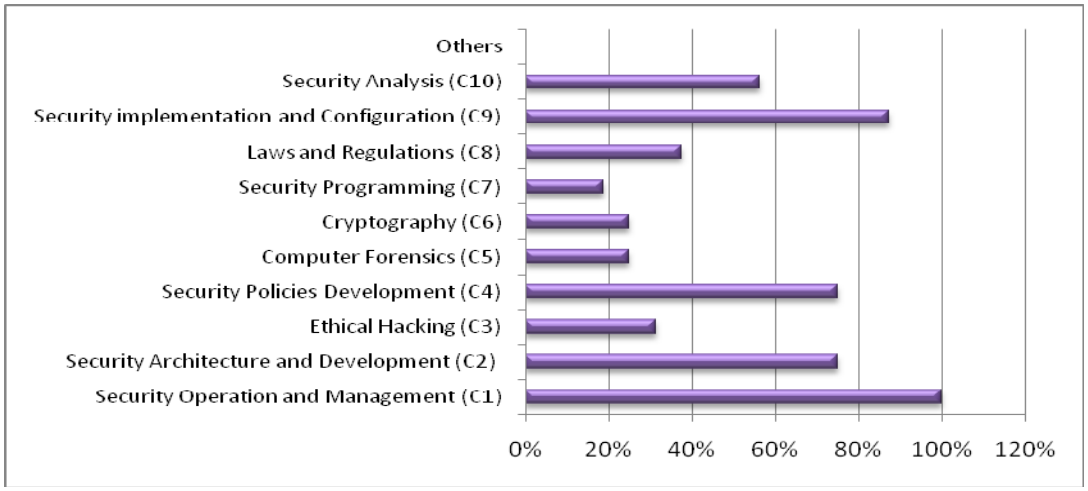


Figure 63: Mandatory security competencies

- Having a security competency layer as a part of a security model will enhance the security level of an organisation as a complement to other important layers also was agreed by 16 respondents (100%).
- A total of 15 respondents (94%) confirmed that there is a direct link between security competencies and security technologies implemented in any organisation.

6.5.7. Analysis of information security management and monitoring

- A total of 8 respondents (50%) stated that information security management and monitoring is very important, 7 respondents (44%) stated that it is important but not essential, whilst a single respondent stated it is not important.
- Information security and management must be there for all security technologies implemented as per the opinion of 12 respondents (75%) while it is not necessary to have by 4 respondents (25%).
- A total of 14 respondents (88%) stated that there is a direct link between strength of the security programme/system in any organisation and the strength of the security. Only a single respondent stated that there is no direct link between the two.
- Having a good level of security management and monitoring can give a good indication of the strength of the security competency, policies, and technologies in the organisation was agreed by 14 respondents (88%) whilst not agreed by 2 respondents (13%).

6.5.7.1. Strength of the security management and monitoring:

- 6 respondents (38%) **(Figure 64)** identified that the strength of the security management and monitoring is measure based on the number of incidents handled, 13 respondents (81%) stated it is based on the existence of the standard security operation procedure, 10 respondents (63%) stated it is based on infrastructure supporting this function, 13 respondents (81%) stated it is based on response time to incidents, and 11 respondents (69%) stated it is based on correlation of data collected from all security devices.

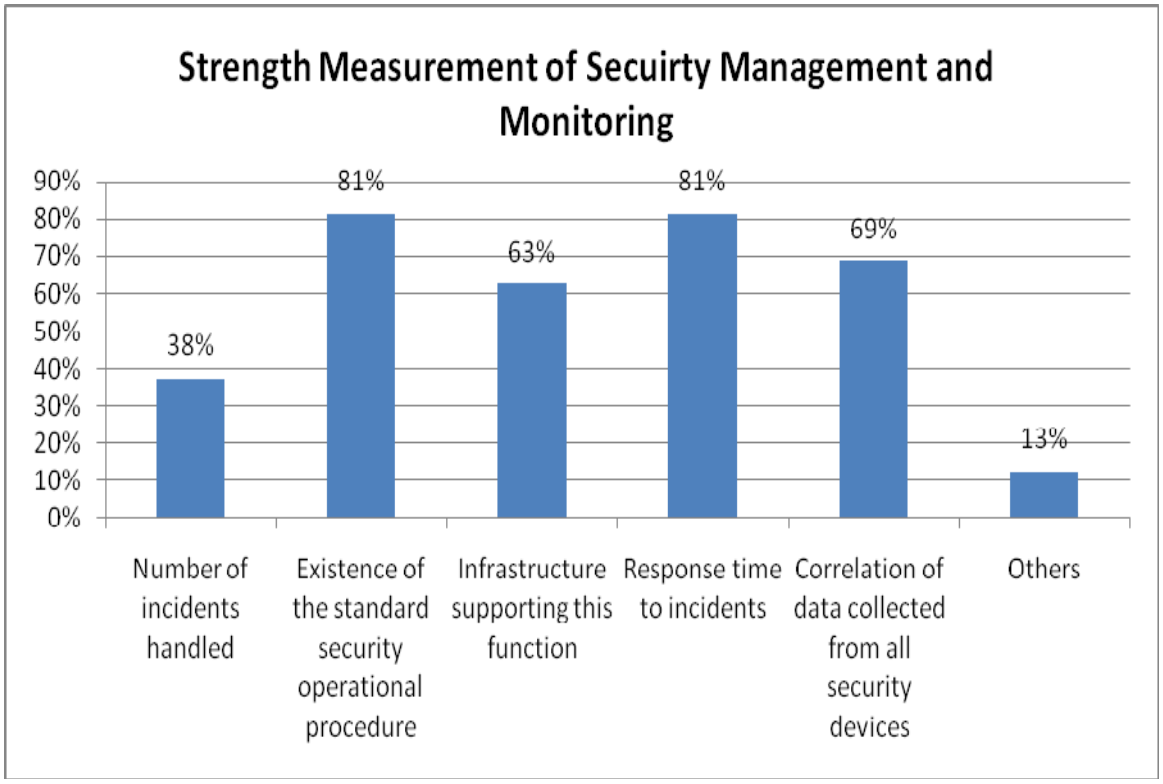


Figure 64: Strength measurement of security management

- A total of 11 respondents (69%) stated that having organisation A and B exchanging information over the Internet will stress the need of security management and monitoring. Only 5 respondents (31%) disagreed with this statement.

6.5.7.2. Components of the security management and monitoring layer:

- The results of the survey **(Figure 65)** identified 16 respondents (100%) selected operational policies and procedures (D1), 10 respondents (63%) selected management tools (D2), 14 respondents selected correlation and data management (D3), 13 respondents (81%) selected reporting and responses (D4), and 10 respondents (63%) stated it is analysis and human intervention (D5).

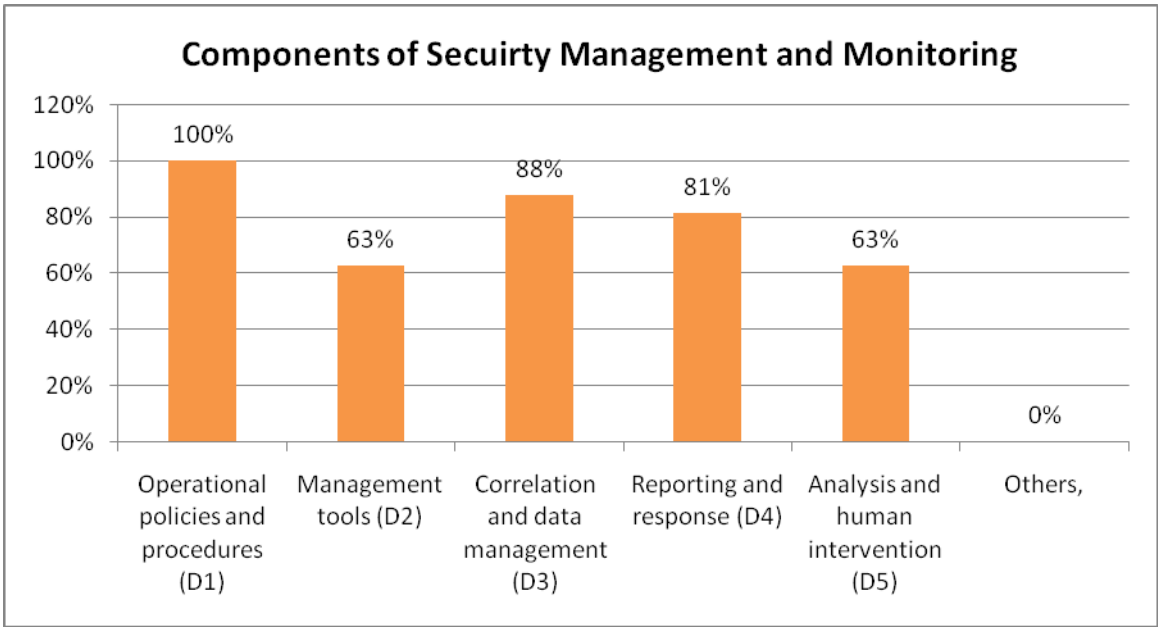


Figure 65: Components of security management and monitoring

- A total of 14 respondents (88%) confirmed that having security operation and management as part of the risk assessment model is the right thing to do. Only 1 respondent (6%) didn't agree with that.
- Security operation and management was given an importance rate between 50-70% by 6 respondents (38%) and a rate of 70-100% by 10 respondents (63%).
- A total of 5 respondents (31%) stated that they have experienced security incidents which were due to lack of security operations and management, 5 respondents (31%) stated no, while 3 respondents (19%) could not answer this question.

- Having a security operation and management as a local competency in the organisation was confirmed by 10 respondents (63%) and only 7 respondents (44%) stated that it is outsourced.

6.5.8. Analysis of decision factor:

Factors will assist in reaching the decision for selecting or considering a security technology, policy, operational procedure, or hiring a resource with certain security competency:

- A total of 10 respondents (63%) stated that it is based on the cost factor, 9 respondents (56%) stated that it is based on the background of the security subject, 11 respondents stated that it is based on being a need or a want, and 12 respondents relied on the availability of competencies/technologies and ease of implementation **(Figure 66)**.

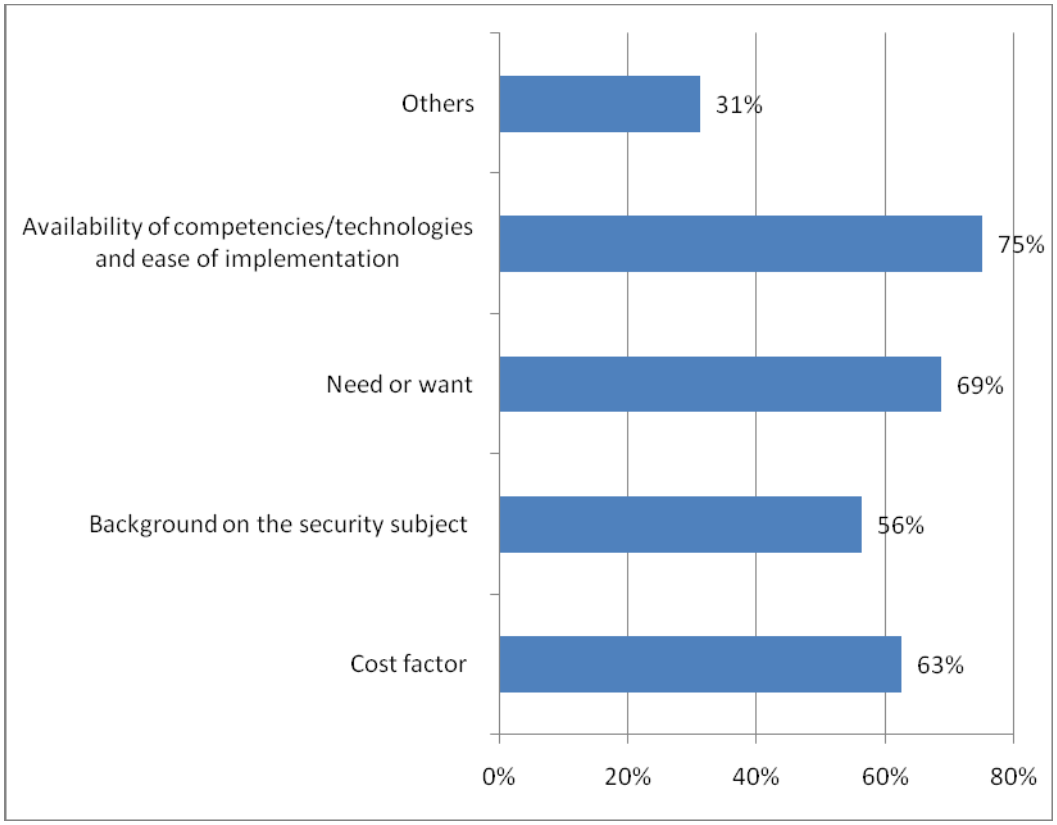


Figure 66: Decision factors

6.5.8.1. Decision Factors

- Not having enough information on the subject was identified by 9 respondents (56%) **(Figure 67)** as a factor which may affect the decision process. The 8 respondents (50%) stated that not having an ROI justification will affect the decision, 6 respondents (38%) selected the lack of competencies on the technology within the organisation, 9 respondents (56%) selected high cost of implementation, training, and transition, and 9 respondents (56%) selected major and core business processes change.

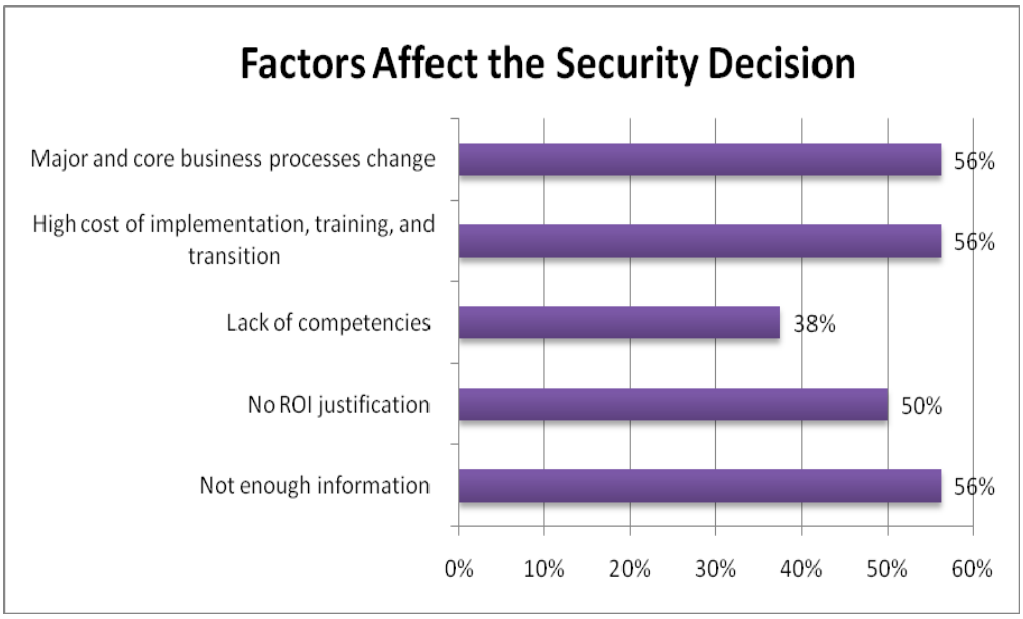


Figure 67: Factors affect the security decision

- A total of 9 respondents (56%) stated that decision on the technology layer of any security system for an organisation will have a deep impact on the competencies, policies, and operations. Only 7 respondents (44%) stated that no impact will be there if the decision was carefully studied.
- A total of 10 respondents (63%) stated that taking a decision to adopt some policies and leave others in any organisation might defeat the security programme whilst 6 respondents (38%) saw no effect will be there if the security technologies were well architected.

- The decision on the security programme of any organisation will have an effect on the method of communication and interaction the organisation has with others as confirmed by 9 respondents (56%) and disagreed with by 7 respondents (44%).
- A total of 14 respondents (88%) confirmed that the decision factor can be one of the factors an organisation must be assessed on as part of any security assessment programme while a single respondent didn't believe so.
- Ten (10) respondents (63%) confirmed that there is no method of having the security decision layered on technologies, policies, and competencies so it does not create a severe impact on the overall security programme in the organisation. Only 5 respondents (31%) confirmed that there is a method but didn't mention it.
- The objective of limiting and synchronizing the decision making process between two organisations A and B communicating/exchanging information with each other can be achieved as stated by 9 respondents (56%) while 3 respondents (19%) stated that this can't be achieved.
- A total of 7 respondents (44%) confirmed that they have experienced a security breach in their organisation which was directly or indirectly related to a wrong decision made on the security programme/system of the organisation, 9 respondents (56%) stated that this was not experienced.

6.6. Analysis of the correlation questions related to different services:

6.6.1. Reasons for low usability of e-services

- The number of participants answered this section of the questionnaire was 10 out of the total of 16 participants (63%). This might be due to the low frequency of the information publish e-service use which might be indirectly due to the low quality of the content of the portals.
- The percentage of each sub layer was taken by dividing over the number participants participated in this section (10) not the total number of the survey participants (16).
- Achieving a 40% of an applicability rate will give a strong support to implement the security measure in the organization. The rate of 40% was determined to be the

lowest acceptable level for any security measure applicability rate/percentage. This will be applied on all e-services surveyed and it is based on the industrial experience. The rate might be changed from a security practitioner to another. The observation of having some sub layers lower than others will remain the same as security practitioners select based on their perception of how a security measure will mitigate a security threat.

