AN INVESTIGATION OF INFORMATION SECURITY POLICIES AND PRACTICES IN MAURITIUS

---

by

OUMESHSINGH SOOKDAWOOR

submitted in fulfilment of the requirements for

the degree of

MASTER OF SCIENCE

in the subject

INFORMATION SYSTEMS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF E SMITH

CO-SUPERVISOR: PROF L M VENTER

NOVEMBER 2005

DECLARATION OF OWN WORK

Student Number: 3204-192-6

"I declare that **AN INVESTIGATION OF INFORMATION SECURITY POLICIES AND PRACTICES IN MAURITIUS** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references".

_____ _____

SIGNATURE DATE

(Mr O SOOKDAWOOR)

ABSTRACT OF THE DISSERTATION

Information Security:

An Investigation of Information Security Policies and Practices in Mauritius

by

Oumeshsingh Sookdawoor

MSc. Information Systems

University of South Africa, 2005

With the advent of globalisation and ever changing technologies, the need for increased attention to information security is becoming more and more vital. Organisations are facing all sorts of risks and threats these days. It therefore becomes important for all business stakeholders to take the appropriate proactive measures in securing their assets for business survival and growth. Information is today regarded as one of the most valuable assets of an organisation. Without a proper information security framework, policies, procedures and practices, the existence of an organisation is threatened in this world of fierce competition.

Information security policies stand as one of the key enablers to safeguarding an organisation from risks and threats. However, writing a set of information security policies and procedures is not enough. If one really aims to have an effective security framework in place, there is a need to develop and implement information security policies that adhere to established standards such as BS 7799 and the like. Furthermore, one should ensure that all stakeholders comply with established standards, policies and best practices systematically to reap full benefits of security measures.

These challenges are not only being faced in the international arena but also in countries like Mauritius. International researches have shown that information security policy is still a problematic area when it comes to its implementation and compliance.

Findings have shown that several major developed countries are still facing difficulties in this area.

There was a general perception that conditions in Mauritius were similar. With the local government's objective to turn Mauritius into a "cyber-island" that could act as an Information Communication & Technology (ICT) hub for the region, there was a need to ensure the adoption and application of best practices specially in areas of information security.

This dissertation therefore aims at conducting a research project in Mauritius and assessing whether large Mauritian private companies, that are heavily dependent on IT, have proper and reliable security policies in place which comply with international norms and standards such as British Standard Organisation (BSO) 7799/ ISO 17799/ ISO 27001. The study will help assess the state of, and risks associated with, present implementation of information security policies and practices in the local context. Similarities and differences between the local security practices and international ones have also been measured and compared to identify any specific characteristics in local information security practices.

The findings of the study will help to enlighten the security community, local management and stakeholders, on the realities facing corporations in the area of information security policies and practices in Mauritius. Appropriate recommendations have been formulated in light of the findings to improve the present state of information security issues while contributing to the development of the security community.

LIST OF KEYWORDS

Information security policy, Information security practices, Security standards, Compliance, Information security risk, Procedures, Information security framework, Adherence to established standards, Information Communication & Technology.

This research is dedicated to my late father, Gyan Heerahsingh Sookdawoor

&

my living and caring mother Sateecoomaree Sookdawoor

for their lifetime blessings.

ACKNOWLEDGEMENTS

This research has been possible thanks to the contribution and help of the following parties:

- The Registrar of UNISA – for approving the research proposal;
- The promoters, Prof. E.SMITH & Prof. L.M.VENTER - for their valuable supervision and guidance over the whole research project;
- The referenced authors and gurus of the security community – for their contribution to the literature survey of this project through their books, publications, white papers, proceedings and websites;
- The management and security personnel of the surveyed companies – for their kind participation and openness in responding to the survey;
- Friends and colleagues – for the support and assistance during the field research work;
- The software writers of Analyse-It & Raosoft – for extending their statistical tools online to assist such researches;
- My wife, children and family – for their moral support, collaboration and understanding during the research period.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

1. *Asia Pacific (APAC)*
2. *Asymmetrical Digital Subscriber Line (ADSL)*
3. *Asynchronous Transfer Mode (ATM)*
4. *British Standard (BS)*
5. *British Standard Organisation (BSO)*
6. *British Standards Institution (BSI)*
7. *Business Continuity Planning (BCP)*
8. *Business Process Outsourcing (BPO)*
9. *Canadian Trusted Computer Product Evaluation Criteria (CRCPEC)*
10. *Central Investigation Division (CID)*
11. *Certified Information System Security Professional (CISSP)*
12. *Chief Executive Officers (CEOs)*
13. *Chief Information Security Officer (CISO)*
14. *Chief Security Officers (CSOs)*
15. *Computer Sciences Corporation (CSC)*
16. *Consultative, Objective and Bi-functional Risk Analysis (COBRA)*
17. *Control Objectives for Information and related Technology (COBIT)*
18. *Critical Success Factors (CSFs)*
19. *Europe, Middle East and Africa (EMEA)*
20. *European Commission (EC)*
21. *Federal Information Security Management Act (FISMA)*
22. *Generally Accepted Information Security Principles (GAISP)*
23. *Generally Accepted Information Systems Security Practices (GASSP)*
24. *Generally Accepted System Security Principles (GASSP)*
25. *Gross Domestic Product (GDP)*
26. *IEC (International Electrotechnical Commission)*
27. *Information Communication Technology (ICT)*
28. *Information Communication Technology Authority (ICTA)*
29. *Information Security (IS)*
30. *Information Security Management System (ISMS)*
31. *Information Technology (IT)*
32. *Information Technology Security Evaluation Criteria (ITSEC)*
33. *Institute of Electrical and Electronics Engineers (IEEE)*
34. *International Standards Organisation (ISO)*
35. *Key Performance Indicators (KPIs)*
36. *Latin America and Caribbean (LACRO)*
37. *Mauritius Commercial Bank Ltd (MCB)*
38. *Mauritius Qualifications Authority (MQA)*

LIST OF ABBREVIATIONS (Cont.)

39. *Mutual Recognition Arrangement (MRA)*
40. *National Institute of Standards and Technology (NIST)*
41. *Organization for Economic Cooperation and Development (OECD)*
42. *Plan-Do-Check-Act" (PDCA)*
43. *Rivest, Shamir & Adleman (RSA)*
44. *Security Online Support (SOS)*
45. *Statement of Applicability (SoA)*
46. *Targets of Evaluation (TOE)*
47. *Total Quality Management (TQM)*
48. *Trusted Computer System Evaluation Criteria (TCSEC)*
49. *United Kingdom (UK)*
50. *United States (US)*

Chapter 1:

Introduction

1 DISSERTATION INTRODUCTION

1.1 Introduction

Mauritian organisations have invested significantly in their overall Information Technology (IT) operations. Security has always been proclaimed to be their prime concern, but yet one can see the absence of a well formulated IT Security Policy in quite a large scale.

It can also be noted that, while in some cases such policies are inexistent, in others their defined IT Security Policies are simply not being enforced as they should.

Most of the time, it goes beyond just setting up an IT Security Policy and enforcing it. Another key attribute to its success is the degree of conformance to established and proven norms and standards.

There is a tendency to allocate information security issues a low priority in the implementation and running of most information systems at the expense of other business requirements despite stakeholders claimed differently. Technical solutions by themselves are limited in their effectiveness and require management support. According to quality management, it is important to audit the success of any actions taken and whenever necessary, to identify appropriate corrective action. Management of information security is therefore not static but a continuous process which necessitates commitment from top management.

1.2 Background to the study

Whilst information security policies provide a solid foundation for the development and implementation of secure practices within an organization, the policies themselves are, too often, neither instructional nor descriptive. They simply represent the rules which must be adhered to. Compliance with them, however, requires an understanding of not only the individual policies, but also of the circumstances in which such compliance is expected in the staff's day-to-day activities. Knowing the policies is only one half of the equation; staffs need to

know how they should comply with a procedural perspective. This has to some extent made the implementation and enforcement of proper policies in a systematic manner more difficult, especially when it formalises certain practices.

With this objective in mind, the Security Online Support (SOS) Information Security Policies have been drawn from the extensive experience of senior Information Security Consultants who have delivered business systems and security sensitive projects across the world (Information Security Policy World, 2001). Based upon the foundation of the International Organisation for Standardization (ISO) 17799, they are both extensive and up to date, and may be inspired from and adopted by organizations to form the basis of an information security conscious culture.

Furthermore, the literature describes that according to industry analysts and trade journals, the problem is neither a lack of information for security analysts nor just an increasing level of data, but an increasing rate of change in the data (SAS, 2002). From all this information, Chief Security Officers (CSOs) and their experts have worked hand in hand to assess the state of information security by determining the threats and risks associated with it. This has in turn helped to clarify several managerial issues such as:

- **Business continuity and disaster planning** – An organisation's survival depends on several key components such as information assets, critical business processes and supporting systems. Information is probably one of the most important and valuable resources in an organisation necessitating optimal protection. Therefore there is a need to assess the value of information by measuring it in terms of availability of service, confidentiality of data, integrity of data, and processes. The absence of critical data or the loss of confidential information can affect the organizational existence. It is prerequisite that management takes proactive measures to ensure business continuity.
- **Routine vulnerability assessments** – There is a need to identify, assess and correct any vulnerability that may affect an organisation. Thus identifying known vulnerabilities and tracking them until they are

mitigated is crucial for securing the organisation and society at large. Moreover, sustainable efforts should be maintained to ensure such risks are managed at all times.

- **Operational procedures** – An organisation cannot fully mitigate business risks if there is an absence of proper operational procedures. Formal escalation procedures and incident response procedures are some of the examples. These form part of the basic underlying framework of information security.
- **Remedial procedures** – An organisation's procedure framework should also incorporate remedial procedures on how to release updates and patches, fixing compliance issues and addressing configuration matters. Furthermore, it is fundamental to develop a reporting process to establish effectiveness of the remedial procedures.
- **Measuring the performance of security program** – Management should also establish an appropriate measurement framework to assess the viability of the security programs. This should cover compliance with policies, adherence to standard and best practices, threat management, vulnerability identification and tracking. This will provide an overview of the overall effectiveness and efficiency of mitigation measures and security programs in place.

Clearly, the biggest challenge for CSOs is to bring together all the data from various sources and provide an integral view of the state of information security issues. Without this overall and consolidated view and methods to communicate the security status to senior management, security teams and employees, it is absolutely hard for the CSOs to set up a security-conscious culture within the organisation in which one can implement an effective enterprise-wide security policy for safeguarding the business as a whole.

In order to build an effective enterprise-wide security policy, CSOs and their teams have to embrace the challenge of:

(a) identifying the core assets of the business and implementing appropriate preventive and corrective measures for their protection;

(b) devising and implementing an integrated approach to threat management;
(c) Responding promptly to business risks and threats;
(d) Communicating the security policies and procedures effectively to the rest of the organization
(e) and continually monitoring , assessing and acting upon them.

For instance the implementation of the famous Deming Wheel with its "Plan-Do-Check-Act" (PDCA) cycle can support this process (Juran, 1974). The basic PDCA cycle was developed by Shewhart and then modified by Deming. This is a continuous chart widely used in Japan to describe the cycle of control. Proper control starts with the 'Planning', 'Do' what is planned, 'Check' studies the results, and then applies any necessary corrective action. PDCA is considered ubiquitous within the Total Quality Management (TQM) framework today.

1.3 Research aims

The aim of this study is to identify whether Mauritian companies, especially those which are heavily dependent on IT, have proper and reliable security policies in place which comply with international norms and standards such as British Standard Organisation (BSO) 7799, ISO 17799, ISO 27001 etc.

For those which are not conforming to established norms, an analysis will be performed to respond to questions like:

- What are the implications?
- What are the business risks and exposures?
- What could be the impact?(s)
- What is the extent of their deviation from these norms?

For those which do conform to international norms, a coherent analysis will be made under the following key areas:

- How reliable is their implementation and complies with norms and standards (Ex ISO 17799, etc)?
- What is their general risk exposure?

- What improvement can still be made over the long run?

While there is a general unsubstantiated feeling that there is no adherence to standardized security policies in Mauritius, the main aim of this research is to investigate and report whether this is indeed the case.

Furthermore, the dissertation will aim at assessing whether there is a correlation between the local information security practitioners' experience and the presence of security policies at their workplaces. Besides, the study will also establish whether there exists any association between the industry and security practices in Mauritius as well as test certain hypotheses around this topic.

Research will be conducted on conglomerates and organisations of the Mauritian economy which are highly dependent on IT with a view to coming up with an original and unique study on these Mauritian organizations with respect to the formulation, implementation and adherence to standard IT Security Policies.

This could be used as a benchmark as well as guidelines for any upcoming security policy implementation in this developing "cyber island".

1.4 Limitations of the study

The key limitations of this study are:

(a) The scope of the study is limited to the Mauritian context;

(b) The study focuses on the key area of compliance with security standards whereby other areas of security are yet to be studied further;

(c) The study attempts to identify any problems and risks encountered by local private firms. The survey will be targeted to this particular group exclusively.

1.5 Research Form & Approach

The form chosen will be "Discovery & Interpretation" as conceptualized by Leedy (Leedy, 1993). The research will primarily focus on discovering the

current practices within Mauritian organizations with respect to IT Security Policy standards and subsequently interpret the results obtained from an in-depth analysis. The dissertation will be conducted in 3 key phases:

Part 1: Comprehensive Literature Survey

(a) A comprehensive literature survey of current international norms and standards with respect to security management and best practices will be undertaken. This survey will include most of the well-known standards such as (BS 7799, ISO 17799, ISO 27001, etc).

(b) An in-depth description of the theory underlying these practices will then be attempted. The survey will also include an analysis of these practices, leading to a critical analysis of each, and identifying points of overlap and difference which could be considered as best for the Mauritian situation.

Part 2: Field Survey & Research

(a) A survey of current practices will be carried out using questionnaire on identified Mauritian companies which are heavily dependent on IT. This will include a number of companies, ranging from small to large in the Mauritian context. The survey will be based on a questionnaire, which will be compiled according to acceptable scientific practices.

Part 3: Interpretation of findings & Recommendations

(a) The feedback received will then be analyzed statistically, and scientific conclusions will be drawn from it. There is a strong possibility of recording inconsistencies in the theoretical findings on best practices of Phase 1 which will then be critically analyzed and the potential reasons behind them stated.

(b) In conclusion, the dissertation will come up with:

1. An overview of the relationship between setting up standard practices and risk exposures to the corporations.
2. An assessment of the uniqueness of the Mauritian situation with respect to the global trend.

3. The general unsubstantiated feeling that there is no adherence to standard security policies in Mauritius will be assessed.
4. An assessment of whether there is an association between local industries and security practices.
5. A conclusion on comparisons with similar studies of other countries.

1.6 Summary

The aim of this chapter was to set the scene on the objectives of the research theme, its scope and limitations, and the research approach which will guide this dissertation. Given the absence of such a research in Mauritius, specifically in the area proposed, it motivates one to conduct this research and come up with findings that will contribute to the development, implementation and adherence to standard IT Security Policies in Mauritius. The subsequent chapter will set the scene on international security practices and standards as conceived by the security gurus and renowned institutions.

Chapter 2:

Background Study

2 INFORMATION SECURITY POLICIES, STANDARDS & PRACTICES

2.1 Introduction

The purpose of an information security program is to protect the valuable information resources of an enterprise (Peltier, 2001). Through the selection and application of appropriate policies, standards and procedures, an overall security program helps the enterprise meet its business objectives or mission charter.

Information security policies are high level plans that describe the goals of the procedures (Barman, 2002). They provide the blueprints for an overall security program. Furthermore, security policies are not guidelines or standards, nor are they procedures or controls. Policies describe security in general terms, not specific (Barman, 2002). Questions arise when people are told that procedures are not part of policies. Procedures are implementation details. A policy is a statement of the goals to be achieved by procedures. General terms are used to describe the security policies so that the policy does not get in the way of the implementation. Although policies do not discuss how they have to be implemented, they indicate what is being protected and what restrictions should be put on those controls.

Furthermore, it is often found that organisations that have sets of security policies and procedures do not comply with industry standards or best practices. The end result is that the organisations are still exposed to risks which may easily compromise their survival. A security policy which is implemented in an adhoc, non systematic norm and which is not aligned on known and established security standards, is simply a defect in the whole security enforcement process.