6.6.2. Information publishing e-services:

Table 32: Information publishing e-services

Layer	Sub layers/Cells															
Technology	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12				
	50%	80%	50%	20%	40%	20%	10%	60%	30%	10%	100%	10%				
Policies	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
	50%	30%	70%	40%	20%	30%	20%	30%	60%	40%	60%	30%	20%	40%	70%	80%
Competencies	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10						
	80%	70%	60%	50%	30%	20%	20%	50%	90%	50%						
Operational Mgmnt	D1	D2	D3	D4	D5											
	80%	70%	60%	80%	50%											
Decision Factor	E1	E2	E3	E4	E5											
	70%	60%	70%	60%	0%											

- The applicability survey results show the following:
- In the technology layer the following security technological measures were rated low:
    - Authentication and Passwords (A4) (20%)
    - Cryptography (A6) (20%)
    - VPN (A7) (10%)
    - Digital Signature and certificates (A9) (30%)
    - Biometrics (A10) (10%)
    - Security Protocol (A12) (10%)

- In the policy layer the following policies were rated low:
    - Login Process (B2) (30%)
    - Intellectual Property Rights (B5) (20%)
    - Data Privacy (B6) (30%)
    - Privilege Control (B7) (20%)
    - Data Confidentiality (B8) (30%)
    - Encryption Policies (B12) (30%)
    - HR Security Policies (B13) (20%)
- In the competency layer the following competencies were found unnecessary:
    - Computer Forensics (C5) (30%)
    - Cryptography (C6) (20%)
    - Security Programming (C7) (20%)
- In the decision factors layer, the following factor was found unnecessary:
    - FUD (E5) (0%)

The security measures given a low percentage were justified as they were unrelated to an information publishing e-service. Some of the security measures given low percentages might be found needed if the information publishing online service is designed for selected partners and key customers and contains sensitive information which is meant to be accessed only by authorized users. Such security measures like the security programming, computer forensics, encryption, authentication and passwords, and intellectual property protection policies will be required to provide strong protection and add to the reliability of the e-service. The Fear, Uncertainty, and Doubt (FUD) can't be a strong decision factor affecting the other security measures since the information publishing e-service is well known to most IT executives and management.

6.6.3. *One way interactive e-services:*

Table 33: One-way interactive e-services

Layer	Sub layers/Cells															
Technology	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12				
	70%	100%	50%	80%	50%	30%	20%	70%	40%	20%	90%	20%				
Policies	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
	70%	90%	70%	40%	20%	30%	20%	30%	60%	40%	60%	30%	20%	40%	70%	80%
Competencies	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10						
	80%	70%	60%	50%	30%	20%	20%	50%	90%	50%						
Operational Mgmnt	D1	D2	D3	D4	D5											
	80%	70%	60%	80%	50%											
Decision Factor	E1	E2	E3	E4	E5											
	70%	60%	70%	60%	0%											

- In the technology layer the following security technological measures were rated low:
  - Cryptography (A6) (30%)
  - VPN (A7) (20%)
  - Biometrics (A10) (20%)
  - Security Protocol (A12) (20%)
- In the policy layer the following policies were rated low:
  - Intellectual Property Rights (B5) (20%)
  - Data Privacy (B6) (20%)
  - Privilege Control (B7) (20%)
  - Encryption Policies (B12) (30%)
  - HR Security Policies (B13) (20%)
- In the competency layer the following competencies were found unnecessary:
  - Computer Forensics (C5) (30%)
  - Cryptography (C6) (20%)
  - Security Programming (C7) (20%)

- In the decision factors layer, the following factor was found unnecessary:
    - FUD (E5) (0%)

The one way interactive e-service is an online service which allows forms to be downloadable to the users' computers in order to apply for a government service. All security measures rated low made sense from security practice point of view. The Fear, Uncertainty, and Doubt (FUD) have no effect on the other layers and sub layers as the services is well known to IT executives and management.

6.6.4. Two way interactive e-services:

Table 34: Two way interactive e-services

Layer	Sub layers/Cells															
Technology	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12				
	80%	70%	60%	70%	70%	30%	20%	60%	60%	20%	80%	50%				
Policies	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
	80%	80%	60%	70%	50%	60%	60%	70%	70%	60%	40%	50%	40%	50%	60%	80%
Competencies	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10						
	90%	80%	80%	60%	60%	60%	50%	50%	90%	50%						
Operational Mgmnt	D1	D2	D3	D4	D5											
	90%	90%	60%	80%	70%											
Decision Factor	E1	E2	E3	E4	E5											
	70%	70%	90%	70%	10%											

- In the technology layer the following security technological measures were rated low:
    - Cryptography (A6) (30%)
    - VPN (A7) (20%)
    - Biometrics (A10) (20%)
- In the decision factors layer, the following factor was found unnecessary:
    - FUD (E5) (10%)

It can be noticed that the more interactive the e-service will be, the more security measures it will require. The technological security measures rated low can be argued as cryptography and VPN might be needed if the forms are classified and the information filled is private to the citizen.

6.6.5. Transactional e-services:

Table 35: Transactional e-services

Layer	Sub layers/Cells															
Technology	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12				
	80%	70%	60%	90%	90%	60%	40%	70%	80%	30%	80%	60%				
Policies	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
	80%	90%	90%	80%	60%	70%	80%	80%	80%	60%	80%	80%	40%	50%	50%	80%
Competencies	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10						
	100%	90%	60%	60%	60%	60%	50%	80%	90%	60%						
Operational Mgmnt	D1	D2	D3	D4	D5											
	70%	80%	80%	80%	70%											
Decision Factor	E1	E2	E3	E4	E5											
	70%	60%	90%	80%	60%											

The only security measure rated low in the transactional e-service survey was the biometrics (A10) (30%) which might be due to the lack of implementation of such technology in the region. The author can argue that such a technology can be useful for enhancing the accessibility control to terminals or laptops used for online transactions. In addition, since most of the online transactions are conducted over the Internet using SSL and applications layer security, the biometrics technology was not found popular in Dubai. It is mainly used for physical security access control which is a narrowed implementation of its broaden capabilities.

6.6.6. *Combination of all services:*

Table 36: Combination of all services

Layer	Sub layers/Cells															
Technology	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12				
	100 %	70%	80%	90%	100 %	80 %	50 %	70%	90%	30 %	100 %	70 %				
Policies	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
	90%	90%	90%	70%	80%	80 %	90 %	90%	100 %	80 %	90%	80 %	60 %	70 %	90 %	100 %
Competencies	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10						
	100 %	100 %	90%	80%	80%	70 %	60 %	100 %	100 %	60 %						
Operational Mgmnt	D1	D2	D3	D4	D5											
	90%	90%	100 %	70%	80%											
Decision Factor	E1	E2	E3	E4	E5											
	80%	70%	100 %	100 %	10%											

The only security technology was found low in the applicability is the Biometrics. Although there is a strong campaign to promote Biometrics in Dubai, it was observed that the security practitioners participated in the survey strongly believe that the technology is not needed for the government online services. This might be due to the lack of implementations or by being a complementary measure if all measures are put in place. Fear, Uncertainty, and Doubt (FUD) was the only sub layer and security factor found unnecessary in the survey conducted for all types of e-services or the combination of all of them. This depicts that the security factors which can affect the other layers or aspects of the security programme are cost, need, awareness, and technological availability.

Table 37: The model key

	Category		Category	
Technology	Access Control	A1	Intrusion Detection and Prevention	A2
	Anti Virus and Malicious Code	A3	Authentication and Passwords	A4
	Files and Integrity Check	A5	Cryptography	A6
	VPN	A7	Vulnerability Scanning Tools	A8
	Digital Signatures and Certificates	A9	Biometrics	A10
	Logical Access Control (Firewalls)	A11	Security Protocol	A12
Policies	Password Management	B1	Log-in Process	B2
	Logs Handling	B3	Computer Viruses	B4
	Intellectual Property Rights	B5	Data Privacy	B6
	Privilege Control	B7	Data Confidentiality	B8
	Data Integrity	B9	Internet Connectivity	B10
	Administrative Policies	B11	Encryption Policies	B12
	HR Security Policies	B13	Third Party Policies	B14
	Physical Security Policies	B15	Operation Security Policies	B16
Competencies	Security Operation and management	C1	Security Architecture and development	C2
	Ethical Hacking	C3	Security Policies and development	C4
	Computer Forensics	C5	Cryptography	C6
	Security Programming	C7	Laws and regulation	C8
	Security Implementation and Configuration	C9	Security Analysis	C10
OPS mgmt	Operational Policies and Procedures	D1	Management Tools	D2
	Correlation and data mining	D3	Reporting and Response	D4
	Analysis and Human intervention			D5
Decision	Cost	E1	Awareness	E2
	Need	E3	Technologies Availability	E4
	FUD	E5		

6.7. Results/Observations

- A total of 50% of the participants of questionnaire B confirmed that the challenges an e-government is facing in terms of information flow and sharing are related to the low trust between the e-government body and government departments.
- A total of 69% of the participants indicated that it might be due to the lack of common rules or standards which control the flow of information.

- A high percentage of participants (88%) confirmed the need of a standard assessment model for the e-government in order to synchronize the level of the security for intra and inter communication. This confirms that the new model will find a good level of acceptance among the security practitioners. The positive impact of the standard security assessment on the government department in encouraging them to exchange information between themselves and the government authority was confirmed by 88% of the participants.
- The majority of the respondents (47%) indicated that the combination of all e-services is what the e-government departments offer.
- A further analysis was conducted based on the top internal and external threats occurred in the survey conducted for the 5 areas (general, information publishing, one or two ways interactive, and transactional). A frequency rate of at least 4 times was chosen to selected the most frequent threats out of the top 7 threats appearing in all the five areas.
- The **top 7 internal threats** for an organisation offering **information publishing** online services are disgruntled employees, viruses, leakage of information, failure of restoration, lack of security competency, information dealers looking for classified and sensitive information, and loss or corruption of data.
- The **top 7 internal threats** for an e-government organisation offering a **one way interactive** e-service were viruses, failure of restoration, lack of security competency, leakage of information, the high mobility of the government staff from their roles, disgruntled employees, and mission critical attacks.
- The **top 7 internal threats** for an e-government organisation offering a **two way interactive** e-services are lack of security competency, exposure of classified data, leakage of information, disgruntled employees, viruses, information dealers, and failure of restoration.
- The **7 top internal threats** of an e-government organisation offering a **transactional e-service** are lack of security competency, disgruntled employees, exposure of classified data, leakage of information, data and records alteration, information dealers, and failure of restoration.

- Out of the internal threats selected by the participants the internal threats repeated at least 4 times in the five surveyed areas are listed in the table blow with their types.

Table 38: Internal threats identified

Threat	Frequency of Occurrence in the 5 areas Surveyed	Type
Disgruntled employees	5	P
Lack of security competency	5	C
Viruses	4	T
Leakage of information	5	P
Failure of restoration	4	O

- From the table of the types of internal threats, it can be noticed from the above table that the internal threats having a frequency of at least 4 times are mixed from different types and not only related to technologies or policies. These threats can only be mitigated through applying the counter security measures related to the types of threats identified.

6.7.1. External threats

- The highest 7 general threats identified are the mis-configuration of any IT infrastructure element, financial frauds, rerouted attacks, viruses, denial of service, man in the middle attacks, and declassification and mishandling of information.
- The top 7 external threats for organisations offering information publishing services are rerouted attacks, denial of services, physical security breaches, viruses, attacks generated from e-government external users, declassification and mishandling of information and miscofiguration of any IT infrastructure element.
- The top 7 external threats on organisations offering a one way interactive e-services are attacks coming from other government departments, man in the middle attacks, denial of services attacks, viruses, mis-configuration of any IT infrastructure element, financial frauds, and declassification and mishandling of information.

- The top 7 external threats on organisations offering two way interactive e-services are rerouted attacks, attacks generated from e-government external users, denial of services, man in the middle attacks, mis-configuration of any IT infrastructure element, information alteration, and physical security breaches.
- The highest 7 threats for an organisation offering transactional online services are mis-configuration of any IT infrastructure element, attacks generated from e-government external users, rerouted attacks, denial of services, and man in the middle attacks.
- A further analysis was conducted on the top 7 external threats occurred for the 5 areas surveyed. Threats occurred 4 times or higher in the five surveyed areas are listed in the table below.

Table 39: External threats identified

Threat	Frequency of Occurrence in the 5 areas Surveyed	Type
Mis-configuration of any IT infrastructure element	5	T
Rerouted Attacks	4	T
Viruses	4	T
Denial of Services	5	T
Man in the middle attacks	5	T
Attacks generated from e-government external users	4	T

6.8. The correlation section analysis:

- The list of security measures rated with low percentages was the same for both information publishing and one way interactive forms and started to be less in the two way interactive e-services.

- In the information publishing e-services 6 security technologies were rated between 10-30%, 7 security policies were rated either 20% or 30%, 3 security competencies were rated either 20% or 30% and one decision factor was rated 0%.
- The one way interactive e-service has 4 security technologies rated either 20% or 30%, 6 security policies were rated either 20% or 30%, 3 competencies were rated 20% or 30% and one decision factor was rated 0%.
- In the two way interactive e-services only 3 technologies were rated either 20% or 30% while one decision factor was rated 10%.
- There are 3 security technologies which were rated low (10%-30%) in information publishing, one interactive and two interactive e-services. These security technologies are **(Figure 68)**:
    - Cryptography (A6)
    - VPN (A7)
    - Biometrics (A10)

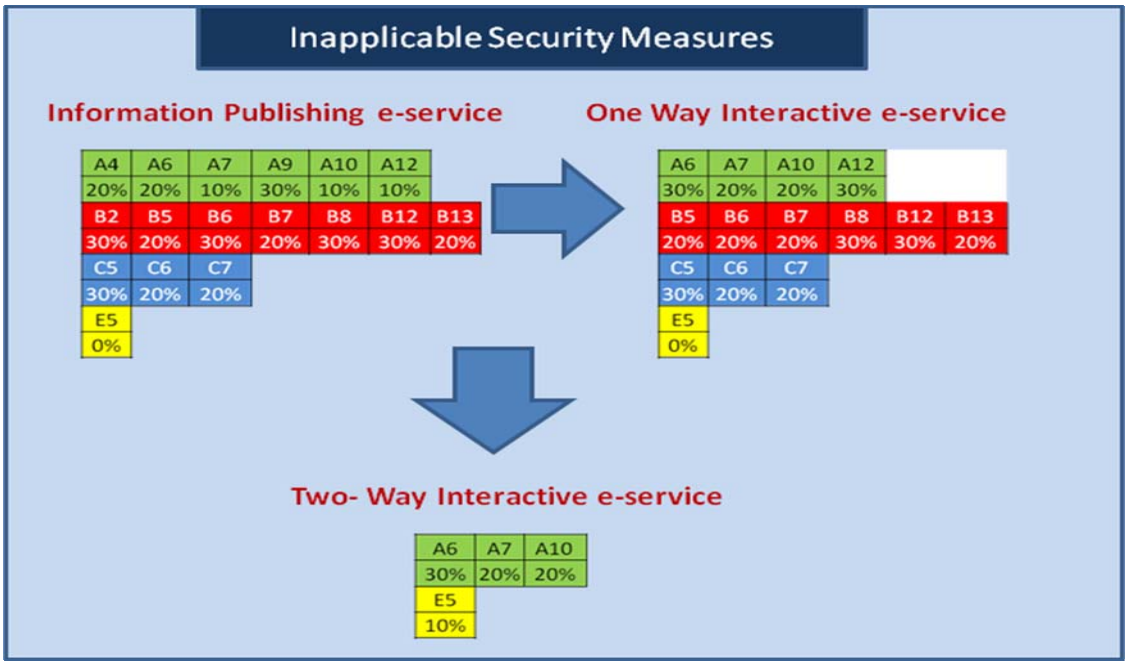


Figure 68: The model evolution

- The percentage rates went higher for all the sub layers when it was assessed against the combination of all services. The assessment rates were varying from 70%-100% except for the following:
    - VPN technology scored 60%
    - Biometrics technology scored 30%
    - Laws and Regulations scored 60%
    - Third party policies scored 60%
    - FUD scored 10%

6.9. Chapter summary:

The objective of this chapter was to discuss the survey results of the questionnaire B deployed to 16 highly recognized security practitioners in Dubai. The results of the analysis confirmed the need of all the sub layers proposed by the new model and the removal of the FUD sub layer due to the low selection rate scored. Based on the analysis of the external and internal threats, different types of threats were raised by the respondents which will need different types of security measures to mitigate.

Chapter seven: Validation

The validation process was part of the research methodology used. Since this research is a life case scenario the validation process was crucial to confirm model applicability. The process of validation caused a slight modification of the new model by omitting a cell from the decision layer. The validation process was the eighth step of the overall research methodology as illustrated in **Figure 69.**

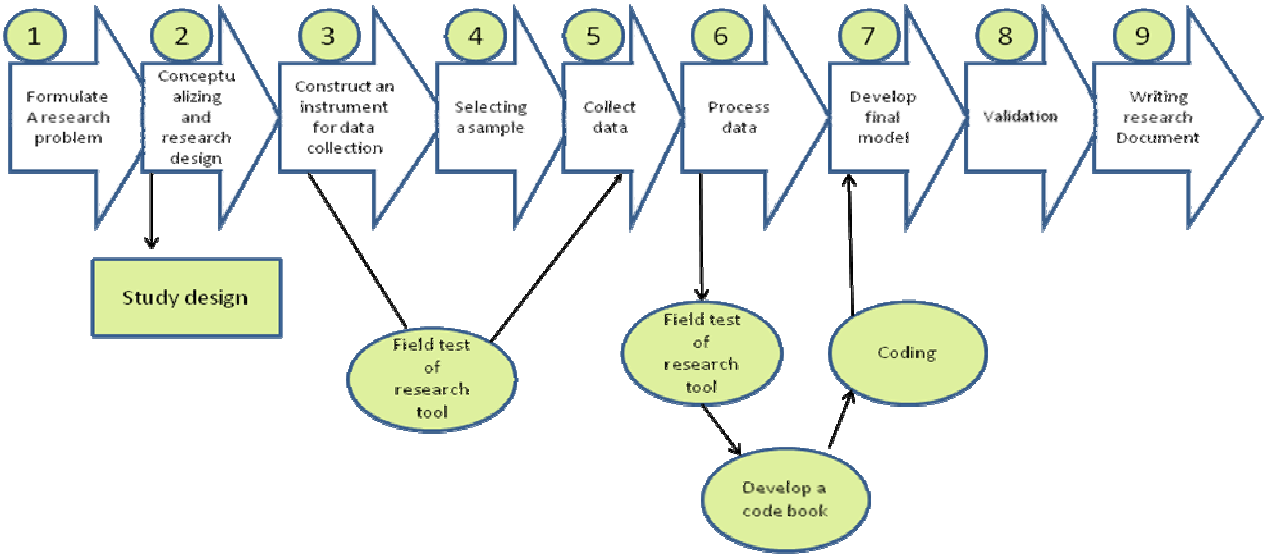


Figure 69: Validation process as part of the research cycle

7.1. Questionnaire analysis:

After the analysis of the survey and the correlation questions related to the layers of the model, it has been observed that all the layers were required and selected by both the security practitioners and the government departments management surveyed. The selection was based on understanding the needs of different aspects of protection and correlation between the threats and the security measures required in any government departments. As discussed in Chapter 6, all categories of services required all layers and sub layers of the proposed model. The only sub layer which was will be dropped from the

model is the Fear, Uncertainty, and Doubt (FUD) (E5). The modified model is shown in **Table 40** and the key of the cells is illustrated in **Table 41**.

Table 40: The Modified model

Layer	Sub layers/Cells															
Technology	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12				
	100 %	70 %	80 %	90 %	100 %	80 %	50 %	70 %	90 %	30 %	100 %	70%				
Policies	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
	90%	90 %	90 %	70 %	80 %	80 %	90 %	90 %	100 %	80 %	90 %	80%	60%	70%	90%	100 %
Competencies	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10						
	100 %	100 %	90 %	80 %	80 %	70 %	60 %	100 %	100 %	60 %						
Operational Mgmnt	D1	D2	D3	D4	D5											
	90%	90 %	100 %	70 %	80 %											
Decision Factor	E1	E2	E3	E4												
	80%	70 %	100 %	100 %												

Table 41: Model key

	Category		Category	
Technology	Access Control	A1	Intrusion Detection and Prevention	A2
	Anti Virus and Malicious Code	A3	Authentication and Passwords	A4
	Files and Integrity Check	A5	Cryptography	A6
	VPN	A7	Vulnerability Scanning Tools	A8
	Digital Signatures and Certificates	A9	Biometrics	A10
	Logical Access Control (Firewalls)	A11	Security Protocol	A12
Policies	Password Management	B1	Log-in Process	B2
	Logs Handling	B3	Computer Viruses	B4
	Intellectual Property Rights	B5	Data Privacy	B6
	Privilege Control	B7	Data Confidentiality	B8
	Data Integrity	B9	Internet Connectivity	B10
	Administrative Policies	B11	Encryption Policies	B12
	HR Security Policies	B13	Third Party Policies	B14
	Physical Security Policies	B15	Operation Security Policies	B16
Competencies	Security Operation and management	C1	Security Architecture and development	C2
	Ethical Hacking	C3	Security Policies and development	C4

	Computer Forensics	C5	Cryptography	C6
	Security Programming	C7	Laws and regulation	C8
	Security Implementation and Configuration	C9	Security Analysis	C10
OPS mgmt	Operational Policies and Procedures	D1	Management Tools	D2
	Correlation and data mining	D3	Reporting and Response	D4
	Analysis and Human intervention			D5
Decision	Cost	E1	Awareness	E2
	Need	E3	Technologies Availability	E4

7.2. The criteria of success

The proposed model was derived from the extensive research and literature review, industrial experience, and results of the survey and analysis. The development of the layers was done based on a scientific approach and the each sub layer was justified and backed up with either an academic literature or an industrial white paper. The followings are the critical success factors (Wood, C., 2005) , (Lankhorst, M., 2005) which were considered during the development of the model:

- ***Simplicity of the model***: The model must be clear to the intended users (government departments or individuals). The layers of the model must be explicit and should make sense to a non security or IT expert.
- ***Applicability:*** The model must be applicable to any organisation which intends to use it for its internal or external communication or information sharing.
- ***Standards compliant:*** The model must comply with the security standards in terms of acronyms, references, objectives.
- ***Doable:*** The model must be doable for the e-government authority and its government affiliates.
- ***Flexible:*** The model must be flexible and can be implemented in phases.
- ***Open standards:*** The model must address general technologies, policies, competencies, and operational procedures. It should not be biased to any brand,

proprietary solution, or special procedures applicable only to specific vendor or forum.

- ***Renewable and expandable:*** the model must be easy to update with the introduction of new trends in the security field and it also can allow merge group of security technologies, policies, procedures, or competencies.

The following checklist entitled as "Validation Form" **(Table 42)** was developed for the e-government to use in order to evaluate and validate the model:

Table 42: Validation form

Criteria	Description	Validity Rate
Simplicity of the model	The model must be clear to the indented users (government departments or individuals). The layers of the model must be explicit and should make sense to a non security or IT expert	□ Low □ Medium □ High □ Extremely High
Applicability	The model must be applicable to any organisation which intends to use it for its internal or external communication or information sharing	□ Low □ Medium □ High □ Extremely High
Standards Compliance	The model must comply with the security standards in terms of acronyms, references, objectives	□ Low □ Medium □ High □ Extremely High
Doable	The model must be doable for the e-government authority and its government affiliates	□ Low □ Medium □ High □ Extremely High
Flexible	The model must be flexible and can be implemented in phases	□ Low □ Medium □ High □ Extremely High
Open standards	The model must address general technologies, policies, competencies, and operational procedures. It should not be biased to any brand, proprietary solution, or special procedures applicable only to specific vendor or forum.	□ Low □ Medium □ High □ Extremely High
Renewable and	the model must be easy to update with the introduction of new trends in the	□ Low □ Medium

Expandable	security field and it also can allow merge group of security technologies, policies, procedures, or competencies	□ High □ Extremely High

7.3. Dubai e-government application:

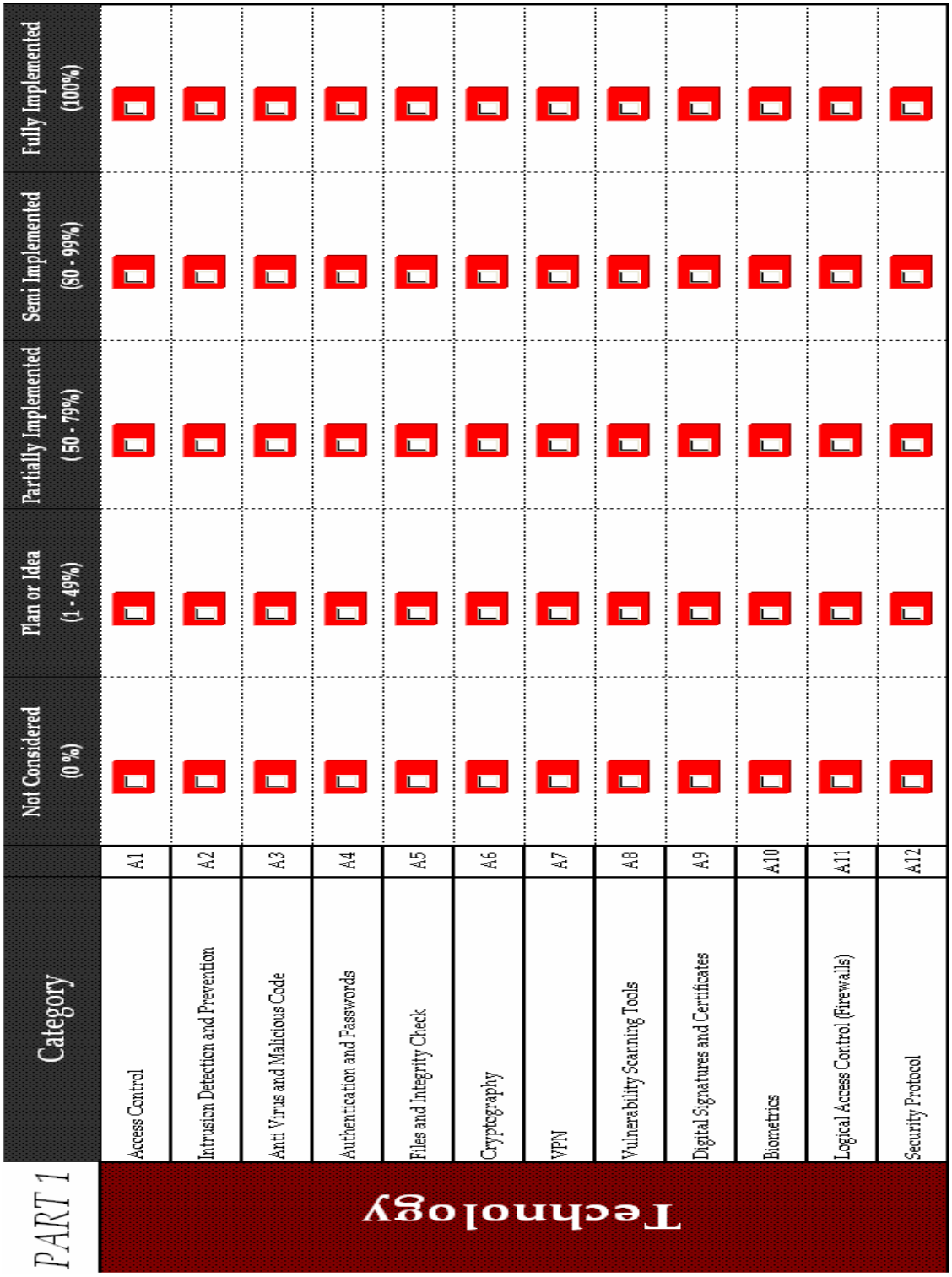
DEG authority has 26 government departments affiliated with it. The concept of e-government was implemented in a decentralized model. Each government department has the responsibility to convert its government services to e-services. The e-government authority has the responsibility to coordinate with the government departments and try to find synergic services across all of them. In addition, the e-government authority has its own e-services launched to the citizens. The e-services maturity varies from information publishing to transactional. Since the model addresses the security aspects for all types of e-services, it can be implemented in the 26 government departments. Taking into consideration that the new Dubai Strategic Plan is consolidating the government departments into 4 main buckets, the number of government departments affiliated to the e-government will definitely be reduced in the future. Dubai e-government Authority (DEG) was selected as the only government department and authority to validate the security model due to the following reasons:

- The only non biased government department and responsible body for the overall e-government initiative in Dubai.
- Launched key e-services which are used by large population of citizens and other government departments.
- Strong ownership over the integration initiative of all the government departments.
- The availability of a large number of security practitioners who will participate in the validation process of the model.

The validation process of the security model was having 2 dimensions. The first dimension was to check the model value and its usability aspects. This was achieved through a distribution of a validation form developed in section 7.2 to assist the participant to select the rate of validity from different success criteria. The second dimension was to check the level of implementation through the second form **(Table 43)**. The second form has each layer and its sub layers listed and a rate from 1 to 5 was assigned against each sub layer.

The rate goes from 1 (not implemented) to 5 (fully implemented). The participants can choose the appropriate rate where it applies.

Table 43: Implementation rating form



PART 1	Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
Technology	Access Control	A1	☐	☐	☐	☐	☐
	Intrusion Detection and Prevention	A2	☐	☐	☐	☐	☐
	Anti Virus and Malicious Code	A3	☐	☐	☐	☐	☐
	Authentication and Passwords	A4	☐	☐	☐	☐	☐
	Files and Integrity Check	A5	☐	☐	☐	☐	☐
	Cryptography	A6	☐	☐	☐	☐	☐
	VPN	A7	☐	☐	☐	☐	☐
	Vulnerability Scanning Tools	A8	☐	☐	☐	☐	☐
	Digital Signatures and Certificates	A9	☐	☐	☐	☐	☐
	Biometrics	A10	☐	☐	☐	☐	☐
	Logical Access Control (Firewalls)	A11	☐	☐	☐	☐	☐
	Security Protocol	A12	☐	☐	☐	☐	☐

PART 2	Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
Policies	Password Management	B1	☐	☐	☐	☐	☐
	Log-in Process	B2	☐	☐	☐	☐	☐
	Logs Handling	B3	☐	☐	☐	☐	☐
	Computer Viruses	B4	☐	☐	☐	☐	☐
	Intellectual Property Rights	B5	☐	☐	☐	☐	☐
	Data Privacy	B6	☐	☐	☐	☐	☐
	Privilege Control	B7	☐	☐	☐	☐	☐
	Data Confidentiality	B8	☐	☐	☐	☐	☐
	Data Integrity	B9	☐	☐	☐	☐	☐
	Internet Connectivity	B10	☐	☐	☐	☐	☐
	Administrative Policies	B11	☐	☐	☐	☐	☐
	Encryption Policies	B12	☐	☐	☐	☐	☐
	HR Security Policies	B13	☐	☐	☐	☐	☐
	Third Party Policies	B14	☐	☐	☐	☐	☐
	Physical Security Policies	B15	☐	☐	☐	☐	☐

PART 3

Security Competencies

Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
Security Operation and management	C1	☐	☐	☐	☐	☐
Security Architecture and development	C2	☐	☐	☐	☐	☐
Ethical Hacking	C3	☐	☐	☐	☐	☐
Security Policies and development	C4	☐	☐	☐	☐	☐
Computer Forensics	C5	☐	☐	☐	☐	☐
Cryptography	C6	☐	☐	☐	☐	☐
Security Programming	C7	☐	☐	☐	☐	☐
Laws and regulation	C8	☐	☐	☐	☐	☐
Security Implementation and Configuration	C9	☐	☐	☐	☐	☐
Security Analysis	C10	☐	☐	☐	☐	☐

PART 4	Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
OPS mgmt	Operational Policies and Procedures	D1	☐	☐	☐	☐	☐
	Management Tools	D2	☐	☐	☐	☐	☐
	Correlation and data mining	D3	☐	☐	☐	☐	☐
	Reporting and Response	D4	☐	☐	☐	☐	☐
	Analysis and Human intervention	D5	☐	☐	☐	☐	☐

PART 5	Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
Decision	Cost	E1	☐	☐	☐	☐	☐
	Awareness	E2	☐	☐	☐	☐	☐
	Need	E3	☐	☐	☐	☐	☐
	Technologies Availability	E4	☐	☐	☐	☐	☐

The validation process methodology can be applied to any case studies which can be considered for the model applicability. The limitation of this research will be due to the limited validation process as it was conducted in Dubai only. In addition, since Dubai was taken as a case study, conducting the validation process in Dubai was imperative as the participants should be part of the e-government system or initiative and should be users of the online services of the e-government.

7.4. Results of the validation process

Based on the completed process the validation rate was acceptable and showed good acceptance from the e-government authority. The model will be considered as a reference checklist for all the government departments willing to share information freely. It was found applicable for designing the security architecture for Dubai e-government authority and its affiliates. It shall contribute to the level of trust enhancement for information sharing between the government departments. The key objectives of the research were met through the development of the new security model as indicated in **Table 44**.

Table 44: Key objectives validation

Research Key Objective	How it was met
Establish the security requirements for Dubai e-government	The recognition of the government departments for the need of a common security model which will act as government enterprise security architecture was the first step of identifying the requirement of security. Having the heads of the departments participating in the questionnaires and identifying the internal and external threats has given the author a holistic view of the security needs for the government departments.
Collate state of the art approaches and methods for the government security.	Studying the different models developed to meet the CIA triad objectives, e-government challenges, and the widely practiced security standards, provided the author a solid back ground of the government security requirements.
Develop model for evaluation security level for inter-government information sharing	The new model can be used in two ways: - As a reference architecture of the government security infrastructure. - As a checklist which government departments will need to go through to set up a strong security infrastructure enabling the information sharing between the different government departments.
Validate the model in Dubai e-government	The model was sent to DEG authority for verification and validation. The model was evaluated by the DEG authority security team and consultants and was found to be applicable to the current needs of the government departments. The author foresees that the model will be implemented in the near future as the common government security architecture for all Dubai government departments.