Because security is sometimes viewed as thwarting business objectives, it is necessary to ensure that effective, well formulated policies, standards and procedures are implemented. This goes even further; not only one has to write them, but also ensure they are up to standards and best practices while being adhered to by all concerned parties.

Whereas information security used to be an arcane technical topic, even Chief Executive Officers (CEOs) know about it today due to the importance of electronic information in their businesses. Actually all business executives now need to understand Internet-based threats and countermeasures and continually fund security work to protect their businesses; hence a stronger need for well devised and standardized approaches to information security implementation.

This chapter therefore aims to present the underlying concepts behind information security, security policies and procedures, its consideration from a business perspective, key developments in the area of information security and finally present the most prominent and established security standards.

2.2 Five Pillars of Information Security

Rivest, Shamir & Adleman (RSA) Security Inc., a prominent long-time network security firm, confirmed that there are five pillars that make up today's security techniques (RSA Security, 2005). These are:

1. Identification & Authentication
2. Authorisation
3. Confidentiality
4. Integrity
5. Non-repudiation

These have also been defined by ISO 7498-2 standard as produced by International Standards Organisation (ISO, 1999). Several authors like Krause & Tipton, Steiner and Pfleeger covered these issues under their security articles and books (Krause & Tipton, 1999; Pfleeger, 2000).

Herewith an overview of the 5 pillars of information security:

2.2.1 Identification & Authentication

Identification is the process of issuing and verifying access privileges. RSA explains this by citing an example using a driver's licence. First, one has to show proof of identity to get one's licence. Once this licence is obtained, it becomes ones's proof of identity but it also states one's

driving privileges, that is, allowed to drive car or truck. Therefore, identification is like being certified to be able to do certain activities.

Authentication means verifying someone's authenticity, that is, they are who they say they are. According to RSA, people can authenticate themselves to a system in three basic ways namely:

- By something they know, such as a password;
- By something they have, such as use of code or token or card and
- Something they are, such as fingerprint, retina scan etc.

Each of these methods has its respective strengths and weaknesses and RSA recommends choosing two of the three, which is called two-factor authentication.

2.2.2 Authorization

Authorization refers to the privileges and permissions granted to a person by a designated responsible party to access or use a system, information, or program. These privileges are often granted on a need-to-know basis. The person holding such authorization is known as an authorized person. He/she has to ensure that such privileges and permissions are not disclosed to any other individual.

2.2.3 Confidentiality

Confidentiality means keeping information from being seen (privacy). It refers to how data is being collected, used and maintained within an organisation. It includes the protection of data from passive attacks and requires that the information is accessible by authorised persons only.

2.2.4 Integrity

This means keeping information from being changed in an unauthorised way. It ensures that data is a proper representation of information, accurate, and in an unimpaired condition. Measures should be taken to protect data from being exposed to accidental or intentional alteration or destruction.

Both confidentiality and integrity are especially important when information travels through the Internet because it is a public space where interception is more possible. Encryption is a means to counter such threats.

2.2.5 Non-Repudiation

It means that neither party in a sales transaction or communication of sensitive information can later deny that the transaction or information exchange took place. Non-repudiation services can prove that someone was the actual sender and the other, the receiver. It can also confirm that no imposter was involved on either side.

In order to ensure that information is protected and secured during its storage, transmission and usage, these services are imperatively needed (Schneier, 2000).

2.3 Information Security from a business perspective

Nowadays top executives are primarily concerned with business objectives and the effectiveness of the organisation to reach them. Information technology (IT) is a means to an end, and information security (IS) is frequently regarded as an attribute of systems and data rather that a business issue. Quite frequently, the risk and the solutions are seen as part of the IT universe, while business leaders want to concentrate on product development, sales and revenue, and customer care. To change this mindset, the Chief Information Security Officer (CISO) has to inform, educate and influence his or her business counterparts.

To be effective, the IS governance reporting must be closely aligned to the organisation's information security management framework. International Standards Organisation (ISO) 17799, information security frameworks and programs are good examples of management frameworks that focus on the controls believed to lead to stronger security posture. Such frameworks must aim at implementing standard security properly.

Most organisations have an information security policy; but having it written and approved by the Chief Executive Officer (CEO) is of little value if the

organisation does not live by it. The real effort therefore lies in communicating the security objectives set in the policy, the organisational accountabilities for implementation, and the standards, procedures, and guidelines available to support the policy. The metrics data reports on the awareness and training programs are needed for an effective implementation of the policy. Intranet Web sites dedicated to information security can play a key role in the awareness and education program by providing targeted information for both security specialists and general IT users. Statistics on visits to the security Web site provide valuable feedback on the reach and popularity of the awareness program.

It was found that the beginnings of this process when the National Institute of Standards and Technology (NIST) began publishing such documents as *An Introduction to Computer Security: The NIST Handbook* (NIST Special Publication 800-12).

On the same wavelength, ISO has published the recently adopted *Information Technology – Code of Practice for Information Security Management* (ISO 17799) and its parent British Standard (BS 7799) to reinforce engagement in this area of activity. ISO 27001 was then published in late 2005 to replace the original standard BS 7799-2. ISO 27001 defines the Information Security Management System (ISMS) thereby creating a framework of the design, implementation, management and maintenance of information systems processes throughout an organisation.

Furthermore, Generally Accepted Information Systems Security Practices (GASSP) has stepped into the void and provided all security professionals with a map of where to take the information security program.

Good security must be measured in how well the assets of the enterprise are protected while the mission and business objectives are met. Thus it is of paramount importance that information security practitioners develop the right set of policies and procedures which are according to norms and are implemented in such a way that adherence to them can be measured and assessed.

2.4 Information Protection

Information protection is a means to an end and not the end in itself (Peltier, 2001). In most businesses, management usually views an effective information protection program as secondary to the need to make a profit. Similarly in the public sector, information protection is secondary to the services the agency provides. The importance of information protection therefore varies from industry to industry and company to company. Security professionals must not lose sight of these tenets.

Moreover, computer systems and the information processed on them are often considered critical assets that support the mission of an organisation. Protecting them can be as important as protecting other organisation resources, such as financial resources, physical assets and employees. The cost and benefits of information protection should be carefully examined in both monetary and non monetary terms to ensure that the cost of controls does not exceed the expected benefits. Information protection controls should be appropriate and proportionate. An information protection program is more than establishing controls for the computer held data. It should address information threats in their forms.

2.5 IT Security Standards

2.5.1 BSI & ISO

2.5.1.1 The History

Information security standards have been attracting the attention of most information security practitioners for long. Since a number of decades, institutions have been working towards establishing high quality standards. In particular, the British Standards Institution (BSI) has carried out studies for the purpose of establishing effective and high-quality standards for this industry (BSI, 2004). Since the beginning of its development in the 1990s, BS 7799 has been worked out to respond to industry, government and business requests for the creation of a common information security structure. No doubt that significant effort was put into the development of such a standard.

Furthermore, in 1993, the United States (US), Canada, the United Kingdom (UK), France, The Netherlands, and Germany pooled their efforts and began a joint activity to align their separate criteria on a single set of IT security criteria that could be widely used. This activity was named the Common Criteria Project.

In 1995, the BS 7799 standard was officially adopted by the UK government.

Subsequently, in May 1999, a second version of the BS 7799 standard was published which incorporated significant improvements on the earlier version. This was considered as a major version which, in some way or the other, attracted the interest of ISO which then participated actively in the process of formalizing this standard.

It was only in December 2000 that ISO took over the first part of BS 7799 and re-branded the work as ISO 17799. In September 2002, the second part of the BS 7799 standard was revised such that it is consistent with other management standards such as ISO 9001:2000 and ISO 14001:1996 as well as with the principles of the Organization for Economic Cooperation and Development (OECD). This was a significant move towards getting this standard aligned on international norms and gaining extended acceptance in the industry.

There is no doubt that the standard will only remain effective if it is continually reviewed and enhanced. As such, consultations are taking place at the international level to keep BS 7799 / ISO 17799 abreast of latest developments while proactively devising measures to address emerging risks and threats.

2.5.1.2 BS 7799 - ISO 17799/ISO 25001 Security Standards

Information is invaluable and certainly considered as a very important asset in any organisation. The protection of such information is vital for the survival of any organisation. Risks that threaten the security of such assets have to be mitigated and controlled at all times.

Information security is a combination of preventive, detective and recovery measures (GASSP, 1995). To put appropriate information security measures in place, there is a strong need to adopt the best practices and use them as the benchmark for implementation.

As such, when it comes to implementing codes of practice for information security management, the best point of reference is BS 7799 / ISO 17799, an internationally recognized standard in this field (ISO, 2004).

The year 2005 has marked another major milestone in the development of information security standards with the publication of the most recent security standards, ISO 27001 (ISO 27001, 2005). The latter has replaced ISO 17799 which was the earlier version.

Basically a history of the development of the standard is given below:

(a) ISO/IEC 17799 (Part 1)

ISO/IEC 17799 is a code of practice for information security management. It acts as a guide containing advice and recommendations to supplement the initiation and implementation and maintenance of information security projects in an organisation. The aim is to ensure the security of a company's information according to ten fields of application which form the underlying framework of security management.

In late 2000, the ISO published ISO/IEC (International Electrotechnical Commission) 17799:2000, Information

Technology — Code of Practice for Information Security Management. The stated objective of ISO/IEC 17799:2000 is to enable business enterprises to mitigate those IT threats that arise from physical disaster, fraud, and industrial espionage.

The international standard ISO/IEC 17799 was developed by the British Standards Institution (BSI) as BS 7799. It was adopted through a special "fast track procedure" by the JTC 1 (Joint ISO/IEC Technical Committee), concurrently with its approval by the national member institutes of ISO and the IEC.

The goal of BS 7799 / ISO 17799, as specified by ISO, is "*to provide a common base for developing organisation security standards and effective security management practice and to provide confidence in inter-organisational dealings*". The key areas covered by the BS 7799 / ISO 17799 standards are depicted in Figure 2-1 below (British European Standards, 2005).

Figure 2-1: Areas covered by the BS 7799 / ISO 17799 standards

Consider Figure 2-1 above which depicts a structure for the ten domains as specified by the standard. Each domain deals with a separate topic built around administrative, technical, physical measures and driven in a top down structure, that is, its impact is felt from the management level all the way to the operational level. The implementation of the standard is across management levels of an organisation.

The 10 sections of the ISO 17799 Standard (ISO/IEC 17799) are presented in the form of guidelines and recommendations that were assembled following consultations with large organisations. The 36 security objectives and 127 security controls contained in ISO/IEC 17799 are divided among ten domains. The following is a brief overview of each of these domains:

1. **Security Policy –** It provides guidelines and management advice for improving information security. It is a formalization of the information security practices as established and approved by the top management for implementation and compliance by all stakeholders in order to protect organizational assets.
2. **Organizational Security** – It is basically the management structure for security including appointment of qualified personnel, definition and assignment of roles and responsibilities as well as the establishment of process flows and controls for security management. In other words, it facilitates information security management within the organization.
3. **Asset Classification and Control** – It facilitates the process of carrying out an inventory and the assessment of organization's information assets including its infrastructure such that the assets are secured, managed and controlled effectively.
4. **Personnel Security** – It minimizes the risks of human error, theft, fraud or the abusive use of equipment by setting security expectations in job responsibilities. Screening of new personnel for criminal records, setting up of confidentiality agreements and

reporting of incidents are key elements covered under this category.

5. **Physical and Environmental Security** – This includes measures to prevent the violation, deterioration or disruption of industrial facilities and data. Policies are established for the protection of infrastructure, plant and personnel.
6. **Communications and Operations Management** – This ensures that adequate and reliable operation of information processing devices prevails within the organisation using preventive measures of various kinds.
7. **Access Control** – This forms the underlying structure for securing information using access controls to network, systems and application resources.
8. **Systems Development and Maintenance** – It ensures that security is incorporated into information systems and that security forms an integral part of any network and systems expansion. It also ensures that systems can be maintained over time.
9. **Business Continuity Management** – This focuses on the planning activities for disaster recovery. It aims to minimize the impact of business interruptions and protect the company's essential processes from failure and major disasters.
10. **Compliance** – Complying with regulatory framework is a directive of this section. Avoiding any breach of criminal or civil law, of statutory or contractual requirements, and of security requirements are key elements of this section.

(b) BS 7799 (Part 2)

In the year 2002, a revision of BS 7799 was published. It was earlier referenced as BS 7799:2002 (hereafter referred to as BS 7799-2). The aim of BS 7799-2 was to harmonise it with other established management standards for consistency purposes. It basically sets the information security management

specifications and recommendations for establishing an effective Information Security Management System (ISMS).

It was also meant to ensure effective information security management is established and maintained through continual improvement process.
It comprised the ten domains and 127 controls of the ISO 17799 standard. This reference applies to the development, implementation and maintenance stages of an information security system. Organizations applying for certification are evaluated according to this document. An organization that bases its ISMS on the provisions in BS 7799 can obtain certification from an accredited body. The organization thereby demonstrates to its partners that its system both complies with the standard and answers the need for security measures as determined by its own requirements.

It is important to understand that an organization that obtains certification is considered ISO 17799 compliant and BS 7799-2 certified. BS 7799-2 is already widely used in many countries as a reference document for information security management certification. These countries include England, Australia, Norway, Brazil and Japan.

One way of looking at the difference between ISO 17799 and BS 7799-2 is that:

- ISO 17799 basically provides a generic implementation framework.
- BS 7799-2 is a normative standard which stresses what an organisation shall do to be eligible and worthy of being certified under the standard. These criteria are used by certification auditor to measure the degree of compliance with the standards.

(b) ISO 27001

The version of BS 7799-2 was revised in 2005. ISO 27001 was published in late 2005 to replace the original standard BS 7799-2. ISO 27001 defines the information management system itself. In other words, it defines the ISMS thereby creating a framework of the design, implementation, management and maintenance of information systems processes throughout an organisation (ISO 27001, 2005).

The new standard has re-organised and harmonised the earlier version of the standard so as to be compatible with other management standards such as ISO 9000 and ISO 14000 series.

The ISMS contains the following chapters:

1. Introduction
2. Scope
3. Normative References
4. Terms and Definitions
5. Information Security Management System
6. Management Responsibility
7. Management review of the ISMS
8. ISMS improvement

The 27001 standard defines a 6-stage process namely:

1. Define an information security policy
2. Define scope of the information security management system
3. Perform a security risk assessment
4. Manage the identified risk
5. Select controls to be implemented and applied
6. Prepare a Statement of Applicability (SoA)

The standard also lays significant emphasis on the use of Plan-Do-Check-Act (PDCA) cycle as the underlying process as conceptualized by Deming. The four stages are:

- Plan – Establish the ISMS
- Do – Implement and operate the ISMS
- Check – Monitor and review the ISMS
- Act – Maintain and improve the ISMS

Eventually, ISO 27001 will be one of a number of security standards published are part of the ISO 27000 series. ISO 27002 and ISO 27004 are likely to be produced in the next few years

2.5.1.3 Benefits of the BS 7799, ISO 17799 and ISO 27001 standards

Complying with the standard definitely brings along certain benefits to the organisation which one should consider namely:

At the organizational level

Certification demonstrates a level of commitment of the organisation towards security of its assets and information. By complying with such standards, the organisation gives a strong signal to all stakeholders that efforts are being put up in information security at all the levels to secure their respective stakes.

At the legal level

Organisations have the duty to comply with prevailing regulatory and legal framework. The effort being put up in certifying for BS 7799 for instance demonstrates to authorities that the organisation is fulfilling its duty by observing and complying with applicable laws.

At the operating level

The implementation of standard such as ISO 27001 elevates the operating conditions of an organisation. It allows organisations to understand the operations from various perspectives including gaining knowledge of information systems, their weaknesses and

how to protect them. This in turn helps to better manage the risks and possible threats for the survival of the business.

At the commercial level

Nowadays organisations are aiming to differentiate from their respective competitors. This has in fact become a critical success factor for business growth. Organisations are seeing in the certification of BS 7799 and ISO 27001 as one of the ways to differentiate from others as this reassures the market, partners and clients as to the capabilities of the organisation. It demonstrates the organisation's standards and working practices. It in turn raises confidence and trust in organisation and its capabilities thereby favouring business development further. It is already being seen that organizations are starting to require ISO 27001 compliance on the international scene.