Chapter eight: Conclusions

8.1. Achievement of the research objectives:

"Digital or electronic government (e-government) is the use of ICTs in general and e-technologies in particular, in order to: Promote and motivate a more operationally efficient and cost effective government; facilitate more convenient government services to citizens and business; enhance economic development; reshape and redefine community and government processes, allow greater public access to information; and make government more accountable to their citizens." (Asgarkhani, M. ,2005).

The definition above of the e-government can be considered as a good reference to the objectives of an e-government. The objectives of the different e-governments categories (G2C, G2B, G2G, and IEEE) are illustrated in the table below **(Table 45)**. Moreover, the different categories of e-services apply on all types of e-governments mentioned in Table 47. The security aspects of the e-services are common as it was proved in the analysis of the survey results.

Table 45: E-government categories

E-government category	Business metaphor	Description	Sub-category	Example practice
Government to citizens (G2C)	Customer Relationship Management (CRM)	Providing opportunities for greater citizen access to and interaction with the government	Managerial interaction	Government's informational web sites
			Consultative interaction	E-voting instant option poling
Government to business (G2B)		Seeking to more efficiency work with business	Businesses as suppliers of goods or services	Government's e-procurement
			Businesses as regulated economic sectors	Electronic filing with various government agencies
Government to Government (G2G)	Supply Chain Management (SCM)	Enabling government agencies at different levels to work more easily together	Vertical integration	Sharing a database among agencies within the similar functional walls but across different levels of government
			Horizontal integration	Sharing a database among agencies at the similar levels of government but across different functions
Government internal efficiency and effectiveness (IEE)	Enterprise Resource Planning (ERP)	Focusing on internal efficiency and effectiveness	Government to employee	web based payroll/health benefits system
			Integrating internal systems	Implementing ERP-like systems to integrate different functions within a single agency
Overarching infrastructure (Cross-Cutting)	Enterprise Application Integration (EAI)	Facilitating the interoperability across different practices	Hardware and software interoperability	Public-key infrastructure interoperability
			Authentication	e-Authentication across different e-government initiatives

The challenge of information sharing between the e-government authority and its affiliates is not related to the technological challenges only. During the research of this thesis it was discovered that the trust element is a key factor to enhance the information sharing and the use of e-services over the Internet by citizens or other government departments. In the essay on Internet trust, Dutton and Shepherd argue that " trust in the Internet and related information and communication technologies-'Cyber trust'-could be critical to the successful development of 'e-services', such as a e-government, e-commerce, e-learning and democratic participation in the rapidly expanding online public sphere" (Dutton, W. H. and Shepherd, A., 2006). From the definition of the e-government mentioned above, the objective of the e-government is to offer e-services over the Internet or a public network for its citizens and affiliates. The Internet and the public network will play the role of the medium where the e-services will be delivered through. The level of trust will definitely impact the level of the e-services usability by citizens or government departments. Dutton and Shepherd illustrated in their paper that there are two separate dimensions of cyber trust. These dimensions were derived through a factor analysis which was done on the results of the survey conducted in the UK. The first dimension is the 'Net confidence' which simply means the degree to which users and non users have confidence in the technology and in the people they can communicate with on the Internet. The second dimension is 'Net Risk' which simply means the perception of and exposure to risks while using the Internet. The risks of the e-services can only be minimized to an acceptable level if the threats on every e-service have a security measure which can mitigate it or make it ineffective. The research of this thesis started with four objectives:

1. Establish the security requirements for Dubai e-government.
2. Collate state of the art approaches and methods for the e-government security.
3. Develop model for evaluating security level for inter-government information sharing.
4. Test the model in the Dubai e-government context.

The following table shows the different activities conducted to achieve the objectives of the thesis **(Table 46):**

Table 46: Research activities

Research Activity	Objective	Results
Literature review of all existing models, e-government issues, etc	• To get acquainted with the existing models, issues of e-government, challenges, and e-services • Confirm the need of the information security in the e-government model and implementation. • Relate the lack of the information flow to the lack of trust in the security level between the departments. • ***Establish the security requirements for Dubai e-government.***	• Was able to understand the issues of all the models and their focal areas. • Identified all weaknesses of each model to build the argument for the new one. • Identified the overlapped areas and how each model can complement each other. • Searched for academic support for each layer and sub layer proposed in the model. • Learn about how academic arguments are built from journals and publications. • Found some journals discussing the trust relationship with the lack of information sharing.
Analysis of the Dubai e-government structure, types of e-services offered, and issues and challenged faced.	• To prepare for the case study that will be applied on DEG authority. • Setting a testing bed of the new model in the e-government authority in Dubai with few governmental departments.	• Confirmed the areas of challenges the e-government authority is facing with its affiliates. • Identified the main government departments and executives who will be participants of the survey process.
Build an academic argument on the multi threats concept for a single e-service	• To prepare the academic ground for the need of a multi layer model which will mitigate multi layered threats on e-services. • ***Collate state of the art approaches and methods for the e-government security***	• Proved the point that a single e-service can have multiple threats related to its processes, supporting systems, or resources. This led to the need of having a model addressing different security aspects other than technologies.

Build the academic argument on the need of a multi layered model.	• To have a strong academic support on each layer and sub layer of the model.	• Through this process, the layers and the sub layers were selected to come up with the representation of the final model.
Collecting Data on the e-government services security aspects	• To prove the sub layers of the model, need of each layer and its sub layers, identify areas which might need to be modified in the model • Prove the need of the different security layers and not only restricted to one. Through this prove, the layers needed for the model can be theoretically provided to construct the new model • The content/cells of each layer will need to be proven theoretically through literature review, surveys, and industrial opinions from the practitioners. • Results of the research to be reflected through the analysis mechanism conducted • ***Develop model for evaluating security level for inter-government information sharing.***	• All layers and sub layers were confirmed through this process. • Management and technical professional opinions were extracted from the survey supporting the proposal of the new model.
Validation process	• To validate the need of each model, its usability, and the rate of implementation of each sub layers currently. • ***Test the model in the Dubai e-government context.***	• The validation process evaluated the model and its usability. It also included a form to rate the current implementation of the sub layers in order to know the level of enhancement the model will contribute with and the appropriate rate of security the governments department will need to adopt.

The objectives of the research were met and a new model is proposed through this thesis document. The new model can be applicable for any governmental department and it can be implemented as architecture or an assessment tool.

8.2. Discussion

An in depth literature review was carried out during this research. The literature review assisted the author to identify the different existing security models and theories and standards. It also gave a good overview on existing models and their construction and challenges, DEG authority and its e-services, and the challenges an e-government might face. The literature review analysis was done to support the derivation of the new model. Theories addressing technological, policies, human aspects, decisions, and the impact of a decision in organisation were studied and analyzed. The literature review was a key step towards the development of the new model. It also assisted the author to identify the weakness of different models to establish the research gap.

Developing a security model which tackles different aspects of security in addition to the technological layer was not a trivial process. Through the research process of this thesis, it was noticed that all existing models were developed to address one aspect or a problem in the information security field. Well known models such as Bell Lapadula, Biba, non interference, Chinese wall, and compartmentation and lattice model were all developed to tackle one aspect of security. Some of them were relying heavily on the enforcement of the security policies, while others were algorithms and logic based. Other models studied and analyzed were taking the quantitative approach such as the network rating model (NRM) while others were more qualitative. Through the thorough analysis and research conducted for this thesis, no comprehensive model was found which addresses all aspects of security for any organisation that offers e-services of the Internet or a public network. Security practitioners form different industries were always highlighting the need of a new security model which will address other aspects than technologies in order to mitigate risks categorized as non-technological risks. This instigated the search of a new method to develop a model which contains multilayer representing technologies, policies,

competencies, operational procedures, and above all the decision factors which may play a major role in enforcing the other layers.

During the extensive research and site visits conducted to e-governments, it was noticed that turning into i-government (where "i" stands for information sharing) was a strategic objective. The objective is simple; an integration between the backend systems which will ensure the ability of having a single profile for the citizens. The concept of i-government is becoming popular in Dubai and the challenge of integration started to be raised. The security aspect of the information sharing was always a concern as information will leave a government department through the Internet or a public network with a certain level of classification but might be mishandled or declassified for any reason. Maintaining the classification of the information, confidentiality, integrity, and availability will require more than a policy to be in place, or a technology to be implemented. The reasons of mistreating information might be due to technological flaws, weak policies, lack of competencies and awareness from the security practitioners or the users, absence or lack of operational management, and wrong decisions taken on how to handle governmental classified information. Other reasons might be raised or argued but all reasons rotate around the fact that multiple threats due to different reasons exist for a single e-service launch or information sharing action. Placing the appropriate security measures will assist in mitigating the multiple threats of information sharing caused by different reasons. The concept of multiple layers of the model addressing different aspects of security is the fundamental design of the new model. This new model has high level of flexibility as sub layers representing technologies, policies, competencies, procedures or decision factors, can be updated with new trends in the security field based on the growth of the need.

During the development of the new model, a case study was needed in order to test the validity of the model. The motivations of selecting DEG authority were:

- Easy access to e-government authority top management.
- Familiarity on the e-services related to the e-government.

- The need of information sharing between the e-government authority and its affiliates.
- The availability of the different type of e-services and different level of maturity.
- The ability to influence the management of the e-government in testing the model and contribute in the validity process.

8.3. Contribution to knowledge

The model presented herewith this thesis document represents a new approach or methodology of assessing the security programme or architecture.

The new model has 5 layers; each layer is important and assists the organisation to achieve a milestone within the security field. The top layer of the model represents the most common in the security field. Security technologies are always implemented and with the proliferation of the Internet access, they became integrated as part of the business support systems. The second layer, the security policies, complements the first one. Security practitioners develop security policies for their organisations and attempt to place technologies in order to tighten the security policies and prevent them from becoming self-defeated policies. The security competencies are needed for the development of the technologies and security policies. Once the organisation establishes the infrastructure, setting the right security policies and recruit the competent security staff, the operational procedures become the next imperative aspect to have for the security programme. Having the proper operational and management procedures is an art and will need to be monitored and evaluated periodically. The management decisions to launch an e-service or implement a security technology for the organisation impact on all the previous layers. Placing the wrong security technology or diluting a security policy is a major threat on the organisation which may lead to security breaches and a defeat to the overall security programme.

The model is unique in the comprehensive inclusion of all known security issues in a form that can be used by e-government security management. Using the new model will assist the government department to achieve the following:

- Having a checklist for all the security measures implemented or planned to be implemented in the future.
- Inventory list of all security assets already implemented or which will be implemented in the future.
- A basic and manual rating tool for the level of security in the government department. The level of security expected from the government department can be agreed and determined by the e-government authority and its affiliates or can be set as a standard based on a questionnaire or consensus among all the participants in the e-government development and e-services provisioning.

This thesis document provides a good background of all existing security models, strength analysis of each model, and a methodology to develop a new model through the research process followed to come up with the new model.

8.4. *Wider application*

The approach to develop the new security model reported in this thesis can be used for any e-government in the world. The selection of the sub layers has to be performed as per the selection criteria recommended in **Chapter 4**. The new security model can be applicable to all e-governments in the GCC as cost is not a limit on the use of the security technologies and policies. The factor of competencies' availability will vary from a country to another but it will not have a great impact due to the flexibility of the employment policies of the expats from the Middle East countries. Countries in the Middle East with limited infrastructures and budgets will not be able to apply the whole model as the decision factor will play a major role in limiting some of the technologies and policies. As a result, the competencies of the security staff will be limited which might lead to a strong probability of being attacked by external and internal intruders.

In comparison to the Far East or the west, the five layers of the model are appropriate but the sub layers will be changed based on the country's security requirements and perception of some of the security policies, competencies, and decision factors. It is expected that minor modifications can be performed upon the proposed model to tailor it to the

requirements of any e-government in the world. This indeed adds a strong advantage of the new model and proves its flexibility as one of the success criteria set in **Chapter 7**.

8.5. Conclusion and future work

Information security plays a key role to enable e-services offered by government departments or authorities, information sharing inter or intra government departments, and above all to improve the trust between authorities and their affiliates. The level of trust or the net confidence is directly related to the security confidence of any organisation.

The usability of the e-services over the Internet can increase if the security level is enhanced within the service provider and the users' security awareness is elevated.

Research conducted on security models highlighted some strong ones which tackle specific aspects of security. Some of the developed models were successful in resolving issues related to the system security, while others were policy oriented addressing either confidentiality or integrity of the information. During the literature review phase and through all the research conducted, no comprehensive security model was found which addresses the different aspects of security. The cycle of developing such a model was based on an academic approach starting from the literature review of all models published in journals or conference papers. They were analysed on the weaknesses and strengths of each model and the approaches to develop the models. The author got acquainted with models which are related to e-commerce security, network/ systems risks, confidentiality, integrity, and conflict interest prevention models. The development of the new model was based on scientific knowledge and a thorough analysis process.

The new model consists of five layers. Each layer represents a dimension of security which need to be addressed in order to mitigate threats associated with it. Each layer has one or more of sub layer. The number of sub layers will be determined by the number of security measures an e-government organisation feels sufficient to provide an acceptable security level. In reality, no common accepted rate of security level was found agreed by the e-

government authority and its affiliates. The new model only reflects the layers and sub layers required to provide an acceptable security programme for any e-government organisation offering services to public citizens. The research establishes the sub layers most required for the security programme to tackle the multiple threats associated with an e-service.

The DEG authority was taken as a case study of the model. Two types of survey questionnaires were deployed to the e-government programme in Dubai. The objectives of the questionnaires were:

- To identify the types of threats on different e-services.
- To get a view from management of the government departments on different types of threats.
- To identity the layers required in the model and their sub layers also.
- To get the security practitioners feedback on the need of technologies, policies, competencies, operational management, and decision factors as layers of the new model.
- To rate the importance of the sub layers of the model in order to authenticate the need of them or drop the ones scoring low percentage.

The research process led to the development of a structured security model which will assist an e-government organisation to evaluate the security level, identify deficiencies in the security system, and put in place the necessary measures to mitigate different threats on e-services. The new model consists of five major layers each one of them tackles group of threats. Each layer represents a portfolio of sub layers which collectively fit together to construct a solid layer of the model.

In the future, the author intends to work on a mathematical representation of the model which will assist in defining the best combination of all sub layers in order to come up with the highest security score for an organisation which need to launch an e-service or share information over the Internet. The mathematical formula can be used in the future for finding the combination of sub layers or any IT model subject that the importance of each

layer or sub layer is defined, a thorough dependency analysis is conducted, the scenarios are well defined and the quantification of the important factors can be achieved.

Another future work can be conducted on the model is to transform it to a security framework (K, C. and S, H. , 2006). The security framework can be integrated as part of the Open Group Framework (TOGAF) which is the most adopted enterprise architecture in the IT industry (TOGAF Forum, 2007). The future research will be carried out by the author as part of the post doctorate programme intended to attend in the near future.

References

1. Akers, R. L., Krohn, M. D., Lanza-Kaduce, L. and Radosevich, M. (1979), "Social learning and deviant behaviour: a specific test of a general theory", vol. 44, pp. 636-55.

2. Alexandros, K., Panagiotis, S., Thanos, K. and Despina, P. *A secure e-government platform architecture for small to medium sized public organizations,* National Technical University of Athens, Athens.

3. Al-Hamdani, W., A. (2007), "Assessment of need and method of delivery for information security awareness program", *Proceedings of the 2006 Information security Curriculum Development Conference, InfoSec CD '06,* Sep 22-23 2006, Kennesaw, GA, United States, Association for Computing Machinery, New York, NY, pp. p 102-108.

4. Anderson, A. and Shain, M. (1991), "Risk Management:", in Caelli, W., Longley, D. and Shain, M. (eds.) *Information security handbook,* 1st ed, Stockton Press, , pp. 75-127.

5. Anderson, R. (April 2001), *Security Engineering: A Guide Building Dependable Distributed Systems,* 1st ed, John Wiley & Sons, Inc, U.S.

6. Anderson. B., Homes., M.D. and Qstresh. (1999), "Male and Female Delinquent's attachment and effects of attachments on Security of Self-Reported Delinquency", *Crime and Behaviour,* vol. 26, no. 4, pp. 435-452.

7. Anonymous, B., Mark., Locher, L. J. and Doyle , C. (1998), *Maximum Security,* 1st ed, SAMS, U.S.

8. Arthur, J. C. and Quey-Jen, Y. (2006), "On security preparations against possible IS threats across industries", *Information Management & Computer Security,* vol. 14, no. 4, pp. 343-360.

9. Asgarkhani, M. (2005), "Digital government and IT effectiveness in public management reform, a local government perspective", vol. 7, no. 3, pp. 465-487.

10. Atreya, M., Hammond, B., Paine, S., Starrett, P. and Wu, S. (2002), *Digital Signatures,* McGraw Hill, New York.

11. Bace, R. G. (2000), *Intrusion Detection,* 1st ed, Sams Publishing, USA.

12. Baker, W. H. and Wallace, L. (2007), "Is Information Security under control? Investigating quality in information security management", *IEEE Security & Privacy,* vol. 5, no. 1, pp. 36-44.