At the financial level

By having security standards defined across the organisation through the 10 areas of BS 7799/ISO 17799:2005 standard, it culminates into reducing risks and associated costs which are related to security breaches and losses. The compliance with such standards thus indirectly helps in reducing the financial cost.

At the human level

Finally employees grow in knowledge while inculcating best practices and disciplines in the area of information security. They become more aware of security problems and threats as well as their respective roles and duties within the organization. In the long run, this develops a security-conscious culture and mindset within the organisation.

Over 80 000 firms around the world are BS 7799 / ISO 17799 compliant, including:

- Fujitsu Limited
- KPMG
- Marconi Secure Systems
- Sony Bank
- Toshiba IS Corporate

2.5.2 Common Criteria

2.5.2.1 History of Common Criteria

Information security was a major concern for military and financial services organisations until recently. However, the September 11 catastrophe radically changed the view on information security. Information security is becoming more and more critical to many organisations. At the same time, the need for a common information security standard became more and more evident. Security may mean different things to different organisations. Any subjective view of security will only be harsh to the overall process. The need for common agreement is clear and this is what Common Criteria is meant to be, a global security standard (NIST, 2005).

Common Criteria ensures common mechanism for evaluating security of technology products and systems. It provides a yardstick which can help to gauge the security level of products. But if one does a retrospective of the past events, one can easily come to know how Common Criteria found its way.

In the United States, the Common Criteria has its roots in the Trusted Computer System Evaluation Criteria (TCSEC) in 1985 but was found that it was not adapting to new computing paradigms in the early 1990's, given that it was not viable for client/server computing.

In Europe, the Information Technology Security Evaluation Criteria (ITSEC) was under development in 1990 and was

published in 1991 by the European Commission (EC) following a joint effort of countries like France, Germany, the Netherlands and the United Kingdom.

The Canadian government was creating the Canadian Trusted Computer Product Evaluation Criteria (CRCPEC) alongside which was nothing but a composite of both ITSEC and TCSEC.

It was obvious that with so many approaches, there was a need to get to a consensus and create a common approach so as to avoid disparity and confusion among people. This is where ISO took the initiative to develop a new set of criteria for general and international use that is now referred to as Common Criteria (ISO 15408:1999). The objective was to unite the diverse international standards into a common methodology. Organisations that joined forces on the international arena to contribute to Common Criteria were:

- NIST (United States)
- NSA (United States)
- SCSSI (France)
- NLNCSA (the Netherlands)
- CSE (Canada)
- CESG (United Kingdom)

Common Criteria got international recognition via the signing of a Mutual Recognition Arrangement (MRA) between the various countries. The idea behind MRA was to enable products having Common Criteria certification to be used in different jurisdictions without the need to be re-evaluated and recertified each time.
This implies that products which have been accepted by one MRA member nation can be accepted in other member states.

2.5.2.2 Key sections of Common Criteria

Security is a process, not a product (Schneier, 2000). This is rightly supported by Common Criteria which defines a number of security processes and functional requirements implemented as "classes" in Common Criteria terminology. Common Criteria is composed of 11 classes namely:

- Audit
- Cryptographic Support
- Communications
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the Targets of Evaluation (TOE) Security Functions
- Resource Utilization
- TOE Access
- Trusted Path/Channels

These form part of the 3 main sections of the Common Criteria where:

Part 1 defines the general concepts and principles of information technology security evaluation and presents a general model of evaluation;

Part 2 defines the specific security functional requirements and details of criterion for expressing the security functional requirements for TOE;

Part 3 details the security assurance requirements and set of assurance components as a standard way of expressing the assurance requirements of TOE.

2.5.3 COBRA

2.5.3.1 Overview

COBRA which stands for "Consultative, Objective and Bi-functional Risk Analysis", comprises a series of risk analysis,

consultative and security review tools (C & A SYSTEM SECURITY LTD, 2002). Security, in any system, should be commensurate with its risks. However, the process to determine which security controls are appropriate and cost effective is quite often a complex, and sometimes, a subjective matter. Hence there is a strong need to have proper processes and methodology to undertake such activities. One of the prime functions of security risk analysis is to put this process into a more objective basis.

COBRA tools were developed largely in recognition of the changing nature of IT and security. Businesses are becoming increasingly demanding in these areas because the risk exposure has somewhat risen in the recent years.

The acceptance that IT security was a business issue grew over the years. It was, and is, becoming largely expected that security reviews should be business related, with cost justified solutions and recommendations (C&A Systems Security Ltd, 2002).

Conventional methods and tools are not likely to address the new demands of businesses completely. COBRA, and its default methodology, evolved very much to tackle these issues properly. This was developed in full co-operation with one of the world's major financial institutions. The outcome of significant research efforts has led to the realisation of a risk analysis methodology and tool that will meet the most stringent of requirements while satisfying the changing demands placed upon the security or audit team in the business context.

COBRA flexibility, automation, knowledge bases and reporting capabilities have filled a gap that conventional tools and methods have; the usage of which can lead to:

(a) Saving of audit/review costs resulting from productivity gains;
(b) Reducing risk exposures significantly by being able to target security threats and issues systematically;
(c) Providing increasing security awareness to the business;

(d) The application of baseline security in a consistent form;

(e) Faster turnaround time from automated processes.

2.5.4 Other developments

2.5.4.1 GAISP/GASSP

With organizations facing challenges to manage and validate compliance with a myriad of standards and regulations, organizations will need to boil requirements down into a common taxonomy. Organizations need to understand the common elements in all of the standards/regulations they have to comply with and show compliance with the common elements, which then can be mapped back to individual standard/regulation. This will drive a renewed growth for the Generally Accepted System Security Principles (GASSP), now awaiting to be renamed the Generally Accepted Information Security Principles (GAISP). GASSP/GAISP is now focused on building out these common detailed elements and mapping them over to security standards and regulations (Krause & Tipton, 1999)

2.5.4.2 CISSP - The trend

Certified Information System Security Professional (CISSP) certification is now set as the management standard for information security professionals (CISSP, 2005). With the focus on managing information security, and the CSO/CISO role being adopted in many organizations, and now mandated in US federal agencies through the Federal Information Security Management Act (FISMA), the CISSP professional certification will continue its lead as the premier information security management certification for information security officers and managers. As organizations face regulatory compliance obligations, or have adopted standards and best practices to manage their information protection programs, there will be a focus on the certification and accreditation of system security before production implementation. This will be followed by the development of a continuous

assessment process to manage risk and compliance on an ongoing basis.

2.5.4.3 COBIT

COBIT stands for Control Objectives for Information and related Technology. It is an open standard for information security and control practices. It basically provides a framework to assist various stakeholders including management, security practitioners, auditors and users in their daily security related activities.

2.6 Summary

The importance of this topic can easily be noticed by discovering the number of security standards that have been formalized so far and their continual development across continents. The aim behind this initial literature survey chapter was to present the fundamentals of information security, importance of proper security policy, its relevance in the business environment as well as the history and development of the principal security standards in the world. This will provide an insight into the topic before being exposed to findings on the global arena which will be addressed in the forthcoming chapter.

Chapter 3:

Compliance Issues Reported on the Global Territory

3 COMPLIANCE ISSUES REPORTED ON THE GLOBAL TERRITORY

3.1 Introduction

Having presented the underlying fundamentals of information security, the importance and relevance of proper security policy and the most prominent security standards presently in place, it now becomes important to research on the present state of information security issues and bring forward findings on compliance problems reported globally. This will provide all stakeholders with a benchmark or state of information security policy compliance and practices on the international ground and against which one can eventually compare similar findings that will be gathered on Mauritius.

This chapter therefore aims to uncover findings on the global scene and specifically report on deviations and compliance issues that were registered in relation to security policy from known sources.

3.2 Critical Success Factors of Information Security

Critical Success Factors (CSFs) are factors which are 'critical' for an organisation or a project to achieve its mission. From the literature, there is a strong support for properly defined and implemented security policy both for business survival as well as for productivity needs (Control Data Systems, 1999). Furthermore, one can gather from the literature that existing policy plans can barely demonstrate the impact on users and business processes. It may lead to a wrong perception on security if the domain area and its application are not understood properly**.**

Disparate security policy and compliance can easily open the way for security breaches. This raises concerns on the risks associated with disparate or non-compliance with security policies and hence enforces the need to give this a focal attention.

Based on the literature review, one can identify certain key factors leading to the failure of security policies within the American market (US and Canada) (Control Data System, 1999).

Security may stand as barrier to progress if it is wrongly outlined and applied. For instance, if security policies are not well designed and implemented, there is a high risk that they stand counter productive to the business. In other words there is a strong need to have a balance between security controls and business practices to avoid chaotic situations that disrupt business operations and productivity of staff as a whole. A complex policy can in itself make it hard to be implemented and understood by the target group. Security policies therefore require careful analysis and assessment before they are formulated and implemented.

Security is a learned behaviour which necessitates sustained attention and effort. Information security procedures are often not intuitive as one may think. For users and employees to recognize the risks associated with compromising security policies and their resulting financial impact, there is a need to put proper education programmes in place. In other words, there is a need to ensure that all employees, irrespective of their levels, are well trained and continually informed of the need to protect the valuable assets of the organisation. This also applies to the top management who need to act as sponsors to ensure such learned practices are prevalent which in turn will justify the reasons of having sound security policies implemented. This also implies that management needs to be aware of security policy, risks of non compliance and accompanying financial impacts so that proper funding or commitment can be made (Carigue & Stefaniu, 2003).

Security must be considered as a continuous and never-ending task for it to be effective. The process of securing company's assets is a continuous process which does not stop once certain security measures and policies are implemented. With the constant introduction of new technologies on the market and the ever developing state of the technological environment, which in turn bring along a number of accompanying technical and security implications, the process of reviewing the implemented policies becomes a must. Every process and security

policy should therefore undergo continual "health checks" and ensure they are relevant, up-to-date and are being enforced. A static security policy that does not cope with new developments and changes to business processes might simply stand as ineffective. Similarly, it was confirmed that one of the recommendations for reducing risks was to ensure IT security policies are up to date and well publicized throughout the organisation (Security Institute, 2001).

A well established framework for information security governance which addresses three primary objectives that can significantly help an organisation to set up the baseline for security policy management was presented in the literature (Carigue & Stefaniu, 2003). These objectives are developed around "Informing", "Educating" and "Influencing" the top executives.
In other words there is a strong need to ensure that:

- top management are informed about issues such as environmental threats and vulnerabilities identified by the industry and research centres, the development of a regulatory framework and security incidents. Furthermore, they also need to be aware of accompanying impacts of such threats on businesses and appropriate measures needed to protect their assets;
- top management are educated on risk factors that affect their organisations' bottom line, risks associated with emerging technologies, roles and responsibilities to ensure security policies and practices are adhered to;
- top management are influenced so that security gets on their priority list so that funds and human resources are allocated to such projects. If this is left out at top management, it will unfortunately have adverse effects on the organisation's bottom line and goodwill. Input from security experts should be sought on security projects as and when needed. This will definitely add value to the overall process thanks to the know-how and exposures of the expert resources. Moreover proper reporting structures for impact assessment, governance and management of the established security framework should also be envisaged in the overall programme.

There is a need to put in real effort in communicating the security objectives as specified in the policy document to the main players and responsible parties. This will in turn set the expectations right, get everyone to be accountable when and where needed while facilitating the implementation and adherence to security policies. Systematic reporting on awareness and training program needed for an effective implementation of the security policy were key success criteria in Canada (OECD Proceedings, 2004).

Along with the above, the right set of metrics needs to be put in place for effective communication of the status on information security, the high priority issues and proposed solutions to continuously improve the security posture of the organisation through well defined practices and policies.

The topic of IT security policy and its application has also attracted the attention of OECD which has led to the publication of sound and comprehensive guidelines for the security community (OECD Guidelines, 2004). Among the guidelines of the information security issues, it has been stressed that every organisation should have a well defined set of information security policies, standards and procedures so that each and every stakeholder knows its role and responsibilities. By getting everyone to be accountable for their respective duties, it will help employees to know exactly what is expected of them and deliver better. Similarly, in the earlier Proceedings of OECD organized in Japan, it was emphasized that well-defined information security policies create better management (Harter, OECD Proceedings, 2001)

Similar observations have also been made by IEEE during its Proceedings where it re-stresses that security policy can be used as an education and communication tool within the organisation for employees to gain and share knowledge among themselves (IEEE, 2003). This also helps in propagating knowledge on security awareness better and faster in a consistent manner. Employees in turn become more acquainted with their roles and responsibilities towards security enforcement (ACSAC 2003).

While these findings are converging to a common conclusion on the importance and role of IT security policies, it is nevertheless a challenge to make it work systematically. This challenge has been here for long. For instance similar concerns on the challenges facing organisations were expressed by the US Department of Treasury where the difficulty in keeping security policies relevant was highlighted (Ferris, 1994). This was mainly due to the rapid growth in IT and its dynamic changing nature. The U.S Treasury, in fact, demonstrated its commitment to developing IT security standards by formalizing and setting up a framework to meet the challenge of "keeping up" with the ever changing IT world.

3.3 Reported Case Studies & Survey Results

3.3.1 2004 Global Information Security Survey by CSO Research

The 2004 Global Information Security Survey conducted by CSO Research is one of the largest security researches conducted with 8,100 respondents from 62 countries (CSO Research, 2004). The purpose of the study was to assess the state of information security practices across the six continents. Information security disciplines, practices, spending, policy compliance, incidents, risks, compliance with regulations and CEO's confidence level on security activities were among the key areas that were surveyed and analysed.

3.3.1.1 Results of the study

A résumé of the findings has been depicted below with accompanying analysis of the outcomes.

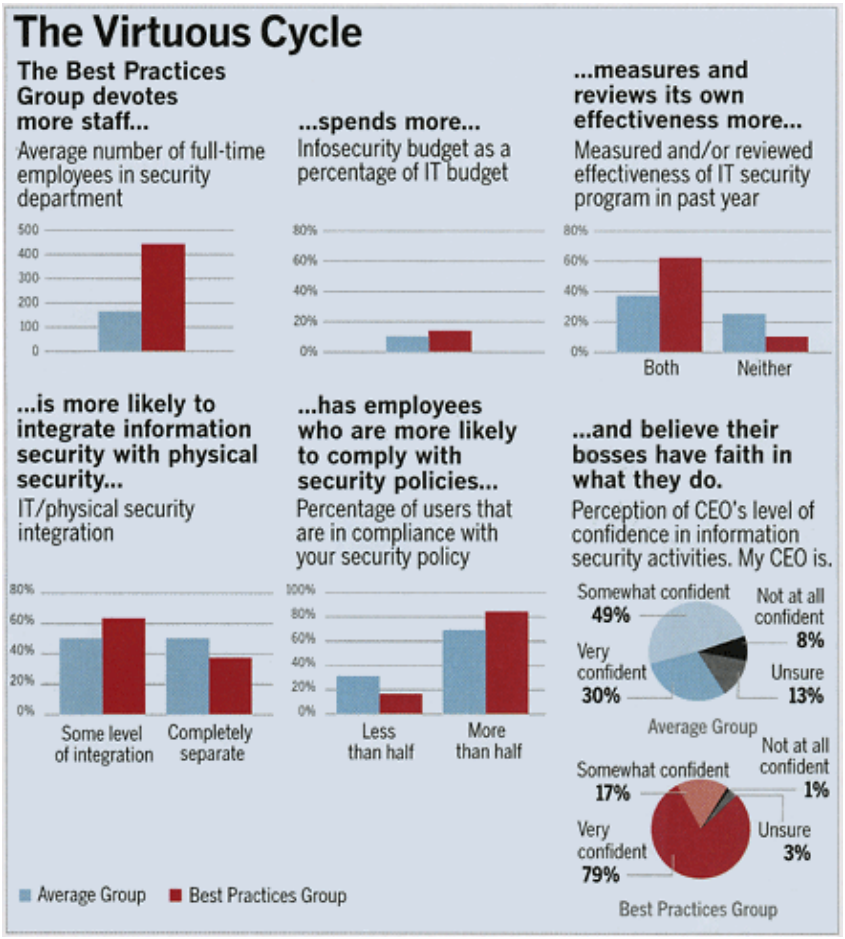

Figure 3-1: Summary of findings for 2004 Global Information Security Survey (CSO Research)

Consider figure 3-1:

- Around 60% of the Average Group respondents did neither measure nor review the IT security program in 2003. Even among the Best Practices Group, it can be noted that a significant rate of 40% of the respondents who did not measure and review their IT security program. Such findings may contribute to the failure of such programs in the future because they are failing to keep up-to-date with the pace of change. This was also experienced and supported by Department of the Treasury in Washington D.C's statement earlier (Ferris, 1994).
- As regards compliance with security policy, there was a significant rate of noncompliance among at least half of the respondents where the rate of noncompliance, among 50% of the two groups, averaged around 80% including respondents from

the Best Practice Group. This is an alarming result which may be contributing to the deterioration of the security policy implementation and thereby increasing the threats associated with such risks.

Furthermore, even for the other half of respondents who claimed to be complying, it can be noted that an average rate of around 25% of non compliance existed among the two groups meaning that there is still room for improvement in this area.

- While analysing the results of the top management confidence in information security activities, one can note that 8% and 13% of the CEOs of the Average Group are not confident at all and unsure of the security activities respectively. However, 49% are somewhat confident. This may imply that further work has do be done at this level and for this group of CEOs to ensure that belief in information security is restored further and any doubts are cleared. The CEOs of the Best Practice Group nevertheless reassure the stakeholders of their beliefs in information security where 79% expressed their high confidence in such programs as compared to only 30% of the CEOs of the Average Group. Strangely, both the Average Group and the Best Practice Group seem to be spending nearly the same percentage of their IT budget in information security projects. This may imply there are factors, other than IT security budget, which may be hampering or delaying the increase of CEOs confidence among the Average Group. The Best Practice Group may be having a better supporting structure and framework to sustaining its CEOs confidence.

A further analysis of the same research yielded other interesting elements both in the home country (US) and abroad (rest of the continents). A summary is shown below:

Figure 3-2: Summary of findings for 2004 Global Information Security Survey (CSO Research)

Consider figure 3-2:

- As regards compliance with security policy, it is worth paying attention to the tendency of compliance or noncompliance over the world. It can be noted that the average compliance rate with security policy, by the users, is around 70% for the overall four continents (excluding Africa and Australia) although 64% of the respondents increased their IT security budget. This implies that there is nevertheless around 30% of noncompliance overall which is a significant rate and thus there is still a long way to go to reduce this to minimum. The root cause for such noncompliance needs to be determined too.

- North America has the highest rate of compliance followed by Europe and then Asia. South America has the lowest rate of compliance with security policy with a rate of around 60%. There is also a significant rate of 17%, among the South American CEOs, who are not confident at all with their information security. It can be deduced that the rate of noncompliance with security policy varies from country to country and continent to continent. There may be several factors behind the rate of noncompliance which thus becomes an interesting area for research. Given the absence of similar statistics or revelation for African countries, it motivates one to conduct similar studies in African countries too. This will help to identify the degree of compliance as compared to developed countries and reveal any disparity arising due to development, cultural or other attributes.
- Furthermore, although IT spending on security is among one of the barriers to good security, there is also growing need for good and dedicated staff in security area (39% in 2003 and 44% in 2004). This implies that human resources not only play an important and yet contributory role in the overall implementation of security practices and policies but also help to elevate the level security across a wide spectrum. Thus finding the right human resource for such projects is a challenge to the setting up of the baselines for security implementation.
- Around 49% of the overall CEOs are somewhat confident in their information security but only 30% expressed high confidence. This confirms that the majority of the top management cannot confirm with high assurance thus implying that there is still a way to go as regards uplifting of confidence in information security.

  A similar trend has been noted at CISO levels too. However, a higher rate of non confidence in information security among 14% of the CISOs can be noted.

- Furthermore, in only 56% of the cases that both business and IT decision makers have jointly engaged in addressing information security issues. This finding calls for attention as information security is not only an IT related issue but also a business issue requiring cooperative efforts from both IT and business drivers.

3.3.1.2 Relevance of the study

The outcome of this study is so informative that it can be regarded as a benchmark for ongoing comparison and analysis. Furthermore, the absence of similar indepth statistics or revelations for African countries motivates one to conduct similar studies in African countries too. Mauritius being a rapid developing African country can be a sound base to be studied and compared with findings of the 2004 Global Information Security Survey. This goes in line with the survey being proposed to be undertaken in Mauritius and identify the similarities and differences in security practices as compared to other territories. The intention is to use this survey as a benchmark to identify where Mauritius stands and confirm certain key perceptions.

3.3.2 2001 & 2002 Security Survey of SearchSecurity

In 2001, an online survey was conducted by SearchSecurity.com on "Security Policies in the Workplace" and which drew 174 responses (SearchSecurity.com, 2001/2). The purpose of the survey was to assess the presence of information security policies and their application in organisations. Spending on the security was also an important element of this survey.

The 2002 survey was also conducted to assess the trend in security policy applications, underlying problems being encountered by organisations in complying with and enforcing security policies.

3.3.2.1 Results of the study

The outcomes of this survey were also alarming as experienced in other surveys as reported above.

Some other interesting findings reported in the 2001 surveys are:

- Around 30% of the respondents communicated their security policies informally through word of mouth;
- Furthermore, around 7% of respondents never updated their security policies while 15% updated it every few years.
- 17% of the respondents confirmed having never checked for policy compliance.

Almost 50% of the respondents either did not have a security policy or were trying to figure out how to create one. One could also note an absence of funding to support the implementation of security related projects.

The same research highlights that the hardest issues faced by most respondents were the enforcement of security policies and end user awareness on security.

The survey conducted in 2002 by the same organisation revealed similar concerns from the respondents. More than 400 who voted in the 2002 poll chose security policies and user compliance as the most pressing issue at their company.

It came out from the survey that developing security policies was one of the challenges and enforcing them was the other.

After having written the policy, the challenge remains on its enforcement, without which the success of the whole information security programme is simply unattainable. To support the implementation and ongoing enforcement processes, there is a need to equip CSOs with the appropriate tools and technology. This will enable them to monitor, review and improve the enforcement plans. Another enabling factor is to empower the CSOs with the necessary authority to enable them to take the

appropriate measures in improving the implementation and enforcement of security policies.

This also confirms the point put forward, that is, adherence to security policies, is an issue which necessitates profound attention and focus so as to ease their implementation and compliance while aiming to mitigate possible risks.

Strangely not many respondents had "security" in their job titles. Most were IT managers/directors and network/systems administrators despite more than 50% of them claiming having spent less than three years in security. This implies that IT security needs to be given more visibility on people's jobs and responsibilities. This will in turn give an identity to the profession and help to elevate the level of security practices far and wide.

The problem is that some companies have yet to elevate IT security as a boardroom priority and, therefore, policies are either in perpetual draft form or do not exist (Mimoso, 2002).

3.3.2.2 Relevance of the study

While the 2001 & 2002 studies confirm the trends around information security policy and practices, such as a significant absence rate of security policies, they also uncover certain important elements in the communication process, maintenance and compliance of security policies such as difficulties faced in enforcing them. These surveys complement the earlier study and can be very helpful and relevant to the proposed study in Mauritius. It will thus allow comparison of not only compliance results, but also organisation culture and practices in relation to information security.

3.3.3 DTI Information Security Breaches Survey 2002

The DTI Information Security Breaches Survey 2002 identified security policy as the most fundamental aspect in information security (Seddon,

2002). The survey was specifically conducted in UK with the aim to identify the underlying security threats and their sources, to assess the relevance and application of BS 7799 and to specify the key elements of a good security policy. It also aimed at identifying the importance of various security disciplines.

3.3.3.1 Results of the study

The main lesson learnt from this survey was that security policy came as the dominant and prime element of information security programmes in UK.

Astonishingly the study found that only 27% of the UK businesses that were surveyed had a documented security policy in place. However 59% of the larger companies had documented policies.

This is still regarded as low although there has been a 100% growth in these measurements as compared to results of the survey of 2000. It is prerequisite for organisations to give information security its place in the main agenda of the business. It must be regarded as a business issue rather than just a technical one. If business managers give the necessary attention and focus, it will help to contain or mitigate security risks further in the Internet and digital era.

Very importantly, it was reported that “16% of large businesses attributed their worst security incident in 2001 to poor training on security issues”. When analyzing security incidents, it was also found that noncompliance with security policy was the main cause of those incidents. This confirms that United Kingdom was among those countries where noncompliance with security policy was an issue of concern.

Furthermore, the Ernst and Young Global Information Security Survey 2002 revealed worrying signs on information security (CSO Online.com, 2004). Less than 50% of the organisations that were surveyed had information security awareness programmes in place. This implies that there was a significant portion that had either poor security policy in place or simply did not have any. Only 7% of DTI survey respondents who had security policy in place stated that they had informed their staff on the security issues and their own responsibilities. The importance of proper communication channel and awareness programme in this area stands as mandatory for the success of such projects.

The general practice in UK revealed that companies were outsourcing their security policy development and implementation. This helped around 60% of the companies to have security policy in place.

3.3.3.2 Relevance of the study

UK has, for long, been a partner of Mauritius. Mauritius has been seeking expertise from UK for implementing proper legislative framework(s) as well as obtaining help in areas of economic development amongst others. Many local organisations have adopted practices prevalent in the UK. It is therefore relevant to compare the findings of both countries and come up with appropriate interpretations on whether Mauritian organisations have similar practices. Furthermore, this survey revealed interesting findings on awareness and training which could be used to benchmark against.

3.3.4 Deloitte 2004 Global Security Survey

In 2004, Deloitte conducted its second global security survey more specifically in the financial services industry. The main goal of the survey

was to assist the participants in assessing the state of information security within their organisations in comparison to other financial institutions around the world. Deloitte had the objective to provide a global benchmark for the state of security in the financial sector. The survey also aimed at collecting information on security related issues including governance, risks, investment, responsiveness, use of technologies and privacy.

3.3.4.1 Results of the study

The survey was conducted globally covering regions of North America, Europe, Middle East, Africa, Asia Pacific, Latin America and the Caribbean. Most of the data collection was done via face to face interviews with CISO/CSO or designate and IT security management teams among whom were respondents from top 100 global banks, financial institutions and the insurance sector. The key findings of this survey were:

- Though Europe, Middle East and Africa (EMEA) were ahead when it came to policy setting, security standards, privacy compliance and had a formal security strategy, they ranked lowest in reporting and tracking security successes. EMEA were ranked at the middle of the table when they were assessed on the value of security as an enabling factor for business operations. This, in turn, demonstrated that they still had to improve on certain fronts to climb up the table and be regarded as role models in the area of security practices.
- It was also reported that Asia Pacific (APAC) was the outgoing world leader as regards providing their employees with training including awareness on security, privacy issues, statutory and policy compliance. Interestingly, one could also note that APAC countries had the maximum number of policies that were described as “ad-hoc”. It was found that there was a lack of clarity and direction within these policies which explained why only 34% of the respondents reported having the right set of security Key Performance Indicators

(KPIs). In other words, a significant scale of 64% had difficulties in responding on their security KPIs and had varying tracking measurements. It was found that a sustainable improvement in the governance and compliance structure would put APAC at the forefront of others. Though the results on APAC were promising in certain areas, there were nevertheless other areas of concern which necessitated focus and attention.

- Latin America and Caribbean (LACRO) respondents confirmed that they had defined and documented job roles and responsibilities for their security staff but, surprisingly, none of them was reporting on security KPIs. This was partly attributed to the fact that there was a lack of skills and expertise in the security area among this group. Furthermore very few (around 20%) were able to confirm that they had and were using performance metrics. Legal and industry regulations were the main motivation for ensuring compliance among 75% of the respondents. This demonstrates that people comply with policy issues when they come from sources of authority.
- Canada hit the top position as being the most compliance-focused country. They had the highest level of top management commitment and funding injected in security projects to address legal and regulatory requirements. Interestingly the report stated that “Canada led the world when it came to understanding the link between security and business strategy.” They were also top in tracking and measuring security project successes. Despite the fact they had the highest rate of respondents reporting on the appropriate sets of security KPIs, there were nevertheless around 30% of the financial institutions that failed to use security KPIs. Canada was also strong at communicating security successes. Skill gaps were also felt by the Canadian respondents.

- Though the US respondents were the highest spenders on security projects, they nevertheless were the least likely to have job roles and responsibilities well documented. Furthermore, over 50% of the respondents claimed that their employees had received no awareness or training on security, privacy and compliance issues over the last year. This could be an area needing attention, given that security awareness and training needs to be continually on the agenda so as to keep pace with ongoing technological development and counter new sources and types of threats.
- Among the good and welcoming moves, it can be noted that financial institutions were adopting the implementation of security framework in a comprehensive and structured manner with the adoption of industry of standards such as ITIL, COBIT and ISO 17799/ISO 27001. This demonstrates the interest and determination of adopting such established standards while giving a strong signal to other non financial institutions and industries.

3.3.4.2 Relevance of the study

This survey provides an insight into security practices across various countries and continents having diversified cultural, economic and social characteristics. This survey is also very recent and can be a sound source to compare with, especially in areas of adoption of known standards, documentation and compliance with security policies and driving factors for compliance.

3.3.5 April 2003 CSO Online Survey - Security Immaturity

In April 2003, over 1,000 respondents responded to an online self-assessment exercise conducted by the Human Firewall Council, a nonprofit information security organization (Slater, CSO Online.com, 2003).

The purpose of the survey was to measure the state of information security against ISO guidelines.

3.3.5.1 Results of the study

1,057 organizations took part in the survey online which was held between September and November 2002. The average number of employees at these organizations was approximately 12,900. Respondents were from 78 different countries, and the majority (55%) were based in the United States.

The key outcomes of this survey were alarming where several areas of security were low-graded and which required significant effort to uplift the levels. The key findings have been summarized below:

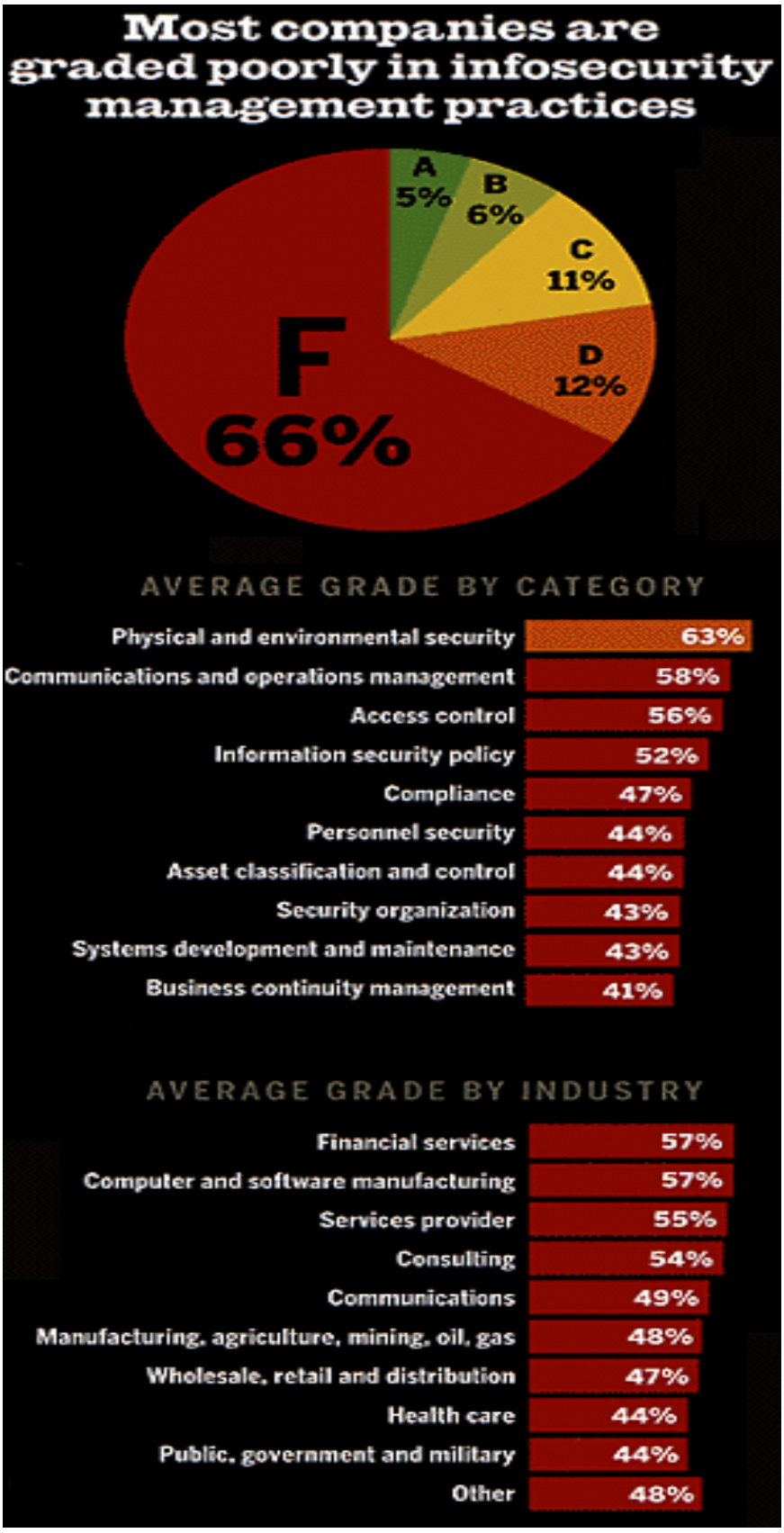

Figure 3-3: CSO Online 2003 Survey Results

Consider figure 3-3:

- It can be noted that most respondents had a reactive approach to information security, that is, they reacted to security problems by purchasing solution rather than devising a systematic and comprehensive approach that could address education, policy, architecture and so forth. Michael Rasmussen, an information protection analyst for Giga Information Group and one of the principal authors of this survey reported that the approach currently being contemplated by the respondents was simply tactical. Instead, it required a shift in mentality to give information security increased attention of business drivers and management. In other words, it should be considered as a business problem rather than a technical one.
- Furthermore, findings on information security policy and compliance have not been great as depicted in the diagram above (figure 3-3). Only 52% of the respondents claimed to have security policies in place while only 47% claimed to be complying with the policies and standards. There was a feeling among respondents that compliance with security policies and regulations was time consuming and required continual and progressive efforts. This was clearly noted among respondents of a Fortune 500 financial services company. At the end, these findings are effectively low and worrying in these days especially when security concerns are rising day by day.