13. Barnett, F. (1996), "Computer Security training and education: A needs analysis", 6-8 May 1996, Oakland, CA, USA, IEEE Comput. Soc. Press, Los Alamitos, CA, USA, pp. 26-7.

14. Bell, D. and Lapadula, L. (1973), ""Secure Computer System": Unified Exposition and Multics Interpretation,"", *Technical Report MTR-2997 Rev.1,* .

15. Benabdallah, S., Fatmi, G. E. and Ourdiga, N. B. (2002), "Security issues in E-government models: what governments should do?", *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics,* Vol. 2, Oct 6-9 2002, Yasmine, Hammarnet, Tunisia, Institute of Electrical and Electronics Engineers Inc., Tunis, pp. 398-403.

16. Bertucci, G. (2005), "UN Global E-government Readiness Report 2005: From E-government to E-inclusion", , no. 14, pp. 1-253.

17. Beynon, D. P. (2005), "Constructing electronic government: The case of the UK inland revenue", *International Journal of Information Management,* vol. 25, no. 1, pp. 3-20.

18. Biermann, E., Cloete, E. and Venter, L. M. (2001), "A comparison of intrusion detection systems", *Computers and Security,* vol. 20, no. 8, pp. 676-683.

19. Bishop, M., Cheung, S. and Wee, C. (1997), "The Threat from the net (Internet Security)", *IEEE Spectrum,* vol. 34, no. 8, pp. 56-63.

20. Bodeau, D. J. (1992), "A Conceptual Model for Computer Security Risk Analysis", 1992, Bedford, MA, the MITRE Corporation, 202 Burlington Road, Bedford, MA 01730, pp. 56.

21. Brewer, D. F. C. and Nash, M. J. (1989), "Chinese Wall security policy", *Security and Privacy, 1989 IEEE Symposium,* 1-3 May 1989, Oakland, CA, USA, pp. 206-214.

22. Brown, S. (2001), *Implementation Virtual Private Networks,* 1st ed, McGraw-Hill, New York, USA.

23. C&A systems security limited (2000), *CORBA consultant products for windows, evaluation & user guide,* C&A systems security limited.

24. Carroll, J. M. (1995), *Computer Security,* 3rd ed, Butterworth-Heinemann, Burlington, MA.

25. Clark, D. D. and Wilson, D. R. (1987), "A comparison of commercial and military computer security", *Proceedings **of** the 1987 IEEE Symposium on **Security** and Privacy (Cat. No.87CH2416-6),* Oakland, CA, USA, IEEE Comput Soc Press, Washington, DC, USA, pp. 184-94.

26. Cohen, F. B. (1992), "Defence in-depth against computer viruses", *Computer and Security,* vol. 11, no. 6, pp. 563-79.

27. Cole, E. (2002), *Hackers Beware-Defending Your Network from Wiley Hacker,* 1st ed, New Riders Publishing, US.

28. Conklin, A. and White, G., B. (2006), "e-Government and cyber security: The role of cyber security exercises", *Proceedings of the 39th Annual Hawaii International Conference on System Sciences, HICSS'06,* Vol. 4, Jan 4-7 2006, Kauai, HI, United States, IEEE, US, pp. 79b.

29. Creswell, J. W. (2003), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches,* 2nd ed, SAGE Publications, Inc, 2455 Teller Road, Thousand Oaks, California 91320.

30. Cronkhite, C. and McCullough, J. (2001), *Access Denied Hackers,* 1st ed, McGraw Hill/Osborne, California, USA.

31. Dawes, S., Pardo, T. and Cresswell, A. (2004), "Designing electronic government information access programmes: a holistic approach", *Government Information Quarterly,* vol. 21, no. 3-23.

32. Doughty, K. (2003), "Information Systems Control as "Implementing Enterprise Security": A Case Study (Part 1)", *Information Systems Control Journal,* vol. 22, no. 2, pp. 99-114.

33. Dutton, W. H. and Shepherd, A. (2006), "Trust in Internet as an experience technology", *Information Communication & Society,* vol. 9, no. 4, pp. 433-51.

34. Eero, K. and Slltonen, L. A. (1993), "The Constructive Approach in Management Accounting Research", *Journal of Management Accounting Research,* , pp. PP 244-264.

35. Evans, D., L., Bond, P., J. and Bement, A., L. (2004), Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, NIST.

36. Evans, D. and Yen, D. (2005), "E-government: An analysis for implementation: Framework for understanding cultural and social impact", *Government Information Quarterly,* vol. 22, no. 3, pp. 354-73.

37. Farn, K., Lin, S. and Fung, A. R. (2004), "A study on information security management system evaluation-assets, threats & vulnerability", *Computer Standards & Interfaces,* , pp. 501-513.

38. Finne, T. (1996), "A DSS for Information Security Analysis: Computer Support in a Company's Risk Management", *Proceedings of IEEE International Conference on Systems, Man and Cybernetics,* Vol. 1, 14-17 Oct 1996, Beijing, China, IEEE, New York, NY, USA, pp. 193-8.

39. Fraster, T. (2001), "LOMAC: MAC you can live with", *Proceedings of the FREENIX Track. 2001 USENIX Annual Technical Conference,* 25-30 June 2001, Boston, MA, USA, USENIX Assoc, Berkeley, CA, USA, pp. 1-13.

40. Geray, O. (Feb 2007), Dubai eGovernment eServices: 2006 strategic Progress Review Report, 4, Dubai eGovernment Authority, Dubai.

41. Glassey, O. (2004), "Developing a one-stop government data model", *Government Information Quarterly,* vol. 21, pp. 159-169.

42. Goguen, J. A. and Mesequer, J. (1982), "Security policies and security models", *Proceedings of the 1982 Symposium on security and privacy,* 26-28 April 1982, Oakland, CA, USA, IEEE, New York, NY, USA, pp. 11-20.

43. Gollmann, D. (2001), *Computer Security,* 2nd ed, John Wiley & Sons, New York, USA.

44. Goncalves, M. (1999), *Firewalls A Complete Guide,* McGraw Hill, New York.

45. Gottfredon, M. and Hirschi, T. (1990), *A General Theory of Crime,* Stanford University Press, Stanford California.

46. Gupta, M., Rees, J., Chturvedi, A. and Chi, J. (2006), "Matching Information Security Vulnerabilities to Organizational Security Profiles: A generic Algorithm Approach", *Decision Support Systems,* vol. 41, no. 3, pp. 592-603.

47. Haney, C. (1999), *Chinese hackers reportedly get death sentence*, available at: http://www.computerworld.com.au/index.php/id;1224861705 (accessed 01/04).

48. Hansen, J. (2001), "Internet Commerce Security: Issues and models for control checking", *Journal of the Operational Research Society,* vol. 52, no. 10, pp. 1159-1164.

49. Hardy, G. (2006), "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges, Information security technical report", *Elsevier Science,* , pp. 55-61.

50. Hinde, S. "The law, cybercrime, risk management and cyber protection", *Computer and Security,* vol. 22, no. 2, pp. 90-95.

51. Hone, K. and Eloff, J. H. P. (2002), "Information Security Policy-What do International Information Security Standards Say?", *Computers & Security,* vol. 21, no. 5, pp. 402-9.

52. Hornes, A. B. "Male and Female Delinquent's attachment and effects of attachments on Security of Self-Reported Delinquency", *Crime and Behaviour,* vol. 26, no. 4, pp. 435-452.

53. Huth, M. R. A. (2001), *Secure Communicating System-Design, Analysis and Implementation,* Cambridge University Press.

54. Icove, D. C. and Vonstorch, K. (1999), *Computer Crime, A Crime fighter's Handbook,* O'Reilly and Associates, Inc, Sebastopol, CA.

55. Jaeger, T. and Rubin, A. D. (1996), "Preserving integrity in remote file location and retrieval", *Proceedings of Internet Society Symposium on Network and Distributed Systems Security,* 22-23 Feb. 1996, San Diego, CA, USA, IEEE Comput. Soc. Press, Los Alamitos, CA, USA, pp. 53-63.

56. Jie, W., Fernandez, E. B. and Zhang, R. (July 1992), "Some extensions to the lattice model for computer security", *Computers & Security,* vol. 11, no. 4, pp. 357-69.

57. K, C. and S, H. (2006), "Feature-based survey of model transformation approaches", *IBM Systems Journal,* vol. 45, no. 3, pp. 621-645.

58. Kaliontzoglou, A., Sklaros, P. and Karantjias, T. (2005), "A secure e-government Platform Architecture for Small to Medium Sized Public Organization", vol. 4, no. 2, pp. 174-86.

59. Karabacak, B. and Sogukpinar, I. (2005), "Information Security Risk Analysis method", *J comput secur,* vol. 24, pp. 147-159.

60. Karabacak, B. and Sogukpinar, I. (Sept 2006), "A quantitative method for ISO17799 gap analysis", *Computer and Security,* vol. 25, no. 6, pp. 413-19.

61. Kaylor, C., Deshazo, R. and Van Eck, D. (2001), "Gauging e-government: A report on implementing services among American cities", *Government Information Quarterly,* vol. 18, pp. 293-307.

62. Keller, J. (1974), "Optimum checking schedules for systems subject to random failure", *Management Science,* vol. 21, no. 3, pp. 256-260.

63. Kesh, S., Ramanujan, S. and Nerur, S. (2002), "A Framework for Analyzing e-commerce Security", *Computer and Security,* , pp. 149-158.

64. King, C. M., Dalton, C. E. and Osmanoglu, T. E. (2001), *Security Architecture-Design, Development & Operations, Business and Application Drivers (Case Study),* McGraw-Hill/Osborne.

65. Klander, L. (2002), *Hacker Proof,* 2nd ed, CENGAGE Delmar Learning, U.S.

66. Krull, R. A. (1996), "Generally-Accepted System Security Principles: A trip to Abilene?", *Proceedings of COMPSEC International 1996. 13th World Conference on Computer Security Audit and Control,* Vol. 15, 22-25 Oct.1996, London, UK, Elsevier, UK, pp. 567-75.

67. Kumar, R. (1996), *Research Methodology a Step-By-Step Guide for Beginners,* 1st ed, Addison Wesley Longman Australia Pty Limited, Australia.

68. Kurtz, R. L. and Vines, R. D. (2002), *CISSP Prep Guide,* 1st ed, Wiley.

69. Lambrinoudakis, C., Gritzals, S., Dridi, F. and Pernul, G. (2003), "Security Requirements for e-government services: a mathematical approach for developing a common PKI-based Security Policy", vol. 26, pp. 1873-1883.

70. Lambrou, M. A. (2003), "Advancing the One-Stop Shop E-Government Paradigm", 2-4 Nov 2003, Albany, NY, USA, IEEE, Piscataway, NJ, USA, pp. 489-93.

71. Lankhorst, M. (2005), *Enterprise Architecture at Work,* 1st ed, Springer, Berlin.

72. Lanotte, R., Maggiolo-Schettini, A., Tini, S., Troina, A. and Tronci, E. (2004), "Automatic Analysis of the NRL pump", *Elsevier Science/Electronic Notes in Theoretical Computer Science,* , pp. 245-266.

73. Lee, J. and Lee, Y. (2002), "A holistic model of computer abuse within organizations", *Information Management and Computer Security,* , pp. 57-63.

74. Lindgreen, E. E. O. R. and Herschberg, I. S. (1994), "On the Validity of the Bell-LaPadula model", *Computers & Security,* vol. 13, no. 4, pp. 317-33.

75. Lindup, K. R. A. (1995), "New Model for Information Security Policies", *Proceedings of COMPSEC International 1995,* 25-27 Oct. 1995, London, UK, SRI International, Oxford, UK, pp. 95-121.

76. Lipner, S. (1982), "Non-Discretionary Controls for Commercial Applications", *Proceedings of the 1982 Symposium on Security and Privacy,* 1982, Oakland, CA, USA, IEEE, New York, NY, USA, pp. 2-10.

77. Loch, k. D., Carr, H. H. and Warkentin, M. E. (1992), "Threats to information system: Today's reality, yesterday's understanding", *MIS Quarterly,* vol. 16, no. 2, pp. 173-186.

78. Madnick, E. S. (1978), "Management politics and procedures needed for effective computer security", *Sloan management review,* , pp. 61-74.

79. McClure, S., Scambray, J. and Kurtz, G. (2002), *Hacking Exposed Cryptography,* McGraw-Hill/Osborne.

80. Mckosky, R. A. (1990), "File integrity checking system to detect and recover from programme modification attacks in a multi-user computer systems", *Computer & Security,* vol. 9, no. 5, pp. 431-46.

81. Mclean, J. (1990), "Security Models and Information Flow", *Proceeding.1990 IEEE Computer Society Symposium on Research in Security and Privacy,* 7-9 May 1990, Oakland, CA, USA, IEE Comput. Soc. Press, Los Alamitos, CA, USA, pp. 180-7.

82. Mitra, A. (2005), "Direction of electronic governance initiatives within two worlds: case for a shift in emphasis", *Electronic Government,* vol. 2, no. 1, pp. 26.

83. Mitrakas, A. *Information Security and law in Europe: Risks checked?* Europe network and information security agency (ENISA), Greece.

84. Moeller, R. R. (1981), *Computer Control and Security,* 1st ed, Wiley, New York.

85. Nichols, R. K., Ryan, D. J. and Ryan, J. J. C. (2000), *Defending your Digital Assets Against Hackers, Crackers, Spies & Thieves,* 1st ed, McGraw-Hill, U.S.

86. Northcutt, S., Novak, J. and McLachlan. D. (2000), *Network Intrusion Detection an Analyst's Handbook,* New Riders Publishing.

87. O'Gorman, L. (2003), "Comparing passwords, tokens, and biometrics for user authentication", *Proceedings of the IEEE,* vol. 91, no. 12, pp. 2021-40.

88. O'Leary, Z. (2004), *The Essential Guide to Doing Research,* 1st ed, SAGE, SAGE Publication Inc, 2455 Teller Road, Thousand Oaks, California 91320.

89. Oppliger, R. (1998), *Internet and Intranet Security "Access Control Mechanisms",* Artech House.

90. Ozier, W. (1998), "GSSP Preface/Overview", *Computers and Security,* vol. 17, pp. 14-18.

91. Pabrai, U. O. and Gurbani, V. K. (1996), *Internet and TCP/IP Network Security-Securing Protocols and Applications, Firewall Systems,* McGraw-Hill.

92. Pelitier, T. R. (1998), *Information Security Policies and Procedures,* Auerbach, New York.

93. Perry, W. E. (1982), "Developing a Computer Security and Control Strategy", vol. 1, no. 1, pp. 17-26.

94. Pheeger. C.P. (1997), *Hash Algorithms,* Prentice Hall.

95. Platt, A. and Warwick, S. (1995), "Review of soft systems methodology", *Industrial Management + Data Systems,* vol. 95, no. 4, pp. 19-21.

96. Posthumus, S. and Von Solms, R. (2004), "A framework for the governance of Information Security", *Computer & Security,* vol. 23, pp. 638-646.

97. Qasem, I. R., Yaghi, H. M. and Hubbell, J. N. (1990), "Computer viruses: Detection and prevention techniques", *southeastcon 90 proceedings,* Vol. 1, 1-4 April 1990, New Orleans, LA, USA, IEEE, New York, NY, USA, pp. 199-201.

98. Qlnes, J. (1994), "Development of Security Politics", *Computer and Security,* vol. 13, pp. 628-636.

99. Quirchmayr, G. (1997), "Selected Legal Issues Related to Internet Use", 1997, ENCRESS, .

100. Rainer, R. K., Jr, Snyder, C. A. and Carr, H. H. (1991), "Risk analysis for information technology", *Journal of Information Management Information Systems,* vol. 8, no. 1, pp. 129-147.

101. Reddick, C. (2005), "Citizen interaction with e-government: From the streets to servers?", *Government Information Quarterly,* vol. 22, no. 38-57.

102. Relyea, H. C. (2002), "E-gov: introduction and overview", *Government Information Quarterly,* vol. 19, no. 1, pp. 9-35.

103. Richardson, R. (2007), Computer Crime and Security Survey, 12, CSI.

104. Risk Advisory Services Group (2006), 2006 Global Information Security Survey; EYG No. AU0022, Ernst & Young, UK.

105. Riskwatch (2005), *Rw-Information systems*, available at: http://www.riskwatch.com/.

106. Robson, C. (2002), *Real World Research,* 2nd ed, Blackwell Publication, US.

107. Sadeqhi, A. R. and Stuble, C. (2005), "Towards Multilaterally secure computing platforms with open source and trusted computing", *Information Security Technical Report,* vol. 10, no. 2, pp. 83-95.

108. Sampler, J. and Eigner, S. (2003), *Sand to Silicon, Achieving Rapid Growth Lessons From Dubai,* First ed, Profile Books Ltd, UK.

109. Schechter, S. (2004), *A thesis presented for Computer Security Strength & Risk: A Qualitative Approach* (unpublished PhD in Computer Science thesis), Harvard, US.

110. Schneier, B. (2004), *Secrets and Lies, Digital Security in a Networked World,* 1st ed, Wiley, US.

111. Schneier, B. (2003), *Practical Cryptography,* 1st ed, Wiley, US.

112. Schneier, B. (1996), *Applied Cryptography, Protocols, Algorithms and Source Code in C,* John Wiley & Sons, Inc, New York.