3.3.5.2 Relevance of the study

The interpretation of the result was interesting and gave factual information on information security practices by industry sectors. There could be some correlation between security practices and industry characteristics in Mauritius as well. This could be valuable information to analyse and report on and against which one can benchmark too. It will help to dissipate any doubt or

wrong perceptions on industry practices in relation to information security.

3.3.6 Computer Sciences Corporation Survey

The purpose of this survey was to shed light on the most pertinent concerns of information security; that of assessing and reporting on the state of information security practices across the world.

3.3.6.1 Results of the study

A survey which was conducted by the Computer Sciences Corporation (CSC) in 2001 revealed inadequate information security practices among corporates worldwide (El Segundo, 2001).

The survey results revealed certain key findings among the respondents such as:

- 46% of the respondents confirmed absence of a formal information security policy in their organisations;
- 59% confirmed that they did not have a formal compliance program as part of their Information Systems function and structure;
- The majority of the respondents (around 68%) did not conduct security risk analyses or security status tracking on a regular basis. It seems this was done on an ad hoc basis and not systematically.

3.3.6.2 Relevance of the study

Looking at the results obtained from the organisations polled, it can be noted that there are similarities with other surveys conducted where a significant absence of formal information security policy as well as low compliance rate were found. No doubt, this is not a reassuring statement for the community of security practitioners. It also gave rise to concerns on threats and risks associated with absence of and/or noncompliance with formal security policy, an area worth researching to understand why such practices are prevailing.

3.4 Lessons learnt from the global findings

There are some common findings reported by most of the researches and which are being summarised in Table 3-1 below:

Negative Issues	Positive Issues
1. There is a problem of compliance with information security policy, standards and regulations across the world; 2. It has also been found that there are many cases where there is either an absence of properly defined security policies or simply defined on an ad hoc and unstructured basis; 3. There is a lack of effort to measure and track security projects systematically using proper security KPIs; 4. Where security policies exist, it was found that they were not maintained regularly to stay up-to-date with changing conditions; 5. Some surveys revealed low participation or commitment of top management in certain areas of security implementation.	1. There is a strong need for security training and awareness for employees and staffs and the management's readiness to invest along these lines; 2. There is a growing investment in security projects across the globe; 3. Organisations around the world are concerned about security policy and compliance issues and efforts are being dispensed to address any gaps in compliance.

Table 3-1: Summary of findings on the global territory

3.5 Summary

From security governance to policy compliance and education, one could note that information security policy is not just about writing it down but instead setting a proper framework for its implementation, adherence and ongoing improvement. Furthermore, setting the right KPIs to measure the performance of security implementation is mandatory for the success of security projects.

This chapter has compiled and brought forward findings on security policy and its compliance from various sources around the world. Several renowned survey results were analysed and presented here.

Despite certain studies revealing an improvement in some areas of information security, like recent increases in budgets/spending on security projects, there are still major issues to address to bring information security where it should be. For instance findings on compliance with security policy revealed to be in a problematic state across board. Without the commitment of management, institutions and authorities including government, such realisation could be a cry in the desert. Thus, it should get the attention of everyone in order to improve further.

The results obtained from the above-mentioned sources can be used as a benchmark to compare similar findings in the Mauritian context. This will be discussed later in this document.

Having reached this stage, it is worth asking the question where Mauritius stands at this moment. Are there similar compliance problems reported in Mauritius? Are there any similarities or differences in Mauritius in relation to security policy and practices? To answer such questions, it requires a comprehensive research effort to be done on Mauritius. Thus, the target of the subsequent chapter will be to gather, study and present compliance issues reported in Mauritius so that gaps and specificities can be identified between the realities of the world and within the local context.

Chapter 4:

Compliance Issues Reported in Mauritius

4 COMPLIANCE ISSUES REPORTED IN MAURITIUS

4.1 Introduction

The background study has enabled a better understanding of the subject matter across the globe. One could easily note a certain tendency in security practices especially in areas of security policy formulation, implementation compliance and education. The various studies conducted and reported globally gave a clear and factual state on information security.

Presently the Mauritian economy is based on five pillars including agriculture, manufacturing, tourism, financial services and ICT. After analyzing the outcomes of the global studies, a common question is set on whether Mauritius, an island on the verge of developing ICT as its 5th pillar of the economy, is facing similar problems as that reported internationally.

There is a general perception that Mauritius which is a developing country in Africa, is also facing security policy compliance problems. It is also perceived that security implementation in Mauritius is not to the level of internationally established standards.

Thus it becomes important to conduct an in-depth study on Mauritius so as to identify reported cases that can help to understand local practices in security policy implementation and compliance.

The purpose of this chapter is therefore to conduct a background study of the local Mauritian context, identify and report on such cases where compliance with security policy was absent and the resulting effects.

4.2 About Mauritius

Mauritius is an island covering 1,865 square kilometres, situated some 2,000 kilometres off the south-east coast of Africa in the Indian Ocean. The population of Mauritius is 1.2 million consisting of five main ethnic groups, Hindus, Muslims, Chinese, Creoles and Franco-Mauritians (2003, Central Statistical Office). Most Mauritians are bilingual being equally fluent in French and

English, and over time this has given Mauritius a competitive edge on other countries which are either English or French speaking.

Mauritius enjoys a strong literacy rate of over ninety per cent, and is one of the few countries in the developing world that is close to achieving universal literacy. The large pool of well educated young people, versatile and easily trainable, is a valuable asset for the country to meet the challenges of an ever-increasing competitive working environment.

Political stability has been one of the most significant factors that have helped Mauritius in its economic success. The Republic of Mauritius is a presidential democracy modelled on the British system of parliamentary democracy, and has been crucial in providing an economic environment that encourages foreign investment. The main challenge that the government faces is to sustain the pace of economic growth achieved in the last five years.

From a sugar-based economy, Mauritius has successfully diversified its economy by developing the manufacturing and tourism industries. Full employment and a lower, stabilized rate of inflation have accompanied the high growth rate generated by these two industries in the past five years.

By exploiting the ideal geographical location of Mauritius, a hub connecting Africa, Asia, Middle East, Europe and Australia together, the financial sector has become the fourth pillar of the economy as an overall strategy designed to diversify the economic base and to sustain growth. This sector has been enhanced by developments in the offshore sector, a more dynamic stock exchange, and the extension of Freeport activities. Furthermore, a greater exposure to global financial markets, through liberalization of both banking and exchange transactions, will certainly provide more dynamism to the financial services sector.

Mauritius is now on the verge of transforming itself into an Information Communication Technology (ICT) hub in the region.

4.3 Major undertaking – The development of the 5th Pillar of the economy

Massive investment and resources are being put in transforming Mauritius into a "Cyber Island" which will constitute the 5th pillar of the economy in the coming years. While one of the major initiatives of the government has been to lay out a strong legal framework by instituting regulations like Computer Misuse and Cyber crime Act, ICT Act, Data Protection Act, Electronic Transaction Act, Information Technology Act, Internet Service Provider Act and Copyright Act that will provide a sound environment for operators, it has also set an ambitious goal of turning the country into a "cyber island" in the coming years. One of the priorities will be to transform the country into a world class off-shoring and outsourcing destination through:

- The development of Mauritius as an ICT hub
- The building of a state-of-the-art Technology Park
- Partnership & Alliances
- Human resources development in ICT
- A sound and strong legal environment
- The liberalisation of telecommunications
- Remarkable incentives to investors in ICT

Mauritius is being positioned in the areas of Business Process Outsourcing (BPO), Business Continuity Planning (BCP) and IT Enabled Services with a view to achieving this goal. Strong skills and infrastructure development programmes are under way to accompany this wave.

India and other partnering countries are the main players in this development process. Local and foreign expertises are joining forces to create the synergy to make this a real success.

4.4 Reported compliance issues

While very few documented evidence(s) exist on compliance or noncompliance with security policy, standards and procedures, it has been possible to identify certain major cases which are worth presenting at this stage to express the state of

security issues locally. These cases are somewhat linked, in one way or another, to security compliance.

4.4.1 MCB Scandal: Financial Fraud of 2003

4.4.1.1 Introduction

The Mauritius Commercial Bank Ltd (MCB), one of the most prestigious banks of the country, has been the victim of a massive fraud in February 2003 (Mauritius News, 2003). Everyone has been stunned as a consequence, seeing the financial scope of the fraud ranging in the amount of MUR 880 million. Such fraud has never been reported in the past but this issue has taken an important dimension in the local and regional contexts.

4.4.1.2 The findings

As soon as this fraud was detected, an internal investigation was immediately ordered with a view to determining its scale. In fact, a fixed deposit of the National Pension Fund (NPF), made by the government on behalf of its stakeholders since 1998, had astonishingly disappeared and could not be traced. After investigation, the MCB admitted the massive fraud of MUR 880 million stolen from the accounts at the bank in the name of the National Pension Fund. This caused a severe set back to the goodwill of the bank which has been exposed to heavy criticism from all stakeholders. This fraud was largely covered for long by the local and regional press.

Several people were arrested and released on bail, including the senior management of the bank. Police has yet to find the culprits behind this scandal.

Though the outcomes of the investigation exercise were not disclosed by the bank due to ongoing police inquiry and confidentiality reasons, the press was nevertheless able to shed

some light based on information obtained from confirmed sources.

The different press reports have created a perception in the minds of the public that there were:

(a) A lack of segregation of duties given that one or very few persons were able to transfer such a huge amount of money by some means without leaving any trail;

(b) An absence of strong security policy and procedures that could harden or obstruct such fraud to happen on the computer system of the bank;

(c) A deviation from or violation of the established policies, procedures, code of practice and duties and responsibilities by certain officers;

(d) The banking process, procedures and regulation might be outdated needing prompt review. This was supported by Mr Dev Erriah, fiscal and legal specialist from Erriah and Uteem Chambers, who has been observing the banking process in Mauritius over the past years and confirmed that it is outdated and lacked proper accountability. In his opinion, such funds should have been deposited with the Bank of Mauritius which is the government banker and the supreme controlling bank locally instead of depositing in commercial banks like MCB (Trust and Trustees, 2003).

4.4.1.3 Relevance

This case shows a lack of proper controls in certain areas of the bank's operations. Despite the presence of regulatory framework and policies, such fraud was committed. For such fraud to happen, one can infer that security and control policies were not adhered to. The absence of compliance with defined control and security policies impacted severely on the goodwill of the bank as well as the country.

This case has a direct relevance to the subject matter under study as it is a vivid case of failure to comply with security policy and controls leading to severe impacts on business performance, trust and goodwill.

4.4.2 MCB 51 Million Rupees Scandal: 2005

4.4.2.1 Introduction

While the root of the 2003 scandal is yet to be found, the bank was not spared from a second blow in February 2005.

In February 2005, MUR 51 million vanished from the coffers of the main branch of the Mauritius Commercial Bank (MCB) in Port-Louis. Four people allegedly entered the main vault, killed one senior employee, a 49-year-old supervisor, inside the coffers and made away with the money (Mauritius News, 2005).

This is the second time in two years that the MCB, the biggest bank in the island, hit the headlines.

4.4.2.2 The findings

There is no doubt that the robbery was well organized with knowledge of internal operations, security controls, procedures and ways to commit this crime without anyone noticing it. The robbery took place very discreetly through a rather calm penetration into the bank's secured zone and taking the money out of the vault without breaching the alarm system or being noticed by security controls in place. The bank gained knowledge of this robbery only when the management was informed that one of their personnel was murdered inside the vault.

Months have gone by but the police has yet to find the mastermind of this daring robbery at the main vault of the MCB. At least MUR 51 million have been taken away in this operation.

To date, six people have been arrested and charged provisionally; among them was one bank cleaner/office attendant. According to police sources, the suspects have all named the 49-year-old bank supervisor, the man who was killed during the operation, as a partner in this crime, together with the mastermind of the operation who, they alleged, also works at the MCB. They refer to him as “Big Boss 007”. Police has yet to identify this person.

Based on preliminary findings, there is a strong perception that people involved in this criminal act had in-depth knowledge of internal operations and the loopholes of the control system. There is a common observation that the security controls at the bank were lacking and ineffective after determining the ease with which this robbery was committed. It could also be interpreted that security controls and policies were deviated and that they were not tight enough to protect the bank from such risks.

These issues have unfortunately created a negative impact on the bank, the financial services sector and the country as a whole. It has, in turn, given a strong signal to all stakeholders that security measures can easily fail if strong security controls, policies and procedures are not implemented properly and reviewed frequently.

4.4.2.3 Relevance

Like the earlier case, this one also directs people to a common thought, that is: are the local organisations’ security policies and procedures up to the standard and being complied with?

The case which is presently being analysed sets out a series of questions and concerns:

(a) Were there proper security controls at the bank that could have obstructed this robbery from happening and alerted the security control room promptly?

(b) Were these security measures implemented properly at the bank?
(c) Were there proper security policies in place that were being adhered to and properly controlled?
(d) Are security of data, people and resources being given enough attention by organisations of Mauritius?
(e) Are Mauritian organisations complying with security standards and policies systematically?

There is no doubt a converging concern on the presence, relevance, completeness and compliance of security policies and procedures in Mauritius. Such findings, concerns and perceptions further motivate one to investigate and study the subject matter in-depth so as to give inside knowledge on local practices and help the security community to learn and develop better.

Today, the challenge of the top management is to gain sound knowledge on the state of their security implementation and establish the degree of conformance to international standards and best practices in respect of security policies and procedures. Accurate knowledge on the degree of compliance with international norms, best practices and security policies set out are also crucial from a risk management perspective for every organization.

4.4.3 Cybercrime: Mauritius Telecom ADSL & ATM Network Affected

4.4.3.1 Introduction

In March 2005, Mauritius was completely disconnected from Internet for more than 48 hours leaving the country in total isolation from the electronic world.

The Asymmetrical Digital Subscriber Line (ADSL) and Asynchronous Transfer Mode (ATM) network was seriously

affected after an act of sabotage. The majority of businesses were affected where they had their wide area network and internet connectivity down for a significant number of hours. Mauritius Telecom, the service provider for these network services, could not limit the impact of consequences arising from this event.

4.4.3.2 The Findings

Given the severity of this issue, major investigation bodies in Mauritius were called to shed light on this sabotage. Experts of Mauritius Telecom, Central Investigation Division (CID) of the police and Information Communication Technology Authority (ICTA) joined forces to determine the exact cause and source of this event.

The preliminary investigation and findings of ICTA confirmed that Mauritius Telecom's ADSL and ATM network were hacked causing this severe down time. The cyber crime had its origination from Mauritius itself where the hacker used a dial up connection to log into the network of Mauritius Telecom (L'Express, 2005). It took 90 minutes for the hacker to delete the configuration details of the system software and disks which contained the main backups. The system operating on the main exchange of Port Louis was also tampered with, concluded the experts of Mauritius Telecom and Nortel.

The network also went down as soon as the hacker disconnected and unfortunately Mauritius could not rollup by restoring its backups since they were deleted.

It was confirmed that this manipulation could only be done by someone holding administrative rights. The administrative password was known to a very restricted group of personnel at Mauritius Telecom.

Finally it was found that the person that committed this crime was an ex-employee of Mauritius Telecom who held administrative rights at the time of committing this crime, and who was now working for a competing firm. The equipment(s) through which this crime was committed were seized by the police and seem to contain enough evidence(s) to elucidate this crime. The court will now have to give its verdict on this issue.

One can easily deduce that the security controls and policy in place were not adhered to since the rights and access codes of the ex-employee were still active after his resignation. The basic security policy describes that in the event of an employee's resignation, the person's account and all of his/her access permissions are deactivated with immediate effect. This was not the case here and it finally caused a severe loss of business for Mauritius Telecom due to the absence of basic preventive security and control measures. The event not only affected Mauritius Telecom's reputation and business, but also that of its subscribers who were in great numbers.

4.4.3.3 Relevance

This case is a concrete example where compliance with security policies and best practices has failed. Basic security procedures were not followed and preventive measures ignored leading to severe impact on the business environment in Mauritius. The case is highly relevant to the subject matter being studied and further motivates one to pursue alongside.

4.5 Summary

Having identified concrete local cases where ineffectiveness of security policies, procedures and practices have been found, it can now be confirmed that even the topmost organizations like the ones mentioned above can face such problems in Mauritius. In other words, findings in Mauritius prove that conditions are not so

different from countries around the globe with regard to security practices and policy compliance. It thus becomes even more important and motivating to conduct a study in this respect so as to clearly identify and understand local security practices and areas of improvement. Without tangible findings, it will be difficult to confirm or generalize the perceptions obtained so far.

However, before undertaking a field study to gather primary data, it is worth analyzing the specificities of the local context with respect to security practices, that is, comparing the local practices with those of other developing countries. This will help one to identify any such attributes that characterize its behaviours and practices with regard to information security policy locally. Furthermore, it will be possible to identify any gaps in practices between counterparts and best practitioners.

Thus the objective of the next chapter will be to come up with any such gaps and appropriate interpretations so as to support the remaining stages of the study and help to conclude better at the end.

Chapter 5:

Comparing Mauritius & Other Developing Countries:

Differences & Specificities

5 COMPARING MAURITIUS & OTHER DEVELOPING COUNTRIES: DIFFERENCES & SPECIFICITIES

5.1 Introduction

While compiling all these research findings on information security across the globe, one stumbles over the question as to how Mauritius compares with the rest of the world. It becomes a challenge to test Mauritius along similar parameters so as to get a feel of where one stands, especially when Mauritius is targeting to become a “cyber island” in the years to come.

While the previous chapters have given a clear indication of the state of information security compliance around the world as well as in Mauritius, a stage has now been reached where a fine analysis and comparison between global cases and findings have to be undertaken with that of Mauritius. This will enable one to gain further knowledge on the local specificities that make the home context unique. This will also help earmark any gaps between the local findings and international standards and best practices.

The objective of this chapter is to compare the findings obtained from the local cases with international ones and come up with proper interpretation. Moreover, the aim is also to come up with the degree of variation between established standards and local realities. These differences will also lay the foundation for setting concrete hypotheses for further research so that appropriate measures can be identified and implemented in view of closing any identified gaps.

5.2 Differences and Specificities

Despite very few documented case(s) and evidence(s) on the implementation of security standards and compliance with security policies, procedures and standards in Mauritius, one can nevertheless identify certain concrete differences and specificities which can motivate this research. Some of the main differences and specificities in Mauritius as compared to other developing countries are:

5.2.1 Absence of relevant secondary data in Mauritius

Based on the findings to date from secondary sources (e.g., past researches, findings, publication or documentation) there has been no such research conducted in Mauritius to establish:

- the degree of conformance to known security standards;
- the degree of compliance with implemented security policies and procedures among organisations operating locally;
- whether those organisations that have implemented security controls, policies and procedures have systematic ways and means to review and improve them over time;

These stand as major differences that strongly motivate one to conduct a research more specifically on Mauritius and come up with the necessary findings. This can in turn provide tangible and precise data to Mauritian CIOs, CSOs, top management and government on the state of information security in Mauritius instead of relying on certain perceptions.

5.2.2 Investment behaviour

Most developing countries are injecting significant finance and effort in information security and are being supported by increasing commitment from their top management (Deloitte & Touche 2004). While data exist on investment being made by organizations through their corporate annual reports, one cannot unfortunately earmark investment relative to information security projects. There is a tendency that investments being made by Mauritian organizations are almost of financial orientation, that is, in view of getting financial returns on investment. Local organizations are investing on projects that have direct and measurable financial returns. It does not seem that investment in security is among their primary motives. This is yet to be found and confirmed for Mauritius. Unavailability of concrete data on investment behaviour leaves several questions on information security unanswered and stands as a major gap. The investment being made on security projects will indicate the importance of and consideration given to information security by local organizations.

5.2.3 Education and its orientation in Mauritius

Based on global findings, it could be noted that major developing countries are sustaining their investment in security awareness programmes and skill development while others are simply outsourcing this function or the skills from foreign countries (Seddon, 2002). While data are available on skill development programmes in Mauritius, they are unfortunately not specifically geared to security projects but rather to general ICT skill uplifting (MQA 2004). Despite various established training and education bodies in Mauritius, their main focus has so far been towards providing knowledge on generic functions and products. Training on risk management, security threats and controls, security standards and best practices is yet at its very infant stage in Mauritius. Very few organizations have started engaging in education in these areas. There is yet a great need for Mauritius to channel its effort to this area specially after witnessing the problems as reported in the earlier chapter.

5.2.4 Financial assessment of security breaches

While evidences on security breaches have been recorded, it has been possible to scope the financial implication for the affected organisation as compared to other developing countries. The cases that were reported in Mauritius had direct financial implications which could be estimated following the breaches. Although, it was possible to estimate the financial loss in monetary terms for the cases in Mauritius, one can barely confirm whether local organizations have a systematic way of estimating risk exposures and losses from security breaches. The cases as reported earlier are very specific, in the sense that the fraud and sabotage that occurred had a direct financial impact on the business (L' Express, 2005). The absence of proper security policies and controls was a key abettor of these crimes. Among the cases which were reported on the global territory, it was quite difficult to estimate the impact in financial terms. The findings on the global territory seem to demonstrate that either the organizations faced difficulties estimating the financial losses for breaches arising from

absence of security policy compliance or the estimating practices are different on the global territory.

5.2.5 Cultural and economic diversification

Mauritius is on the verge of a major undertaking, that of transforming the country into a “cyber island”. The government and the private sector are optimistically channelling their efforts in making ICT the 5th pillar of the economy (Business Park of Mauritius Ltd, 2004). Many developing countries have not had a similar development history as Mauritius, that is, developing from an agricultural based economy, to manufacturing, tourism, financial services and now to an ICT based economy. This is a very specific condition that is somewhat unique to Mauritius. It would be interesting to find how the Mauritian culture adapts to such challenges and how it views or implements information security over such diversification phases. It will be interesting to study security practices in a culturally and economically diversified country such as Mauritius. This can reveal certain realities that may be prevalent in such context.

5.2.6 Ethnicity & Literacy Levels

Mauritius may be small in size but it groups various ethnic characteristics together, contrary to some other developing countries. The population at large is composed of multi ethnic groups who have their origins from Africa, Asia & Europe (CSO, 2003). This is another attribute that is specific to Mauritius. There is also a high level of literacy in Mauritius as compared to other countries in Africa, Asia or Latin America. However, it would be interesting to research how these specificities differentiate Mauritius from other countries in the area of security and whether there is any correlation among these characteristics and attributes.

The differences that have been identified so far lay a strong ground for researching further in this area and especially in the local context. The differences and specificities identified motivate one to go to the root of the

subject matter so as to research and disclose findings on the local realities and contribute to the knowledge base of the security community. They strongly justify the need for researching along the lines stipulated above.

There is no doubt that the absence of relevant data on information security, compliance with policies, procedures and standards in Mauritius are strong motivators for undertaking such challenges. Hopefully, the findings will contribute towards elevating information security across organisations in Mauritius and helping the local security community to make a significant leap in this area while embracing the challenge of transforming this country into an ICT hub.

Consider Table 5-1 below which provides a summary of the commonalities and differences in information security practices between Mauritius and other developing countries.

Commonalities	**Differences**
Other developing countries as well as Mauritius have undergone information **security problems and breaches**. This seems to be a general problem nowadays.	**Absence of accurate and up-to-date secondary data** on information security practices in Mauritius as compared to other countries.
Information security is starting to gain management attention across levels and countries, although this is still slow in certain countries.	The **local investment behaviour differs** from other countries to a large extent when it relates to information security. Business projects tend to have priority on risk management projects in Mauritius. **The risk management culture is yet to be improved locally** as compared to the international arena.
Mauritius faces similar threats and risks as other developing countries. These threats and risks are not particularly related to geographical characteristics.	While one could note **an increase in the investment towards security training in the international scene**, such practices are not yet clearly apparent locally.

Commonalities Cont…	Differences Cont...
Information security policies and compliance problems have been noted across the world. These issues are not specifically associated with a specific country.	**It was possible to assess the direct financial impact of information security breaches** (due to absence of security policies & controls) that took place in Mauritius as compared to other countries. In the latter cases, this was not directly measurable.
	Though Mauritius is small in size, it nevertheless **has diversified cultural and ethnic characteristics** that are not generally common in the cases of other developing countries. Furthermore, **Mauritius enjoys a high literacy level** as compared to similar counterparts. These may have some correlation to information security practices in the local context.

Table 5-1: Information Security Practices - Comparison between Mauritius and other countries

5.3 Summary

While undertaking this chapter, it was possible to learn from the local findings and compare with cases reported internationally. There is no doubt that the context in which the local practitioners operate is different and may lead to different behaviours and practices as regards information security. While there are elements which are common to global findings, there are nevertheless certain concrete differences where solid information on security policies and practices is either lacking or inexistent in the local environment. The history of the economic development, social and cultural conditions is somewhat very specific to Mauritius. It therefore motivates one to find primary data (i.e., fresh data from survey) and undertake a study to explore further and confirm certain perceptions.

The next chapter will aim at setting the foundation to conduct a field study to support this dissertation and help in gathering primary data. The chapter will also set the scene on the research methodology and statistical tests to be conducted so as to confirm or refute hypotheses and perceptions that have been noted so far. Given the lack of information in the areas of security policies, compliance and practices in Mauritius, this field survey will be highly contributory to the

advancement of knowledge and information on information security in the local context.

Chapter 6:

Research Methodology

6 RESEARCH METHODOLGY

6.1 Introduction

In any research exercise, the availability of correct data and research methodology are mandatory for solving the problem under study. The credibility of the results derived from the application of such methodology is dependent upon up-to-date information about pertinent characteristics of the problem area. Data that is now known as information can be used and interpreted

In other words, neither a business decision, nor a government decision, nor a research conclusion can be made in a casual manner in the highly involved environment prevailing in this age (Mustafi & Rao, 2003). It is through appropriate data and their analysis that one can come up to the right conclusion and decision. Decisions and conclusions cannot be based upon mere perceptions but rather upon strong foundation of up-to-date facts and figures.

In the same frame of mind, this dissertation can only serve its purpose to the security community if it is backed by sound data and research methodology.

Following the investigations carried out in Mauritius at the level of academic institutions, government and relevant ICT bodies, it was found that there is a lack of information that could be used to support this research work. Given this absence of relevant secondary data in Mauritius in the area of compliance with IT security policy and standards, it has been decided that the best approach would be to gather afresh data from primary sources for analysis. In other words primary data will be collected from a population comprising the top 100 private companies operating in Mauritius. These companies are basically the most developed organizations and stand as the main drivers of the economy. Gathering fresh data directly from these sources will be very useful and contributory to this research. Though considerable effort will be needed to capture the right set of information from these sources, it is nevertheless justifiable to spend time and effort in undertaking this exercise for the welfare of the security community while serving the need of this research exercise.

6.2 Techniques for Data Collection

While initially it was planned that a questionnaire approach for data collection would suffice, the decision had to be revised, given certain local realities.

Following considerable reflection and discussions with past research students, it was noted that the best technique for a sound data collection in Mauritius would be to use a well-devised questionnaire to be filled in during an interview or phone conference session with the selected party. One must reckon that this method carries a number of advantages as well as drawbacks. However, the advantages of this technique outweigh the associated drawbacks and hence it is worth pursuing along this line. The main reasons for adopting this combined technique are:

6.2.1 Higher response rate

A high response rate is crucial when results have to be generalized to a larger population. Whether one makes use of face-to-face interviews, telephone interviews, or mail-in surveys for data collection, the aim is to maximize response rate. The lower the response rate, the greater the sample bias (Fowler, 1984).

It was noted that when a mailed questionnaire is used as an exclusive method for data collection, it often results in a poor response rate which in turn influences the correct analysis, interpretation and conclusion on the subject matter.

Many research students in Mauritius have witnessed situations where mailed questionnaires are either not responded to or simply not responded within the time limit. There is a high risk that responses obtained are insufficient for proper analysis and interpretation. Furthermore, the quality of data obtained may be poor due to absence of assistance and lack of adequate attention paid to time of response. Using a combined approach, that is, using an interview or phone conference session to fill in a formal questionnaire with assistance of the interviewer can guarantee a higher response rate and better quality of data. By arranging for on site meetings or phone conference sessions with the target group, there is a higher chance of obtaining sufficient data. This approach also allows for immediate clarifications to be furnished if ever required by interviewee.

6.2.2 Flexibility

Though it may be a time consuming approach, it however stands as one of the most flexible methods of obtaining data for research and analysis,

given that interview sessions can be arranged at the most convenient time and place of the respondent. This further opens the door for increasing response rate given it is being held at their convenience and without disrupting their professional plans. It is also envisaged that in certain cases, fact finding is done over the phone especially in the event where respondents are busy and can only spare a few minutes for such work. However, the questionnaire will stand as the underlying document to guide this investigation exercise in a structured manner.

6.2.3 Identity of respondents

The success of this research greatly depends on who is responding to the set of questions. With this approach, the identified targets are earmarked, contacted and surveyed during preferably a face-to-face session. Under such approaches, the identity of the person is confirmed while providing enough assurance that the respondent is effectively the person who is being targeted.

Sometimes obtaining information from anybody within a department or company may not be correct and may dilute the effectiveness of the research work. This risk can be mitigated by using the proposed approach.

Furthermore, it is prerequisite to reassure and provide enough comfort to the respondents that all information being collected will remain confidential and that no disclosure will be made publicly as to their identities. This is mandatory if one want to get an unbiased and fair view of the state of information security locally.

6.2.4 Structured Approach

The fact that the data collection activities will be guided by a formal questionnaire, it is very unlikely that one misses important data. The questionnaire will help to structure the interview and assist in obtaining the necessary information only. There is very little chance that one ends up losing time on unnecessary open and biased discussions since questions will be carefully selected to avoid such situations.

Furthermore, the questionnaire will be designed in such a way that respondents can reply to an organized set of questions pertaining to

specific areas at one time. During the document formulation exercise, one will aim at avoiding any overlapping, misleading or irrelevant questions that could eventually affect the survey. The logical and structured flow of questions will have to be tested with certain individuals before undertaking a full scale field survey.

6.2.5 Faster approach for data collection

One common problem with a questionnaire-exclusive approach is that the researcher is dependent on the respondents who may respond at various time intervals thereby lengthening the field study. With a mixed questionnaire/interview approach or assisted data collection method, the exercise is more likely to be completed within a defined schedule as plans can be set and followed upon so as to finish by a specific date. In fact the control of this process stays in the hand of the researcher.