113. Schneier, B. (2001), "Managed Security Monitoring, Network Security for the 21st Century", *Commuter Secur. J.,* vol. 17, no. 2, pp. 1-12.

114. Schroder, N. (2005), *Forecast: Security Software, Worldwide,2005-2009*, Gartner.

115. Schumacher, H. J. and Gosh, S. (1998), "Fundamental framework for network security towards enabling security on demand in an ATM network", *Computers & Security,* vol. 17, no. 6, pp. 527-542.

116. Siponen, M. T. (2001), "Five Dimensions of Information Security Awareness", *Computers and Society,* vol. 31, no. 2, pp. 24-9.

117. Skinner, W. F. and Fream, A. M. (1997), "A social learning theory analysis of computer abuse among college students", *Journal of Research in Crime and Delinquency,* vol. 34, no. 4, pp. 495-518.

118. Smith, D. A. and Garton, P. R. (1989), "Specifying specific deterrence", *American Sociological Review,* vol. 54, pp. 94-106.

119. Smith, M. (1993), *Commonsense Computer Security, Your Practical Guide to Information Security,* McGraw-Hill, London.

120. Solms, V. B. (2005), "Information Security Governance: COBIT or ISO 17799 or both?", *Computers and Security,* vol. 24, no. 2, pp. 99-104.

121. Stallings, W. and Brown, L. (2008), *Computer Security: Principles and Practice,* 1st ed, Pearson Education, Inc, Upper Saddle River, NJ.

122. Stien, L. D. *Certifying Authorities and the Public Key Infrastructure: Web Security-A Step by Step Reference Guide,* Addison Wesley.

123. Straub, D. W. (1990), "Effective IS security :an empirical study", *Information Systems Research,* vol. 1, no. 3, pp. 255-276.

124. Swiderski, F. Snyder, W.C (2004), *Threat Modelling,* Microsoft Press, Redmond, Washington.

125. Symantec Inc., (2002), *Managing IT Risks in Business*, 1st ed., Symantec Marketing Team, Dubai.

126. Tanaka, H., Mastuura, K. and Sudoh, O. (2005), "Vulnerability and information security investment: An empirical analysis of e-local government in Japan", vol. 24, pp. 37-49.

127. Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2005), "The Insider threat to information systems and the effectiveness of ISO17799", *Computers & Security,* vol. 24, no. 6, pp. 472-84.

128. Thuraisingham, B. (1995), "Multilevel Security for information retrieval systems-II", *Information and Management,* vol. 28, no. 1, pp. 49-61.

129. Tipton, H. F. and Krause, M. (2000), *Information Security Management,* Auerbach Publications, New York.

130. Tiwana, A. (1999), *Are Firewalls Enough?* Web Security, Digital Press.

131. TOGAF Forum (2007), "The Open Group Architecture Framework (TOGAF 8.1.1 'The Book)", in TOGAF Forum (ed.) *The Open Group Architecture Framework,* 8.1.1 ed, Van Haren Publishing, , pp. 541.

132. Tomonori, F. and Masanori, O. (2003), "Protecting the integrity of an entire file system", *Proceedings First IEEE International Workshop on Information Assurance. IWIA 2003,* 24 March 2003, Darmstadt, Germany, IEEE Comput. Soc, Los Alamitos, CA, USA, pp. 95-105.

133. Torres, L., Pina, V. and Acerete, B. (2005), "E-government developments on delivering public services among EU cities", *Government Information Quarterly,* vol. 22, no. 2, pp. 217-38.

134. Tudor, J. K. (2002), *Information Security Architecture-An Integrated Approach to Security in the Organization,* Auerbach.

135. Turban, E., King, D., Lee, J., Warkentin, M. and Chung, M. H. (2001), *Electronic Commerce 2002: A Managerial Perspective,* 1st ed, Prentice Hall, Prentice Hall.

136. Venter, H. S. and Ellof, J. H. P. (2003), "A taxonomy for Information Security Technologies", *Computers and Security,* vol. 22, no. 4, pp. 299-307.

137. Von Solms, R. (1999), "Information Security Management: Why Standards are important", *Information Management and Computer Security,* vol. 7, no. 1, pp. 50-57.

138. Von, S., B. and Von, S., R. (2004), "The 10 deadly sins of information security management", *Computer and Security,* vol. 23, no. 5, pp. 371-6.

139. Walker, K. M. and Cavanaugh, L. C. (1998), *Computer Security Policies and SunScreen Firewalls,* Prentice Hall.

140. Wauters, P., Nijskens, M. and Tiebout, J. (2007), The User Challenge Benchmarking The Supply of Online Public Services, 7, Capgemini, Paris, France.

141. Wauters, P. and Durme, v. P. (2004), Online Availability of public services: how is Europe processing? Web Based Survey on Electronic Public Services, 5, Capgemini, Paris, France.

142. Wheatman, V. (2005), Management Update: The Future of Enterprise Security, G00123949, Gartner Inc, Gartner.

143. Wheeler, P. and Fulp, E. (2007), "A taxonomy of parallel techniques for intrusion detection", *Proceedings Of the 45th ACM Southeast Conference, ACMSE 2007,* Mar 23-Jul 24 2007, Winston-Salem, NC, United States, Association for Computing Machinery, New York, NY 10036-5701, United States, pp. 278-282.

144. White, G. B., Fisch, E. A. and Pooch, U. (1996), *Computer System and Network Security,* , CRC Press.

145. Wood, C. (2005), *Security Policy Made Easy,* 10th ed, Information Shield, U.S.

146. Yixin, J., Chuang, L. and Zhangxi, T. (2003), "An authentication model for multilevel security domains", *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme - System Security and Assurance (Cat. No.03CH37483),* 5-8 Oct 2003, Washington, DC, USA, IEEE, Piscataway, NJ, USA, .

147. Zadeh, L. A. (2000), "Fuzzy Sets", *Information Control,* vol. 19-21, pp. 8, 338-353.

148. Zviran, M. and Haqa, W., J. (1990), "User authentication by cognitive passwords: An empirical assessment", Oct 22-25 1990, Jerusalem, Isr, IEEE, Los Alamitos, CA, USA, pp. p 137-144.

Appendices

- Appendix A: Questionnaire A
- Appendix B: Questionnaire B
- Appendix C: Feedback form for questionnaire A&B
- Appendix D: Validation confirmation from DEG authority

Appendix A: Questionnaire A

Questionnaire-A

Distinguished government department leader information
Name:…….
Title/Designation:……..
Department Name:…….. **Function:……**
Number of Staff……

Purpose:

This questionnaire is intended for management of the e-government authority or the governmental departments' interacting, transacting or exchanging information with the e-government authority or other departments.

Questionnaire structure

There are three main sections of this questionnaire, General e-Government, Internal and External.

- Section 1: General e-government questions

Questions which are related to e-government in general

- Section 2: The internal questions:

Questions which are related to the e-government authority or the governmental department interacting with or through the e-government authority.

- Section 3: The external questions:

Questions which are related to the expectations, threats, and needs generated from trading with other governmental departments or the public.

- References:

1. e-government Authority (e-gov-auth): The government body which offers e-services to other governmental departments and the citizens of the country.

2. Governmental departments: government organisations or agencies interacting with the e-government authority for e-services or offering e-services to citizens through the e-government authority

Section 1: General e-government questions

1. What type of services your governmental department is providing

☐ Information publishing any online available information necessary to start the procedure to obtain an e-service or a catalogue of other e-services offered by the e-government.
☐ A one way interactive e-service which is a downloadable form from the governmental department portal (I-1).
☐ Two-Way Interactive e-services which requires both parties to interact through the governmental department portal (I-2).
☐ A transactional e-service where the users can perform a financial transaction through the governmental department portal. These e-services can be referred to as class (T).
☐ A combination of all the above

Information security measures are essential part of any e-government infrastructure in order to enable the e-government to provide services to the public, protect the information from internal staff, and allow the information flow for interaction, transaction, or publishing with other governmental departments.

☐ Yes, I agree with the above statement
☐ No, I don't agree with the above statement

The current e-government information security programme covers or must cover as an assumption the following security practices:

☐ P1- Information classification policies and procedures
☐ P2- Encryption of classified information related to governmental departments.
☐ P3- Strong authentication for the staff of the e-government authority to the internal network and information resources.
☐ P4- Access control to enforce the concepts of separation of duties and need to know.
☐ P5- Anti-virus programmes (PC based or gateway) which protect from viruses/worms attacks or spread from inside or outside.
☐ P6- Security operation management and monitoring.
☐ P7- Strong and enforced information security policies and procedures.
☐ P8-Network security measures such as firewalls, IDS/IPS, VPN concentrators, etc
☐ P9-Others……

Section 2: Internal security related questions

Internal Threat

1. Select from the list below some of the relevant major threats to the e-government infrastructure which might be caused internally?

☐ T1- Disgruntled employees having access to non-authorized information resources.
☐ T2- Viruses spread intentionally or unintentionally by e-government staff
☐ T3- Loss or corruption of data caused to applications/OS malfunctions, database issues, etc.
☐ T4- Failure of restoration after a major unplanned shutdown due to weak operational and recovery procedures.
☐ T5- Exposure of classified data to unauthorized staff due to a failure of encryption system.
☐ T6- Lack of security and operational competency due to the introduction of new e-services or new technologies supporting the new services.
☐ T7- High mobility of the e-government staff which will increase the threat of accessibility
☐ T8- Leakage of information or espionage related to the privacy of the citizen or public users through electronic transfer, physical leakage through medium handing over, or oral information exchange.
☐ T9- Data and records alteration related to public users or governmental departments.
☐ T10- Attacks on all mission critical systems, and processes from within the governmental departments.
☐ T11- Industrial spies and governmental espionage conducted by internal terrorist and spies working within the governmental departments.
☐ T12- Information dealers looking for classified and sensitive information of publish users/citizens, or other governmental departments.
☐ T13-
Others……
…….

The impact of any threat becomes severe due to the following reasons:

☐ Lack of security knowledge in how to handle an incident.
☐ Lack of proactive security systems which can reduce the impact and contain the risk.
☐ Lack of strong security operational and management systems which assist in the vigilant monitoring of the infrastructure.
☐ Weak security and IT infrastructure which is vulnerable to any level of attacks or security threats.
☐ High dependency on the security systems in running the business operation.
☐ The direct link between the internal e-government infrastructures to the external parties interacting with.

Is there a frequent security assessment programme which runs in the e-government authority?

☐ Yes there is ☐ No there isn't

From your management experience, the security assessment of any e-government authority must cover some if not all of the following:

☐ Technologies used in the e-government
☐ Policies enforced and practiced in the e-government
☐ Competencies available locally or outsourced by the e-government
☐ Security operational procedures enforced and practiced by the e-government
☐ Decision factors and matrix on the security operation, technology selection, and change management.

Do you feel the current security infrastructure available in the e-government authority is capable of protecting all the information resources, allowing customers or other governmental departments to interact in security manner with the authority and enabling the e-government authority to launch more services in the future?

☐ Yes I do ☐ With some extend ☐ No I don't, my improvement is required
☐ Can't tell

How often do you go over or review the security programme available within the e-government authority?

☐ Once a month
☐ Every Quarter
☐ Semi Annual
☐ Annual
☐ Never
☐ Others ……

Is the security programme/system known by all internal e-government staff?
☐ Yes ☐ No

Is the security programme linked directly to the business processes of the e-government authority and integrated with the services launching processes?

☐ Yes ☐ No ☐ Will be in the future

Section 2: External Security Related Questions

What is your definition of an e-government authority?

A common gateway for governmental e-services
A relay and a workflow engine of governmental e-services offered by different departments
An e-catalogue to all e-services offered by different governmental departments

A point of consolidation for shared services of all e-governmental departments
Nothing but a portal
Part of the e-initiative of all governmental departments

2. How many individual users do you expect to have per e-service you offer?

☐ Less than 1,000 users
☐ 1,000 – 10,000 users
☐ 10,000 – 100,000 users
☐ More than 100,000 users
☐ Don't have an exact number but approximately……..

3. How many integrated e-services or processes are you part of?

☐ 1-10 e-services
☐ More than 10 e-services
☐ All e-services offered by the department
☐ None of the e-services offered by the department

4. Please select the closest description of the types of users for the e-services offered by your department:

☐ Public users and residents of the country
☐ Corporate users or representatives of governmental departments who are dealing directly with the department.
☐ Mixed of both public and corporate users

5. Do you feel that your e-services will require a certain level of computer literacy beyond using the Web in order to be accessed and used:

☐ Yes to a certain extent. Please specify…….
☐ No only knowing how to use the Web
☐ At the beginning only
☐ Can't tell

What is the total number of e-services offered directly by your department to all types of users:

☐ Less than 10 Approximate number:……....
☐ 10-100 Approximate number:……
☐ 100-1,000 Approximate number:……....
☐ More than 1,000 Approximate number:……

Kindly fill the following table in order to indicate the number of e-services per each category:

e-services Categories	Information Publishing	One-Way Interactive e-Services	Two-Way Interactive e-Services	Transactional e-Services	Total
Number					

External Threats

8. Please select some of the related threats and fear factors from dealing with the external customers (governmental or individuals) related to the e-services you offer?

☐ T1- Declassification and mishandling of information flowed between the e-government authority and other departments or individual customers.
☐ T2- Man in the middle attacks and interception which may expose the classified information from the e-government to the other departments or individual customer.
☐ T3- Denial of services due to intentional actions (attacks) or unintentional actions (operational problems).
☐ T4- Attacks generated from e-government external users whether from other departments or citizens interacting, transacting, or exchanging information with the e-government authority.
☐ T5- Viruses coming from the governmental departments which are not having good anti-virus infrastructure.
☐T6- Rerouted attacks through penetrated e-government departments by external hackers or attackers.
☐ T7- Financial frauds due to impersonation of authorized users, systems flaws, or non-repudiation.
☐ T8- Miscofiguration of any IT infrastructure element which may lead to leakage of information, wrong assignment of e-services, fraud, or corruption of data.
☐ T9- Disruption of a complete cycle of an e-service due to latency of the network, low bandwidth, or bad integration.
☐ T10- Information alteration or unauthorized modification (information integrity breach)
☐ T11- Physical security breach which may cause of a total destruction of the IT infrastructure.
☐ T12-
Others…….

Why do you think the probability of having a threat coming from an external governmental department is high?

☐ Lack of auditing of governmental department security level and systems.
☐ Lack of a rule or regulation which enforces the equality in the security level of any governmental departments prior to the interaction, transaction, or exchanging of information.

☐ Different perception of how security systems/programmes must be built within any governmental department or e-government authority.
☐ Security is not the main concern of the e-government authority or governmental departments.
☐ No common security framework or model which can be applied on the e-government and its governmental departments and citizens.

What are the key security problems and issues do you think that most if not all governmental department may have?

☐ Security issues related to the Information and security technologies implemented in the governmental department.
☐ Lack of strong security policies which cover all the critical and sensitive areas related to the information handling with other departments/citizens, access of information, and protection of the infrastructure supporting key e-services.
☐ Lack of having competent and strong security practitioners with the governmental department and fully relaying on vendors support, and best efforts from locally available staff.
☐ No vigilant monitoring and strong security operational procedures within the government department.
☐ Wrong decisions regarding implementation of security technologies, enforcement of security policies, and hiring the right staff for the right security jobs.
☐ Security is not being studied carefully and deeply as a business enabler within the governmental departments.
☐ Other reasons…….

What are you expecting from the other governmental departments before exchanging any information:

☐ A review of the applied security policy
☐ A review of the security architecture and infrastructure implemented within the governmental department
☐ A list of the security practitioners and their professional qualifications
☐ A proof of strong security operational procedures within the governmental department.
☐ A security certification such as ISO17799 and other security related certifications
☐ Copy of the BCP/DRP plan implemented with the government department
☐ Others…….

Do you feel comfortable dealing with other governmental departments or citizens without knowing the security level applied in their infrastructure?

☐ Yes ☐ No but can't do anything about it ☐ Don't think it is necessary to know

What do you think is the best way for implementing security measures for the citizens/individual users of e-government e-services:

☐ Installing all security programmes in the citizen PCs
☐ Developing an awareness programme for all public users
☐ Restrict accessibility of e-government authority or any governmental department except from special terminals and kiosks.
☐ Apply the third factor of security (biometrics) for all services accessibility
☐ Run manual authentication in parallel to all e-services authentication

Appendix B: Questionnaire B

Questionnaire-B

Governmental department information technology leaders or security practitioners

Name: ……
Designation:……
Governmental Department:……..
Security Certification:

☐ **CISSP** ☐ **SAN Level…..** ☐ **CISA** ☐ **ICSA**
☐ **Other……**

Number of Years in the Field of Security:
☐ **3-5 years** ☐ **5-10 years** ☐ **10-15 years** ☐ **More**

Domain Knowledge and Background
☐ Programming ☐ Security Policy Developer ☐ Security Architect
☐ Ethical Hacking ☐ Vulnerability and Risk Assessment
☐ Security Operation ☐ Network Security ☐ Security Education
☐ IT Expert and General IT Operation ☐ Security Decision Maker Executive
☐ Others……..

Purpose:

To ask security practitioners for their opinion on what should be the best security model to protect organisations exchange or interact over the Internet.

Questionnaire structure

Section 1: e-Government Questions
Section 2: Information Security Technologies
Section 3: Information Security Policies
Section 4: Information Security Competencies
Section 5: Information Security Management and Monitoring
Section 6: Decision Factors
Section 7: Correlation Questions

Relevance

Each question of this questionnaire will address a challenge of security at your organisation without regard to whether it now exists or it may exist in the future. A box of non-applicable (N/A) is assigned to each question in order to eliminate the scenarios irrelevant to your organisation. Space for comments from the practitioners is also assigned.

Section 1: e-Government related questions

1. Select the challenge an e-government is facing in terms of information flow:

☐ Trust between the e-government body and the governmental departments
☐ No common rule and or standard which controls this flow of information
☐ The technical infrastructure challenges
☐ No direct relation between the government departments and the e-government except on the services the e-government offers.
☐No assurance in data classification or declassification

2. Do you think e-governments will need to have a standard assessment model in order to synchronize the level of security for intra or inter communication?

☐ Yes ☐ Not necessarily

3. Can we state that the data classification and the standard security assessment model will encourage government departments to freely exchange information between themselves and the e-government body?

☐ Yes ☐ Not really, please state other challenges……
……

4. Do you think the fact that cyber crimes occurred for e-governments will force the implementation of a standard assessment model in all organisations related to the e-government?

☐ Yes ☐ No

5. Do you feel that standardizing the technologies, policies, competencies, security operations, and decision factors in e-government will assist the information flow in security manners?

☐ Yes ☐ No

6. What type of services are your governmental department providing

☐ Information publishing any online available information necessary to start the procedure to obtain an e-service or a catalogue of other e-services offered by the e-government.
☐ A one way interactive e-service which is a downloadable form from the governmental department portal **(I-1).**
☐ Two-Way Interactive e-services which requires both parties to interact through the governmental department portal **(I-2)**.
☐ A transactional e-service where the users can perform a financial transactions through the governmental department portal. These e-services can be referred to as class **(T).**
☐ A combination of all the above

Internal threats

7. Select from the list below some of the relevant major threats to the e-government infrastructure which might be caused internally?

☐ **T1-** Disgruntled employees having access to non-authorized information resources.
☐ **T2-** Viruses spread intentionally or unintentionally by e-government staff
☐ **T3-** Loss or corruption of data caused to applications/OS malfunctions, database issues, etc.
☐ **T4-** Failure of restoration after a major unplanned shutdown due to weak operational and recovery procedures.
☐ **T5-** Exposure of classified data to unauthorized staff due to a failure of encryption system.
☐ **T6-** Lack of security and operational competency due to the introduction of new e-services or new technologies supporting the new services.
☐ **T7-** High mobility of the e-government staff which will increase the threat of accessibility
☐ **T8-** Leakage of information or espionage related to the privacy of the citizen or public users through electronic transfer, physical leakage through medium handing over, or oral information exchange.
☐ **T9-** Data and records alteration related to public users or governmental departments.
☐ **T10-** Attacks on all mission critical systems, and processes from within the governmental departments.
☐ **T11-** Industrial spies and governmental espionage conducted by internal terrorist and spies working within the governmental departments.
☐ **T12-** Information dealers looking for classified and sensitive information of public users/citizens, or other governmental departments.
☐ **T13-**
Others……
……

8. Can you relate the different types of **internal threats** to the different types of services offered by your department by filling the following table?

e-Service Category	Information Publishing	One-way Interactive e-Services	Two-way Interactive e-services	Transactional e-Services
Threats Associated	T(_),(_),(_),(_),(_) (_),(_),(_),(_),(_)	T(_),(_),(_),(_),(_) (_),(_),(_),(_),(_)	T(_),(_),(_),(_),(_) (_),(_),(_),(_),(_)	T(_),(_),(_),(_),(_) (_),(_),(_),(_),(_)

External Threats

9. Please select some of the related threats and fear factors from dealing with the external customers (governmental or individuals) related to the e-services you offer?

☐ **T1-** Declassification and mishandling of information flowing between the e-government authority and other departments or individual customers.
☐ **T2-** Man in the middle attacks and interception which may expose the classified information from the e-government to the other departments or individual customer.
☐ **T3-** Denial of services due to intentional actions (attacks) or unemotional actions (operational problems).
☐ **T4-** Attacks generated from e-government external users whether from other departments or citizens interacting, transacting, or exchanging information with the e-government authority.
☐ **T5-** Viruses coming from the governmental departments which are not having good anti-virus infrastructure.
☐**T6-** Rerouted attacks through penetrated e-government departments by external hackers or attackers.
☐ **T7-** Financial frauds due to impersonation of authorized users, systems flaws, or non-repudiation.
☐ **T8-** Mis-configuration of any IT infrastructure element which may lead to leakage of information, wrong assignment of e-services, fraud, or corruption of data.
☐ **T9-** Disruption of a complete cycle of an e-service due to latency of the network, low bandwidth, or bad integration.
☐ **T10-** Information alteration or unauthorized modification (information Integrity breach)
☐ **T11-** Physical security breaches which may cause of a total destruction of the IT infrastructure.
☐ **T12-**
Others…….

9. Can you relate the different types of **External threats** to the different types of services offered by your department by filling the following table?

e-Service Category	Information Publishing	One-way Interactive e-Services	Two-way Interactive e-services	Transactional e-Services
Threats Associated	T(_),(_),(_),(_),(_) (_),(_),(_),(_),(_)	T(_),(_),(_),(_),(_) (_),(_),(_),(_),(_)	T(_),(_),(_),(_),(_) (_),(_),(_),(_),(_)	T(_),(_),(_),(_),(_) (_),(_),(_),(_),(_)

10. The impact of any threat (internal or external) becomes severe due to the following reasons:

☐ Lack of security knowledge in how to handle an incident.
☐ Lack of proactive security systems which can reduce the impact and contain the risk.
☐ Lack of strong security operational and management systems which assist in the vigilant monitoring of the infrastructure.
☐ Weak security and IT infrastructure which is vulnerable to any level of attacks or security threats.
☐ High dependency on the security systems in running the business operation.
☐ The direct link between the internal e-government infrastructures to the external parties interacting with.

Section 2: Information security technology

1. Are all necessary security technologies implemented in your organisation?

☐ Yes ☐ No ☐ Some

2. The security system includes all necessary components which cover multiple layers and are not restricted to technologies or policies only:

☐ Yes ☐ No

3. The implementation of the security architecture at your organisation includes the following technologies if not all:

☐ Access Control (A1)	☐ Intrusion Detection & Prevention (A2)
☐ Anti-Virus & Malicious Codes Scanners (A3)	☐ Authentication & Passwords (A4)
☐Files Integrity Checks (A5)	☐ Cryptography (A6)
☐VPN (A7)	☐ Vulnerability Scanning Tools (A8)
☐ Digital Signature and Digital Certificates (A9)	☐Biometrics (A10)
☐ Logical Access Control (Firewalls) (A11)	☐ Security Protocols (A12)
☐ Combination of other technologies such as…….....	

4. Which one of the above technologies do you feel is sufficient enough to provide the organisation enough protection against cyber crimes, denial of services (intentional or unintentional), or loss of data and confidentiality:

☐ Access Control (A1)	☐ Intrusion Detection & Prevention (A2)
☐ Anti-Virus & Malicious Codes Scanners (A3)	☐ Authentication & Passwords (A4)
☐ Files Integrity Checks (A5)	☐ Cryptography (A6)
☐ VPN (A7)	☐ Vulnerability Scanning Tools (A8)
☐ Digital Signature and Digital Certificates (A9)	☐ Biometrics (A10)
☐ Logical Access Control (Firewalls) (A11)	☐Security Protocols (A12)
☐ Combination of other technologies such as…….....	

5. Which technology do you find unnecessary when building a security system:

☐ A1 ☐ A2 ☐A3 ☐ A4 ☐ A5 ☐ A6
☐ A7 ☐ A8 ☐ A9 ☐ A10 ☐ A11 ☐ A12

6. Can all security technologies mentioned above coexist in one layer of a model?

☐ Yes ☐ No

7. Can all above mentioned technologies (A1…A12) construct be part of a risk assessment for the security technologies in any organisation?

☐ Yes ☐ No

If No, please state reasons……
……

8. Can we rate the technological security level by the number of security technologies available in any organisation?

☐ Yes ☐ No

If No, please state reasons……
……

9. Please assign the following technologies a percentage for their importance to any e-organisation:

Access Control (A1)___%	Intrusion Detection & Prevention (A2) ___%
Anti-Virus & Malicious Codes Scanners (A3) ___%	Authentication & Passwords (A4) ___%
Files Integrity Checks (A5) ___%	Cryptography (A6) ___%
VPN (A7) ___%	Vulnerability Scanning Tools (A8) ___%
Digital Signature and Digital Certificates (A9) ___%	Biometrics (A10) ___%
Logical Access Control (Firewalls) (A11) ___%	Security Protocols (A12) ___%

10. Considering the scenario of organisation A and B having business information exchange over the Internet on a frequent basis, do you feel both organisations must have the same level of security technology?

☐ Yes ☐ No ☐ Not Sure ☐ To a certain level, please state the level as percentage____%

11. Can all mentioned technologies, as part of one layer, be the only level of security an organisation has?

☐ Yes ☐ No, state other layers/levels of security an organisation must have:_____
_____

12. Please select from the list below some of the challenges related to the technologies mentioned on any security technology that can be used in your organisation.

☐ Lack of competencies related to the technology applied.
☐ Lack of security policies
☐ No in-depth threat analysis done prior of implementation
☐ Lack of management and monitoring
☐Decision is always based on commercial aspects not technical/security requirements.
☐ Integration with other technologies
☐Right technology in wrong place
☐ Other reasons……

13. As a security expert or technologist, do you agree on the concept of having two entities at the same level of security must be a condition for any information flow over the Internet?

☐ Yes I do ☐ No, I don't agree,
reasons……
……

14. Have you come across any security model that can be applied to any organisation in order to confirm that security level prior exchanging information or assessing the level of security based on a checklist?

☐ Yes, please state the name of the model……..

☐ No ☐ Not Sure

15. As a security expert, or a technologist, do you feel that a model for security level assessment or checklist of any organisation that exchanges information, interact with customers, or transact over the Internet is a required?

☐ Yes ☐ No, not necessary,
Reasons:……

16. Please select some of the reasons for the security breaches which may occur due to exchange of information between two organisations over the Internet:

☐ Lack of security level matching (Org A might be higher than Org B in security level)
☐ Not enough protection measures applied
☐ Declassification of information from one side
☐ Due to technical security breaches or flaws
☐ Over trusting the Internet by sending information or allowing communication in clear text
☐ No common security model/system applied in both organisations
☐
Others,……

Section 3: Information security policies

1. Please rate the importance of the information security policy in relation to the full security system in any organisation:

☐ Not relevant ☐ Not Important ☐ Important ☐ Very Important

2. Please state the degree of relation between the information security policy and the information security technology:

☐ Not related ☐ Related ☐ Complement each Other ☐ Contradict each other

3. Having the two layers (Technologies and Polices) together in a security model will assist in building a robust security system:

☐ Agree ☐ Disagree

4. Which of the following policies do you think is mandatory to have in your organisation? Please assign a percentage.

□ Password Management (B1)___%	□ Data Privacy (B6) ___%	□ Administrative Policies (B11) ___%
□ Login Process (B2) ___%	□ Privilege Control (B7) ___%	□ Encryption Policies (B12) ___%
□ Logs Handling (B3) ___%	□ Data Confidentiality (B8) ___%	□ HR Security Policies (B13) ___%
□ Computer Viruses (B4) ___%	□ Data Integrity (B9) ___%	□ Third Party Policies (B14) ___%
□ Intellectual Property Rights (B5) ___%	□ Internet Connectivity (B10) __%	□ Physical Security Policies (B15) _%
□ Operation Security Policies (B16) __%	□ Others___%	

5. Do you think having some, but all policies mentioned above will help the organisation to reach a high level of security standard:

☐Yes ☐ No If yes, please justify……
……

6. Do you agree that most of the security breaches are related to violation of security policies?

☐ Agree ☐ Don't Agree

7. If two organisations are interacting with each other over the Internet, they must have enough assurance that they have applied the appropriate security policies in order to maintain the confidentiality, integrity, and availability of the information:

☐ Agree ☐ Don't Agree

8. Do you think having a checklist for the security policy implemented is a good method to assess the level of security for any organisation prior the exchange over the Internet is a good model to adopt?

☐ Yes ☐ No

Section 4: Competencies

1. What is the importance of security competencies in any organisation?

☐ Very important than technical competency ☐ As important as IT
☐ More important than IT ☐ Not important at all

2. Do you agree that most of security breaches are happening due to lack of information security competencies in the company?

☐Yes ☐ No

3. Do you follow any standard or method to assist you having the appropriate level of competencies developed in your organisation?

☐Yes, please specify
……

☐ No

4. Have you experienced a security incident due to a lack in a security company?

☐ Yes ☐ No

5. Do you outsource any security function to a third party due to a lack in a local competency?

☐Yes ☐ No

6. Please select the method of assessing the security competency in your organisation:

☐ Number of security certifications in the department of security
☐ Total number of experience in the security field
☐ Number of security training attended
☐ Total number of years in IT related field
☐ Other methods……

7. Do you agree that the security competency is a good method for assessing the level of security in any organisation?

☐ Yes ☐ No
If No, please state
why……

8. Please select from the list below the mandatory security competency to have in any organisation:

☐ Security Operation and Management (C1)	☐ Cryptography (C6)
☐ Security Architecture and development (C2)	☐ Security Programming (C7)
☐ Ethical Hacking (C3)	☐ Laws and Regulations (C8)
☐ Security Policies Development (C4)	☐ Security implementation and Configuration (C9)
☐ Computer Forensics (C5)	☐ Security Analysis (C10)
	☐ Others

9. Having a competency layer as part of the security model will enhance the security level of the organisation as a complement to other important layers also.

☐Agree with the statement
☐ Don't agree with the statement

10. Is there a direct link between security competencies and technologies policies implemented?

☐ Yes ☐ No

Section 5: Information security management and monitoring

1. Please state the importance of information security management and monitoring in any organisation:

☐ Not Important ☐ Important but not essential ☐ Very important

2. Would you consider information security management and monitoring for all security technologies implemented in your organisation?

☐Yes ☐ Not necessarily

3. Do you see a direct link between strength of the security programme/system in any organisation and the strength of the security?

☐ Yes ☐ No

4. Having a good level of security management and monitoring can give a good indication of the strength of the security competency, policies, and technologies in the organisation:

☐ Agree ☐ Don't agree

5. The strength of the security management and monitoring is measured based on:

☐Number of incidents handled
☐ Existence of the standard security operational procedure
☐Infrastructure supporting this function
☐ Response time to incidents
☐ Correlation of data collected from all security devices
☐ Others

6. Having organisations A and B exchanging information over the Internet will stress the need of security management and monitoring:

☐ True ☐ Not True

7. Which of the following you consider must to have as part of the security management and monitoring?

☐ Operational policies and procedures (D1)
☐Management tools (D2)
☐ Correlation and data management (D3)
☐ Reporting and response (D4)
☐ Analysis and human intervention (D5)
☐ Others,
state……
……

8. Do you think that having security operation and management as part of the risk assessment model is the right thing to do?

☐ Yes ☐ No

9. What's the percentage of importance you would give for the security operation and management as part of any security programme?

☐ 10-30%
☐ 31-50%
☐ 51-70%
☐ 71-100%

10. Have you experienced any security incident in your organisation or other places which was due to the lack of security operation and management?

☐ Yes ☐ No ☐ can't answer this question

11. Do you have the security operation and management as a local competency within the organisation or is it outsourced?

☐ Available within the organisation
☐ Outsourced

Section 6: Decision factor

1. How do you reach your decision for selecting or considering a security technology, policy, operational procedure, or hiring a resource with certain security competency?

☐ Cost factor
☐Background on the security subject
☐ Need or want
☐ Availability of competencies/technologies and ease of implementation
☐Others……
……

2. What are the factors which may change the decision of any security technology, policy, or implementation?

☐ Not having enough information on the subject
☐ No ROI justification
☐ Lack of competencies on the technology within the organisation
☐ High cost of implementation, training, and transition
☐ Major and core business processes change

3. What's the impact of any decision on the technology layer of any security system in any organisation?

☐ Deep impact on the competencies, policies, and operations
☐ No impact if the decision was carefully studied

4. What's the impact of any decision regarding the adaptation of some policies and leaving others in any organisation/

☐ Might defeat the security programme
☐ No effect if the security technologies were well architected
☐ Slight impact but not major

5. Do you feel that decision on security programme of any organisation will affect the method of communication and interaction the organisation has with others?

☐Yes ☐ No

6. Can we consider the decision factor as one of the factors an organisation must be assessed on as part of any security assessment programme?

☐Yes ☐ No

7. Is there a method of making the decision regarding any security technology, policies implementation, or having competencies layered so the impact becomes light on the core security programme of the organisation?

☐ Not aware of ☐ Yes,
state……
……

8. If two organisations A and B are communicating /exchanging information with each other, can we limit or ask for synchronization in decision making between them once the exchange of information starts?