6.3 Sampling Design, Process & Approach

Given that a complete enumeration or census exercise is unfeasible due to limited time and resources available for this research project, it has been decided that a sample representative of the population will be studied. Sampling is basically the process of inferring something about a large group of elements by studying only a part of it (IGNOU, 2002). The following parameters are key elements of the sample design:

6.3.1 Population

The population or target population is basically the group that a researcher is interested in and on which he or she wishes to draw a conclusion (Kothari, 1985).

The population, in this context, is composed of well-established private companies operating locally in various sectors of the economy. This population stands as the main driver of the Mauritian economy and has so far played a major role in the economical and social stability of the country. It can also be inferred, to a certain extent, that the welfare and progress of Mauritius in turn depends on the survival and success of this population group. If they are affected by security related risks, there is a high chance that the country is also affected.

The population comprises 100 private companies which are being taken from one of the most renowned business magazines of Mauritius “The Top 100 Companies” (Riviere, 2004). The magazine has, over the years, become a reference document of the economy. It is published annually, reporting performances of the private organisations of Mauritius. This magazine is the only documented source which holds company and performance related information on the private organisations in a readily and regular manner. It contains information on the board of directors, management and their respective roles together with their annual financial performances. The companies reported in the magazine are ranked in an order of size, profit and turnover. They are basically the most influential private organisations in terms both of economic and social input in the economy. Thus it stands as a reliable source of information in the local context and is being used as the baseline for the formulation of the proposed field work.

6.3.2 Probability Sampling

Probabilistic sampling was developed out of the need to guarantee representative samples. On the other hand non-probabilistic sampling techniques were developed mainly for situations where representativeness was not the most critical element. While in certain areas probabilistic sampling is the best technique to adopt, in other areas, non-probabilistic can be the most appropriate one.

More explicitly, a probability sampling method is any method of sampling that utilizes some form of random selection. In order to have a random selection method, one must ensure that a defined and systematic procedure is used so that the different units in the population have equal probabilities of being chosen.

Probability sampling is being chosen as the sampling type for this research as it will provide a sound framework for each element to be selected on an unbiased basis.

6.3.3 Sampling Methods

Among the various methods of probability sampling such as simple random sampling, systematic sampling, stratified sampling, quota sampling and cluster sampling, stratified sampling method is being retained.

Stratified sampling is probably the most appropriate sampling technique for this research. The requirements of a stratified sampling approach are:

(1) It should be possible to divide the population into non-overlapping groups having similar characteristics or attributes;

(2) Certain segments of the population can easily be representative of the overall group being studied.

Much research relies on this technique, particularly in survey designs. Simple random samples will then be drawn from each category (called stratum). The main reasons for choosing this technique are:

(a) It can be used as the population can be partitioned into smaller sub-populations, each of which is homogeneous according to a particular characteristic (Arsham, 2004). The sampling units will be categorised on the basis of the industry sector of which they form part.

(b) Stratification can significantly increase the statistical efficiency of sampling if applied correctly (Thompson, 2002).

(c) The fact that one of the hypotheses to be tested has a correlation with physiological characteristics, it will be an appropriate technique to study whether security practices are related to such characteristics;

(d) Stratification of the population will also allow drawing separate conclusions for each stratum; hence allowing a clearer interpretation of findings by industry.

(e) Stratified sampling allows the definition of strata based on the proportion to the size of the stratum in the population. Hence it will enable to group the sampling units proportionally as per the representation of the industry (proportional stratified sampling) in Mauritius.

6.3.4 Sample & Sampling units

As mentioned earlier, a complete census will be very costly and practically impossible to complete in a short span of time, so a sample of the population is being selected. A sample is simply a subset of the population (Aaker, Kumar, Day, 1998).

Basically it is the subject under observation and on which information will be collected for subsequent analysis and interpretation. In other words, it is the actual unit to be considered for selection. It may be an organization (e.g. financial, manufacturing company) or a person or individual.

In this present study, a sampling unit will be the company which forms part of the population and operates in an industry. Thus the companies will be the sampling units. These units will be grouped into strata based on proportional allocation criteria.

6.3.5 Sample Size Calculation

The size of the sample can be determined either using statistical techniques or through some ad hoc methods. Researchers make use of the ad hoc methods when they hold significant experience from which they can draw the sample size. However, for reliability reasons a statistical approach will be adopted to determine the sample size for this survey.

The sample size depends basically on 4 factors:

(a) the number of groups and subgroups within the sample that will be analysed;
(b) the value of information in the study and required accuracy of the results;
(c) the cost of the sample;
(d) and the variability of the population. The more the population vary, the larger the sample must be.

As justified in the earlier section, stratified sampling is being adopted to calculate the size of this sample.

The population is broken down into 8 strata of industry and based on their respective Gross Domestic Product's (GDP) contribution to the Mauritian economy.

Several researchers who are authors have published valuable guidelines in the calculation of sample size. According to statisticians like Thorndike, the minimum size for factor analysis should be ten times the number of variables to meet the criteria of statistical reliability. There is a widely-cited rule of thumb from Nunnally (1978) that the subject to item ratio (i.e. the ratio of the number of subjects per item in a particular analysis was calculated from the information given) for exploratory factor analysis should be at least 10:1. Gorsuch (1983) and Hatcher (1994) recommend a minimum subject to item ratio of at least 5:1.

When reviewing several studies in the computation of sample size, one can conclude that absolute minimum sample sizes, rather than subject to item ratios, are more relevant (Guadagnoli & Velicer, 1988). Based on this guideline, the sample size for this research was calculated.

An acceptable sample size has been worked out using the following attributes:

- a 10% margin of error is tolerated (this margin dictates the amount of error that can be tolerated);
- a 90% confidence level is being used (the confidence level is the amount of uncertainty that can be tolerated);
- a population size of 100;
- a conservative response distribution of 50% is being used.

An acceptable sample size of 41 has thus been obtained for this population with the use of Raosoft online tool (Raosoft, 2005). This is an acceptable size.

When computing the sample size, it is essential that one gets an acceptable response rate when using the stratum method. Otherwise, one cannot draw conclusions.

One should aim to get at least 50% to minimise the danger of non-response bias, while over 65% would be preferable (Saferpak, 2005).

Consider Tables 6-1 and 6-2 below which illustrate the respective industries, their contribution to the Mauritian economy and the sample sizes of each stratum.

Table 6-1 was compiled using MS Excel spreadsheet software. Secondary data, GDP information by industry, from reliable sources was gathered and tabulated to ease understanding (Mauritius Chamber of Commerce and Industry, 2003).

The population is being proportionally attributed to each stratum using GDP contribution, as represented below:

GDP Contribution by Industry (2003)

Industry	GDP Contribution (%)
Trade, Textiles & Manufacturing	31.5
Services	18.7
Transport & Communication	13.7
Tourism	9.8
Agriculture	7.2
Construction	6.2
Financial Services	5.8
Business Activities including IT	5.3
Other	1.8
TOTAL	**100**

Source Mauritius Chamber of Commerce and Industry (MCCI), 2003

Table 6-1: Industry Strata

Table 6-2 was also tabulated using MS Excel spreadsheet software. However, the calculation of sample size was done using a software tool (Raosoft, 2005).

Sampling Size Calculated based on Stratified Method			
Industry	**Strata**	**No. of Elements Per Stratum**	**Sample Size Per Stratum (based on proportion)**
Trade, Textiles & Manufacturing	1	32	13
Services	2	19	8
Transport & Communication	3	14	6
Tourism	4	10	4
Agriculture	5	7	3
Construction	6	6	2
Financial Services	7	6	3
Business Activities including IT	8	5	2
Other	N/A	1	**N/A**
TOTAL		100	**41**

N/A: Not Applicable (Ignored due to size of stratum)

Table 6-2: Sampling Size by Stratum (Proportional)

An acceptable sample size of 41 was obtained for the population. The respective stratum has been allocated a sample size based on the proportion of companies falling within each industry. This will be the targeted number of organisations from which a response to the questionnaire will be sought. The proportion allocation method is a very common procedure and has been chosen for its simplicity (Mustafi et al., 2003). The proportion allocation was conducted through basic arithmetic functions using MS Excel spreadsheet.

6.4 Hypotheses

While studying the subject matter in detail, a number of perceptions has cropped up. The following hypotheses are being formulated and will be tested during the subsequent stages of this research to confirm the perceptions.

6.4.1 Testing conformance to security standards

The null hypothesis (H_O) being:

"Mauritian organisations have implemented security as per established standards";

6.4.2 Testing presence and application of security policies

The null hypothesis (H_O) being:

"Mauritian organisations have properly defined and implemented security policies"

6.4.3 Testing compliance with security policies and procedures

The null hypothesis (H_O) being:

"Organisations are not systematically complying with or adhering to security policies and procedures in place";

6.4.4 Testing measuring practices of security KPIs

The null hypothesis (H_O) being:

"Mauritian organisations do not measure security KPIs";

6.4.5 Testing correlation between certain characteristics and security implementation/practices

The null hypothesis (H_O) being;

"There is no correlation between the respondents' experience in information security and the presence of security policies at their workplace".

6.4.6 Testing association between industry and security implementation/practices

The null hypothesis (H_O) being;

"There is a correlation between industry and security practices".

6.5 Hypothesis Testing

6.5.1 Nonparametric tests

The nature of data obtained through the questionnaire approach can best be analysed and tested using nonparametric tests.

Nonparametric tests are also referred to as distribution-free tests. Nonparametric tests do not require the assumption of normality or the assumption of homogeneity of variance. These tests are basically used to compare medians rather than means.

Nonparametric tests are being favoured for the following reasons:

(a) These tests are most suitable for analysing ranked, scaled and rated data as set in the questionnaire;
(b) These tests involve relatively fewer arithmetic computations as compared to parametric tests and are most likely to be applicable for surveys as this is being undertaken;
(c) These tests require no more or less restricting assumptions than the corresponding parametric tests;
(d) These tests can be used to provide reasonably good results even for small samples;

6.5.2 Statistical Tests

The following statistical tests will be performed on the collected data to test the hypotheses given above.

6.5.2.1 Binomial Test

Binomial test will be used to test the hypothesis as set in 6.4.1, 6.4.2, 6.4.3 and 6.4.4.

This is a statistical test referring to a repeated binary process such as would be expected to generate outcomes with a BINOMIAL DISTRIBUTION. A value for the parameter 'p' is hypothesised (null hypothesis) and the difference of the actual value from this is assessed as a value of ALPHA (Marsh, 1996).

Binomial test is best used when data is of nonparametric nature and where only two possible options exist such as True/False, Yes/No or 0/1 (Siegel & Castellan, 1988).
The answers to the questions pertaining to the above stated hypotheses are of this nature.

The main reasons for choosing binomial test are:

(a) there is only ONE variable;
(b) there is only ONE sample group being tested;
(c) the data is not normally distributed.

6.5.2.2 Spearman Rank Correlation Test

Hypothesis 6.4.5 will be tested using Spearman correlation test. The latter is used for the correlation test between two variables of nonparametric nature.

Spearman rank correlation is the nonparametric analog of the usual Pearson product-moment correlation (Dallal, 2000). This is a test for correlation between a sequence of pairs of values. Using ranks eliminates the sensitivity of the correlation test to the function linking the pairs of values. In particular, the standard correlation test is used to find linear relations between test pairs, but the rank correlation test is not restricted in this way (Long, 2003).

The Spearman's rank correlation technique will be used to test the correlation between the respondents' experience in information security and the presence of security policies at their workplace.

6.5.2.3 Chi-Square ($\chi 2$) Analysis and Test

To test hypothesis 6.4.6, Chi-Square test of independence will be used.

This test is used when the researcher wants to know whether an association exists between two or more variables in a given study (Aaker, Kumar, Day, 1998).

Given the nature of study and data, this technique is among the most common ones to test the above stated hypothesis (6.4.6). $\chi 2$ tests are nonparametric or distribution-free in nature. This means that no assumption needs to be made about the form of the original population distribution from which the samples are drawn while all parametric tests make the assumption that the samples are drawn from a specified or assumed distribution such as the normal distribution (Viswanathan, 2004).

6.6 Summary

Any research needs to be supported by appropriate methodologies for it to be effective. Moreover, statistical techniques form an integral part of any research project, without which the interpretation of outcomes might simply dilute the reality.

This chapter was formulated to guide the present research. The research methodology was defined, appropriate techniques were selected to support the survey and a number of statistical tests were used to test the hypotheses put forward.

The next chapter will be crucial as actual data will be gathered, coded, analysed and interpreted. It will be very enlightening, since several perceptions will either be confirmed or simply rejected. The outcomes of the survey will be tested using the approaches and techniques formulated in this chapter. It is very likely that the findings of the study will be helpful in understanding information security practices in Mauritius. Hence it motivates one to undertake the forthcoming chapter with all passion and dedication in understanding the realities.

Chapter 7:

Analysis & Interpretation

7 ANALYSIS OF FINDINGS

7.1 Introduction

The earlier chapter laid the foundation for the methodology of the research work to be conducted on the field, hypotheses tested, findings analysed and reported. The field work was initiated on the basis of guidelines described earlier.

The survey was undertaken over a period of almost 2 months when the sample group was contacted and information gathered. The technique of capturing data during a face-to-face meeting while using a structured questionnaire as supportive instrument has effectively helped in getting a better response rate and quality output. There was very little editing to be performed on the data collected, given the usage of structured questionnaire and very few open ended questions. The questionnaire that was used for the survey is appended (see Appendix A).

However, this exercise proved to be time-consuming as meetings had to be organized with the target persons and it was not always an easy exercise to get in touch with the most appropriate persons. It must be highlighted that the assistance of some local data collectors was sought in organizing meetings and gathering the necessary information from the target group. Their assistance was limited to field work, without which it would have been difficult to complete this exercise on time.

Furthermore, a common problem was also faced by the target group. Several of the respondents were not keen to fill in the questionnaire or respond to certain questions due to the topic it was addressing. It was felt that members of the organizations found it hard to disclose security related information. Despite these obstacles, it was possible to attain an acceptable level of responses.

The purpose of this chapter is to present the findings of the survey in an analytical form so that hypotheses can be tested and clear conclusions drawn. This chapter presents the findings in two parts; firstly an overview of the response analysis, followed by a series of statistical runs to test the results in line with hypotheses set.

The data collected through the questionnaire were coded and captured into spreadsheets for ease of classification. It was then computed and analyzed using statistical tools and software. MS Excel and Analyse-It were among the most common tools used for this exercise. These tools have greatly helped in the interpretation process of this research exercise. The working of these tools can be referenced online. MS Excel features and functioning can be found on Microsoft web site (Microsoft Corp., 2005). Statistical tests were conducted using the power of Analyse-IT software (Analyse-IT, 2005). This tool can be categorised among the best ones both in terms of diversity of tests possible and ease of use of the software. One can easily perform a variety of statistical tests such as Descriptive, Parametric, Non-Parametric, Anova, Correlation, Regression, Agreement, Diagnostic and Precision testing. The software is fully integrated with MS Excel thereby allowing easy transformation of collected raw data into statistical charts. Test results can easily be reported in various formats for analysis and interpretation.

7.2 Overview of Analysis

7.2.1 Response Rates

MS Excel was used to generate the Table 7-1. Out of 100 well-established private companies, an acceptable sample size of 41 was computed using Raosoft online tool (Raosoft, 2005). The calculation of sample size was based on the following parameters:

- 90% Confidence level
- 10% Acceptable margin of error
- 50% Response Distribution

While the confidence level indicates the amount of uncertainty that can be tolerated, the margin of error defines the amount of error that can be accepted in the present research. The percentages used for confidence level and margin of error may vary from research to research. However a 90% confidence level and 10% margin of error have laid the ground for making an acceptable conclusion on the population (Murphy, 2004). The

response distribution indicates the degree of split in responses. A conservative figure of 50% is being used as an unbiased representation of response distribution.

A response rate of 85% and a refusal rate of 15% were obtained as depicted in Table 7-1 below:

Description	Number	%
Population	100	-
Acceptable Sample Size	41	-
No.of Responses (Obtained)	35	85%
No.of Refused Responses	6	15%

Table 7-1: Response Overview

The overall response rate is acceptable for statistical analysis given it is higher than 65% (Saferpak, 2005). The overall response rate of 85% provides a comfortable foundation for statistical analysis and interpretation (NCES, 2005).