☐ Yes ☐ No

9. Have you experienced a security breach in your organisation or in any previous job which was due directly or indirectly to a wrong decision made on the security programme/system of the organisation?

☐ Yes ☐ No

Section 7: Correlation questions

1. Let a set of a group of security measures which may contain technology, policies, competencies, operational procedures, and decision factors be considered a practice (P). What is the best practice (P) do you consider applicable, doable, and will give the maximum level of security level for any e-government authority or governmental department offering e-services. Please assign a total percentage of each P, next to it based on your industrial experience in the field of security.

Practice	Security Layers combinations
P1 (For Information Publishing e-Services)	☐A1 ☐A2 ☐A3 ☐A4 ☐A5 ☐A6 ☐A7 ☐A8 ☐A9 ☐A10 ☐A11 ☐A12 ☐B1 ☐B2 ☐B3 ☐B4 ☐B5 ☐B6 ☐B7 ☐B8 ☐B9 ☐B10 ☐B11 ☐B12 ☐B13 ☐B14 ☐B15 ☐B16 ☐C1 ☐C2 ☐C3 ☐C4 ☐C5 ☐C6 ☐C7 ☐C8 ☐C9 ☐C10 ☐D1 ☐D2 ☐D3 ☐D4 ☐D5 ☐E1 ☐E2 ☐E3 ☐E4 ☐E5
P2 (One-Way Interactive e-Services)	☐A1 ☐A2 ☐A3 ☐A4 ☐A5 ☐A6 ☐A7 ☐A8 ☐A9 ☐A10 ☐A11 ☐A12 ☐B1 ☐B2 ☐B3 ☐B4 ☐B5 ☐B6 ☐B7 ☐B8 ☐B9 ☐B10 ☐B11 ☐B12 ☐B13 ☐B14 ☐B15 ☐B16 ☐C1 ☐C2 ☐C3 ☐C4 ☐C5 ☐C6 ☐C7 ☐C8 ☐C9 ☐C10 ☐D1 ☐D2 ☐D3 ☐D4 ☐D5 ☐E1 ☐E2 ☐E3 ☐E4 ☐E5
P3 (Two-Way Interactive e-Services)	☐A1 ☐A2 ☐A3 ☐A4 ☐A5 ☐A6 ☐A7 ☐A8 ☐A9 ☐A10 ☐A11 ☐A12 ☐B1 ☐B2 ☐B3 ☐B4 ☐B5 ☐B6 ☐B7 ☐B8 ☐B9 ☐B10 ☐B11 ☐B12 ☐B13 ☐B14 ☐B15 ☐B16 ☐C1 ☐C2 ☐C3 ☐C4 ☐C5 ☐C6 ☐C7 ☐C8 ☐C9 ☐C10 ☐D1 ☐D2 ☐D3 ☐D4 ☐D5 ☐E1 ☐E2 ☐E3 ☐E4 ☐E5
P4 (Transactional e-Services)	☐A1 ☐A2 ☐A3 ☐A4 ☐A5 ☐A6 ☐A7 ☐A8 ☐A9 ☐A10 ☐A11 ☐A12 ☐B1 ☐B2 ☐B3 ☐B4 ☐B5 ☐B6 ☐B7 ☐B8 ☐B9 ☐B10 ☐B11 ☐B12 ☐B13 ☐B14 ☐B15 ☐B16 ☐C1 ☐C2 ☐C3 ☐C4 ☐C5 ☐C6 ☐C7 ☐C8 ☐C9 ☐C10 ☐D1 ☐D2 ☐D3 ☐D4 ☐D5 ☐E1 ☐E2 ☐E3 ☐E4 ☐E5
P5 (Combination of all e-services types)	☐A1 ☐A2 ☐A3 ☐A4 ☐A5 ☐A6 ☐A7 ☐A8 ☐A9 ☐A10 ☐A11 ☐A12 ☐B1 ☐B2 ☐B3 ☐B4 ☐B5 ☐B6 ☐B7 ☐B8 ☐B9 ☐B10 ☐B11 ☐B12 ☐B13 ☐B14 ☐B15 ☐B16 ☐C1 ☐C2 ☐C3 ☐C4 ☐C5 ☐C6 ☐C7 ☐C8 ☐C9 ☐C10 ☐D1 ☐D2 ☐D3 ☐D4 ☐D5 ☐E1 ☐E2 ☐E3 ☐E4 ☐E5

Selections definitions:

Security Technologies

- ☐A1 : Access Control
- ☐A2 : Intrusion Detection and Prevention
- ☐A3 : Anti-Virus & Malicious Code
- ☐A4 : Authentication and Passwords
- ☐A5 : Files Integrity Checks
- ☐A6 : Cryptography
- ☐A7 : VPN
- ☐A8 : Vulnerability Scanning Tools
- ☐A9 : Digital Signatures and Certificates
- ☐A10 : Biometrics
- ☐A11 : Logical Access Control (Firewalls)
- ☐A12 : Security Protocols

Security Policies

- ☐B1 : Password Management
- ☐B2 : Log-in Process
- ☐B3 : Logs Handling
- ☐B4 : Computer Viruses
- ☐B5 : Intellectual Property Rights
- ☐B6 : Data Privacy
- ☐B7 : Privilege Control
- ☐B8 : Data Confidentiality
- ☐B9 : Data Integrity
- ☐B10 : Internet Connectivity
- ☐B11 : Administrative Policies
- ☐B12 : Encryption Policies
- ☐B13 : HR Security Policies
- ☐B14 : Third Party Policies
- ☐B15 : Physical Security Policies
- ☐B16 : Operation Security Policies

Security Competencies

- ☐C1 : Security Operation and management
- ☐C2 : Security Architecture and development
- ☐C3 : Ethical Hacking
- ☐C4 : Security policies and development
- ☐C5 : Computer Forensics
- ☐C6 : Cryptography
- ☐C7 : Security Programming
- ☐C8 : Laws and regulations
- ☐C9 : Security implementation and configuration
- ☐C10 : Security Analysis

Security Operations and Management
☐D1 : Operational Policies and procedures
☐D2 : Management Tools
☐D3 : Correlation and data mining
☐D4 : Reporting and Response
☐D5 : Analysis and human intervention

Security Decision Factors
☐E1 : Cost
☐E2 : Awareness
☐E3 : Need
☐E4 : Technologies Availability
☐E5 : FUD

Appendix C: Feedback form (Questionnaire A & B)

Feedback form on questionnaire A or B

Questionnaire ☐ A ☐ B
Name of reviewer:…Farrukh Khan……..
Information Security Role or Designation:……Senior Network Security Specialist.
Other Related Role:…….
Time Spent in Filling the Questionnaire:…1 hr 30 min
……

1. Please comment on the quality of the questions addressed to the Security Practitioners or Governmental Department Leaders:

☐ The questions were long and irrelevant to the subject matter of the Information Security or Management of an e-government department.
☐ The level of questions were too detailed and boring
☐ The language was weak or didn't reflect the right objective of the question
☐ The choices given for each question were not enough to cover all possible answers
☐ All the above
☐ Other comment…The level of questions are fine covering little on e-government and more on information Security Technology
……
……

2. Please select the appropriate selection related to the length of the questions:

☐ The length of the questions were long compared to the objective behind the questionnaire
☐ The time taken to answer the whole questionnaire was long but the questions were so interesting which led me to complete all of them
☐ The length was suitable and appropriate
☐ Can't tell as each question was different from the others
☐ As management, it took too long for me to go through all the questionnaire questions
☐ Other comment…The length of some of the questions were too long due to which a person who is responding on this questionnaire can lose his interest……..

3. ***(For security practitioners only)*** Do you think that this questionnaire contributes to the knowledge body of the Information Security Field:

☐ Yes ☐ No

4. **(For government department it management or department leadership)** Do you feel the questions related to the management of the e-government department were too specific/detailed for management to answer:

☐ Yes ☐ No **N/A**

5. Out of 100% how do you rate the following criteria related to the questions presented in Questionnaire A or B:

   - Coverage of most of the security field domains: _40____%
   - Analytical thinking behind each question___20___%
   - Knowledge contribution in each question__20____%
   - Raising or highlighting issues which are related to the security of e-government__10_%
   - Scientific quality of each question__10____%

6. Please write your comments on any specific question or the whole questionnaire to assist the author to enhance or develop better quality questions:

Questionnaire Type ☐ A ☐ B

Specific Comments on Question Number____
……
……
……
Specific Comments on Question Number____
……
……
……
Specific Comments on Question Number____
……
……
……
Specific Comments on Question Number____
……
……
……

Overall Questionnaire Comments:
……The questionnaire covers the details required for implementation of Information Security technologies, policies, management and monitoring for any organization..……
……
……
……

Do you recommend this questionnaire to go out to the concerned addressees?

☐Yes ☐ No, unless major comments are considered and amendments made to it
☐ No, the questionnaire will not add value to the researcher
because……
…….

Appendix D: Validation confirmation from DEG authority

Validation Forms Filled by Dubai e-Government Authority

A copy from the email of the director of Dubai e-government authority

Dear Sabri,

It was nice talking to you the other day and learn more about your eGovernment Security Model. I have reviewed the model and found it contributing to the assessment of the security level of the government departments; Furthermore, we might consider it for the security architecture in the future.

Wishing you the very best in your academic and professional endeavour.

Best regards.

(See attached file: Validation Forms.xls) Salem Khamis Al-Shair Director, e-Services Dubai eGovernment Tel. +9714 3190333, Fax. +9714 3304333, Dubai, UAE, http://www.Dubai.ae

A copy from the email of the director of Dubai e-government authority

Dear Mr. Azazi,

Kindly find below my comments on the model; Furthermore, please accept this email as an official document since, as you well know, we are driving the paperless movement in Dubai:

Name of the Valuator: Mr. Salem Khamis Al-Shair

Designation: Director, eServices

Role and Responsibility in DEG: Director General.

Brief Background on the Valuator: Mr. Salem Al Shair is the Director of the overall Dubai eGovernment initiative. He has led the entire initiative from strategic, operational and technology perspectives including strategic progress monitoring. He has a strong business and technical background coupled with a deep understanding of public management.

Validation Comments: I validate the model since it covers various aspects of security from a management point of view. It unifies various areas within the security domain and is quite flexible and practical in nature.

What is your overall impression about the new model?

The new model allows one to identify various issues around security and assign various weights depending on strategic importance for an organization.

Do you feel that the model can be used as security architecture for Dubai e-gov?

I feel that the model is applicable for designing the security architecture and in making operational trade-offs for Dubai eGovernment.

What are your general comments on the model?

The model has several perspectives and is parametric and flexible to adapt to different needs of various organizations. It allows one to emphasize certain areas in relation to others, reflecting the security related choices of an organization. It is quite holistic in nature while preserving its practicality.

Any additional suggestions to the model?

The model reflects the high-level security strategy, architecture, operational and implementation concerns. It can potentially be extended to include further technical implementation details which are technology and / or platform specific, if need be. However, usually those issues go beyond the basic security aspects and needs of an organization.

Best regards.

Salem Khamis Al-Shair
Director, eServices

Tel. +971 4 319 0333, Fax. +971 4 330 4333, Dubai, UAE. http://www.dubai.ae

e-Government Security Survey

PART 1	Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
Technology	Access Control	A1	☐	☐	☐	☑	☐
	Intrusion Detection and Prevention	A2	☐	☐	☐	☑	☐
	Anti Virus and Malicious Code	A3	☐	☐	☐	☑	☐
	Authentication and Passwords	A4	☐	☐	☐	☑	☐
	Files and Integrity Check	A5	☐	☐	☐	☑	☐
	Cryptography	A6	☐	☑	☐	☐	☐
	VPN	A7	☐	☐	☐	☑	☐
	Vulnerability Scanning Tools	A8	☐	☑	☐	☐	☐
	Digital Signatures and Certificates	A9	☐	☐	☑	☐	☐
	Biometrics	A10	☐	☑	☐	☐	☐
	Logical Access Control (Firewalls)	A11	☐	☐	☑	☐	☐
	Security Protocol	A12	☐	☐	☑	☐	☐

PART 2	Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
Policies	Password Management	B1	☐	☐	☑	☐	☐
	Log-in Process	B2	☐	☐	☑	☐	☐
	Logs Handling	B3	☐	☐	☑	☐	☐
	Computer Viruses	B4	☐	☐	☑	☐	☐
	Intellectual Property Rights	B5	☐	☐	☑	☐	☐
	Data Privacy	B6	☐	☑	☐	☐	☐
	Privilege Control	B7	☐	☑	☐	☐	☐
	Data Confidentiality	B8	☐	☐	☑	☐	☐
	Data Integrity	B9	☐	☑	☐	☐	☐
	Internet Connectivity	B10	☐	☐	☐	☐	☑
	Administrative Policies	B11	☐	☐	☑	☐	☐
	Encryption Policies	B12	☐	☐	☑	☐	☐
	HR Security Policies	B13	☐	☐	☑	☐	☐
	Third Party Policies	B14	☐	☑	☐	☐	☐
	Physical Security Policies	B15	☐	☐	☐	☑	☐

PART 3	Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
Security Competencies	Security Operation and management	C1	☐	☐	☑	☐	☐
	Security Architecture and development	C2	☐	☐	☑	☐	☐
	Ethical Hacking	C3	☐	☐	☐	☑	☐
	Security Policies and development	C4	☐	☐	☑	☐	☐
	Computer Forensics	C5	☐	☑	☐	☐	☐
	Cryptography	C6	☐	☑	☐	☐	☐
	Security Programming	C7	☐	☐	☑	☐	☐
	Laws and regulation	C8	☐	☐	☑	☐	☐
	Security Implementation and Configuration	C9	☐	☐	☑	☐	☐
	Security Analysis	C10	☐	☐	☑	☐	☐
PART 4	Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
OPS mgmt	Operational Policies and Procedures	D1	☐	☐	☑	☐	☐
	Management Tools	D2	☐	☐	☑	☐	☐
	Correlation and data mining	D3	☐	☑	☐	☐	☐
	Reporting and Response	D4	☐	☐	☑	☐	☐
	Analysis and Human intervention	D5	☐	☐	☑	☐	☐

PART 5	Category		Not Considered (0 %)	Plan or Idea (1 - 49%)	Partially Implemented (50 - 79%)	Semi Implemented (80 - 99%)	Fully Implemented (100%)
Decision	Cost	E1	☐	☑	☐	☐	☐
	Awareness	E2	☐	☑	☐	☐	☐
	Need	E3	☐	☑	☐	☐	☐
	Technologies Availability	E4	☐	☑	☑	☐	☐

Criteria	Description	Validity Rate
Simplicity of the model	The model must be clear to the indented users (government departments or individuals). The layers of the model must be explicit and should make sense to a non security or IT expert	□ High
Applicability	The model must be applicable to any organization which intends to use it for its internal or external communication or information sharing	□ High
Standards Compliance	The model must comply with the security standards in terms of acronyms, references, objectives	□ High
Doable	The model must be doable for the e-government authority and its government affiliates	□ High
Flexible	The model must be flexible and can be implemented in phases	□ High
Open standards	The model must address general technologies, policies, competencies, and operational procedures. It should not be biased to any brand, proprietary solution, or special procedures applicable only to specific vendor or forum.	□ Medium
Renewable and Expandable	the model must be easy to update with the introduction of new trends in the security field and it also can allow merge group of security technologies, policies, procedures, or competencies	□ High

Key of Modified Model

	Category		Category	
Technology	Access Control	A1	Intrusion Detection and Prevention	A2
	Anti Virus and Malicious Code	A3	Authentication and Passwords	A4
	Files and Integrity Check	A5	Cryptography	A6
	VPN	A7	Vulnerability Scanning Tools	A8
	Digital Signatures and Certificates	A9	Biometrics	A10
	Logical Access Control (Firewalls)	A11	Security Protocol	A12
Policies	Password Management	B1	Log-in Process	B2
	Logs Handling	B3	Computer Viruses	B4
	Intellectual Property Rights	B5	Data Privacy	B6
	Privilege Control	B7	Data Confidentiality	B8
	Data Integrity	B9	Internet Connectivity	B10
	Administrative Policies	B11	Encryption Policies	B12
	HR Security Policies	B13	Third Party Policies	B14
	Physical Security Policies	B15	Operation Security Policies	B16
Competencies	Security Operation and management	C1	Security Architecture and development	C2
	Ethical Hacking	C3	Security Policies and development	C4
	Computer Forensics	C5	Cryptography	C6
	Security Programming	C7	Laws and regulation	C8
	Security Implementation and Configuration	C9	Security Analysis	C10
OPS mgmt	Operational Policies and Procedures	D1	Management Tools	D2
	Correlation and data mining	D3	Reporting and Response	D4
	Analysis and Human intervention			D5
Decisi	Cost	E1	Awareness	E2
	Need	E3	Technologies Availability	E4

Modified Model

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12				
63%	44%	50%	56%	63%	50%	50%	44%	56%	19%	63%	44%				
B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
56%	56%	56%	56%	44%	50%	56%	56%	63%	50%	56%	50%	38%	44%	56%	63%
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10						
53%	69%	56%	50%	50%	44%	38%	63%	63%	38%						
D1	D2	D3	D4	D5											
56%	56%	56%	63%	44%											
E1	E2	E3	E4												
50%	44%	63%	69%												