The refusals were mainly attributed to the nature of the topic being surveyed where certain companies were reluctant to disclose information on their security state.

7.2.2 Responses by Strata

Data that was gathered from the survey was coded and tabulated in MS Excel where the top hundred private companies were grouped into 8 industry strata. Column “No.of Elements Per Stratum” in Table 7-2 below was computed on the basis of GDP contribution of each stratum of the population to the Mauritian economy using MS Excel. Proportional sampling method was then applied to come up to the size of each stratum. The result of the proportional apportionment by stratum is shown in the fourth column “Sampling Size Per Stratum”. This was computed by using simple arithmetic functions in MS Excel. The number of response figures was obtained by using pivot table feature based on which a percentage of responses, column “% Obtained”, was derived using the percentage function.

Industry	Strata	No. of Elements Per Stratum	Sampling Size Per Stratum	Data Collection	% Obtained
Trade, Textiles & Manufacturing	1	32	13	13	100%
Services	2	19	8	5	63%
Transport & Communication	3	14	6	5	83%
Tourism	4	10	4	2	50%
Agriculture	5	7	3	3	100%
Construction	6	6	2	2	100%
Financial Services	7	6	3	3	100%
Business Activities including IT	8	5	2	2	100%
Other	N/A	1	N/A	N/A	N/A
TOTAL		**100**	**41**	**35**	**85%**

Table 7-2: Responses by Strata

While effort was made to attain a 100% response rate among all strata, it was nevertheless very hard to achieve. However, it was possible to attain the 100% responses for 5 strata out of 8 strata. The least response was recorded among the tourism industry with a rate of 50% which is the minimum acceptable response rate for a stratum. Members of this sector are relatively more focused in other areas of management such as customer service and service delivery rather than management of information security, which is one of the reasons explaining this shortfall.

7.2.3 Analysis of Respondents' Profiles

A MS Excel spreadsheet was used to compile and graphically present the results gathered on respondents' profiles. It came out that 91% of the respondents were male and 9% female as presented in Table 7-3 below. There is also a clear indication that most of the ICT positions are being held by males among the top hundred companies.

Gender	Respondents No.	Respondents %
Male	32	91%
Female	3	9%
TOTAL	**35**	

Table 7-3: Gender Analysis

Another interesting point which came out during this survey was that most of the respondents (60%) were among the 31-40 age group as presented in Figure 7-1 below and this is supported by the fact that the development of the local ICT market took place only 10-15 years back in Mauritius. These respondents could be considered as the most modern generation of ICT professionals.

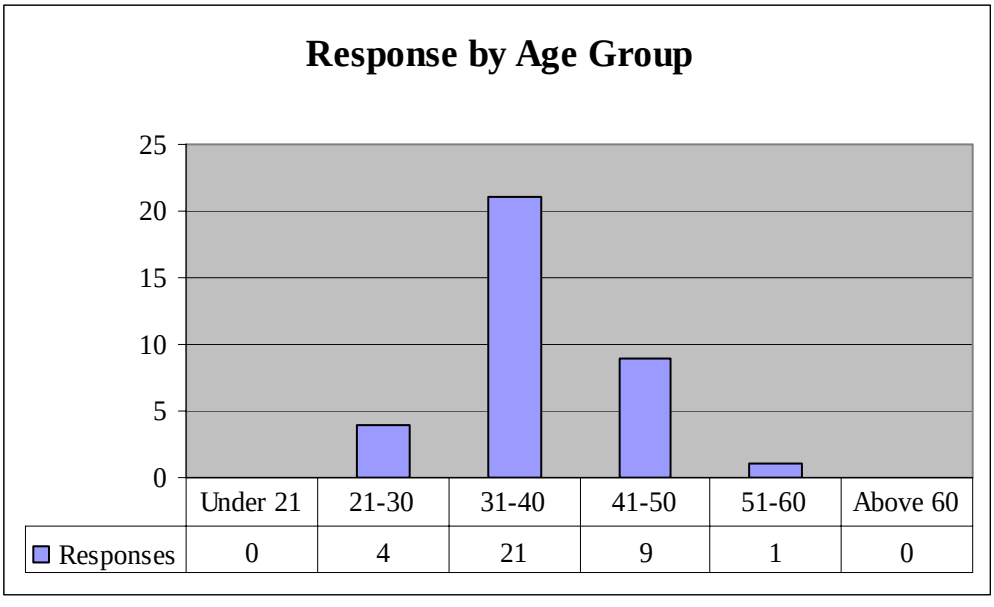

Figure 7-1: Age Group Analysis

Consider Figure 7-2 given below where most of the professionals that were surveyed held a managerial position (60%), i.e. including CIO, IT

Manager and Network & Systems Manager, or senior technical role (23%) such as Systems Administrator. The main objective of this survey was effectively to get the input from this target group so that a more realistic picture from the topmost sources of ICT management could be drawn.

Strangely enough, it could be noted that there was no respondent who was fulfilling the role of a Chief Security Officer. In fact the information security role was not common among organizations in Mauritius. Only 3% of the respondents confirmed having an information security position or function in their respective companies. This is a very low rate stating that organizations are not giving enough attention to security positions within their structure.

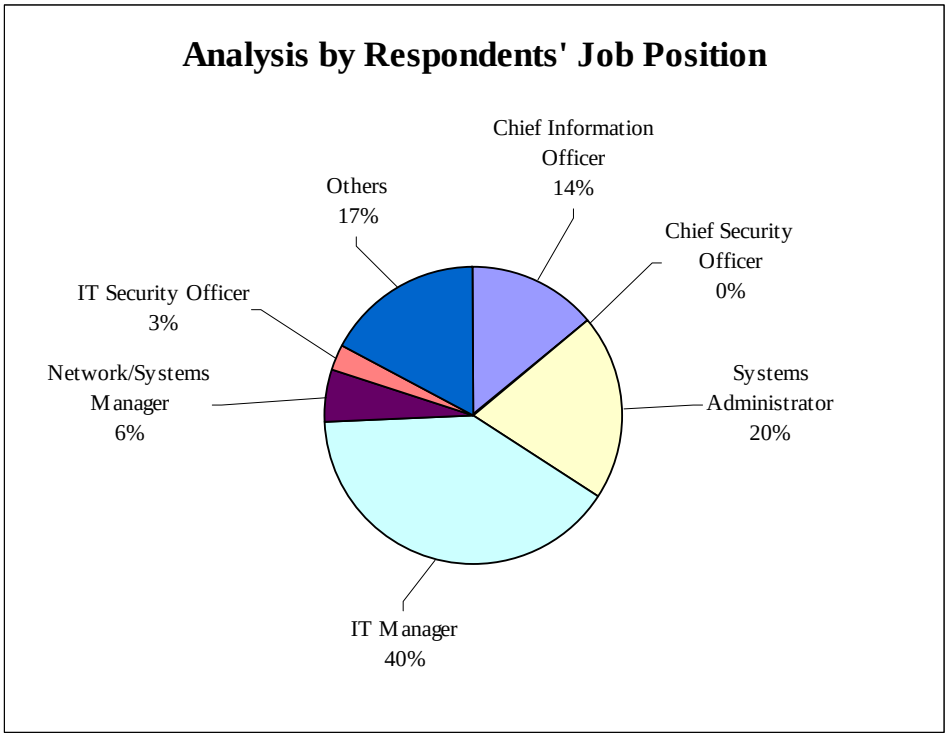

Figure 7-2: Role Analysis

7.2.4 Analysis of Information Security Practices in Mauritius

The analysis of information security practices in Mauritius was done by using MS Excel pivot table and chart features. Enlightening information was obtained in relation to information security practices. This is being categorised in the following areas of relevance to give the reader a comprehensive understanding:

(a) Information security policy: its presence, formulation and review;

(b) Education & training in information security;

(c) Measurement framework for the assessment of information security measures;

(d) Compliance with information security policies & procedures.

The findings on information security practices in Mauritius were alarming in certain areas. Each area will now be analysed in further details.

7.2.4.1 Information security policy: Its presence, formulation and review.

Figure 7-3 shows an analysis of the presence of information security in Mauritius as well as its formulation with regards to established standards. 26% of the respondents indicated that they did not have formal security policy in place. While 74% of the respondents stated that they had a formal security policy in place, 58% of them stated that their security policies were not compliant with established standards. The remaining portion of the respondents (42%) stated that their security policy adhered with established norms as shown in Figure7-3 below.

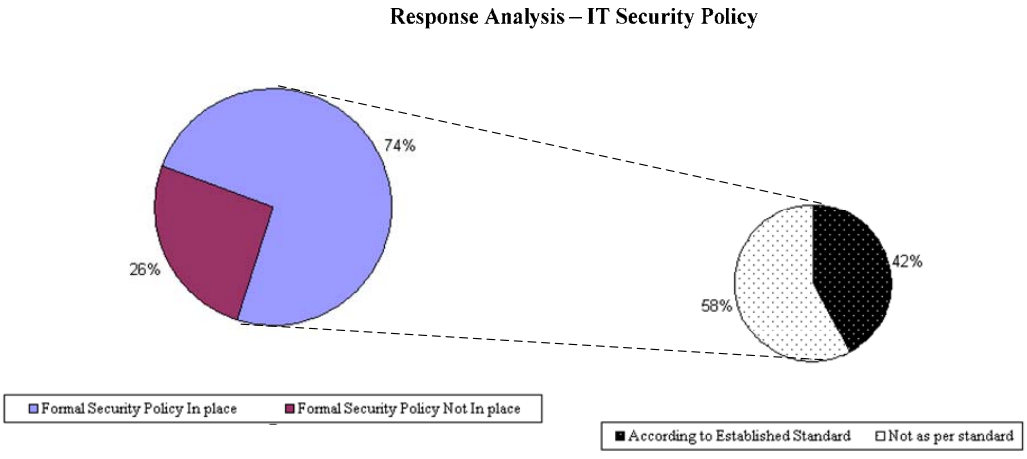

Figure 7-3: Analysis of IT Security Policy: Its Presence & Formulation

Following further analysis of the responses and examples given by the respondents, it was found that the above representation did not provide a realistic overview of the situation. **In fact only 11% of the organisations had effectively implemented well**

established security standards of the likes of BS 7799. While analysing the examples provided by the respondents in the questionnaire, it was clear that those who stated having well established policies in place (42%) simply provided wrong examples or had a misconception of security standards. Thus, it was confirmed that only 11% of the organisations had implemented security policies that were complying with international norms.

The high rate of non standard security policies is a matter of concern. It may prove to be risky since one cannot be sure whether all relevant areas of information security are properly covered. Furthermore, one cannot necessarily assess the effectiveness of their security policies in addressing all the relevant areas. There is no guarantee, at the very outset, that these organisations have a proper information security foundation since it seems that they have adopted ad hoc approaches to defining their respective information security policies. Having security policies is one thing, having properly defined and well-established security policies is another.

When analysing how information security policies are being formulated among Mauritian organisations, as presented in Figure 7-4 below, it can be seen that senior management is not involved in the process in a significant number of cases. Only 53% of the respondents confirmed the involvement of senior executives in the process of information security policy formulation.

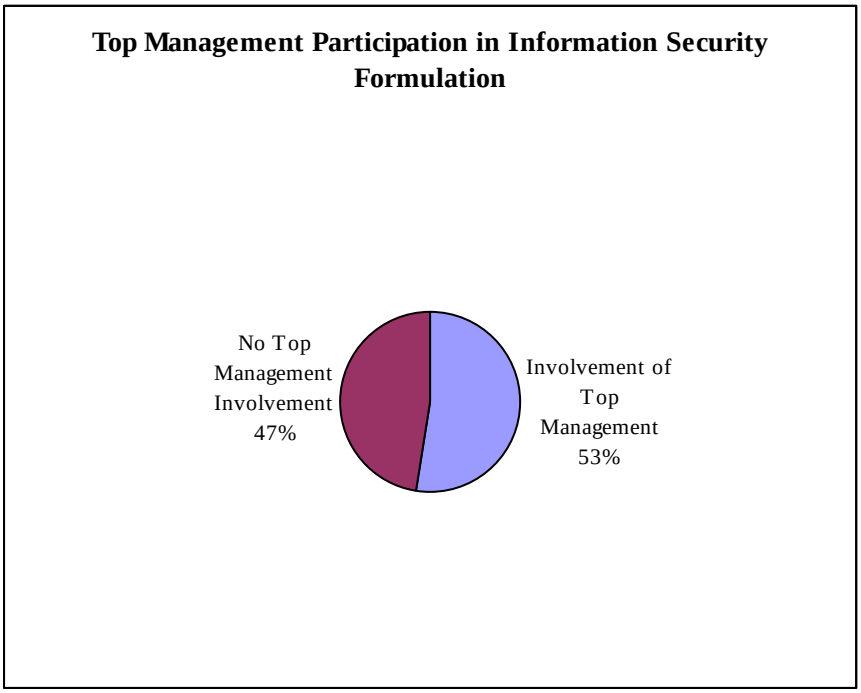

Figure 7-4: Analysis of top management participation in policy formulation

The absence of the top management participation in the overall process of policy formulation could be a major reason why information security policies are not according to established standards and are receiving little attention in areas of security policy application and review. Likewise the risk associated with such practices is that users may simply not pay any attention to security policies and their implementation or compliance since they are not being driven from the top.

The absence of senior executives' participation in the formulation of such policies also implies that a strategic activity of policy formulation and implementation is missing in a significant number of organisations. This can in turn impact on the overall operating processes of the organisations due to lack of top management control, thus leading to business risks.

On a different front as presented in Figure 7-5 below, one can note that there was a high rate of 57% of the respondents confirming that there was no formal process in place to review

their security policies and procedures while 43% confirmed having one.

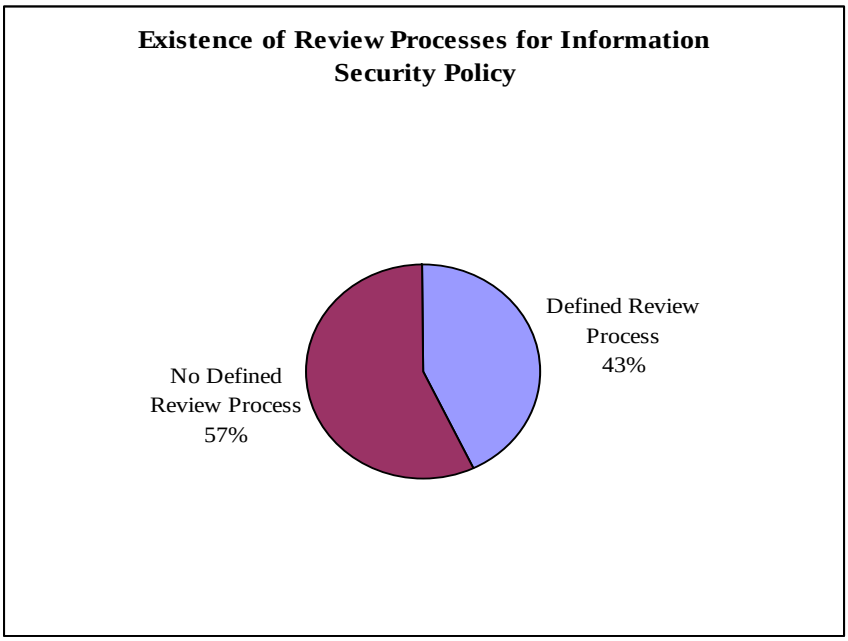

Figure 7-5: Analysis of the existence of review processes for information security policy

This also implies that the state of the security policy in place cannot be confirmed as effective and up-to-date. This again defeats the purpose of having information security policies in place if these are not regularly reviewed and updated. Threats are increasing on a daily basis and if one is not taking proactive measures to review the existing security policies and measures, one is bound to face associated risks which could be detrimental to one's organisation. Here management and auditors have a major role to play in ensuring that processes and/or systems exist to promptly identify such malpractices and that corrective actions are taken systematically to mitigate any associated risks.

7.2.4.2 Education & training in information security

As regards education in information security, it is noted that the majority of the respondents confirmed the absence of a well-defined security awareness program in their respective organizations as shown in Figure 7-6.

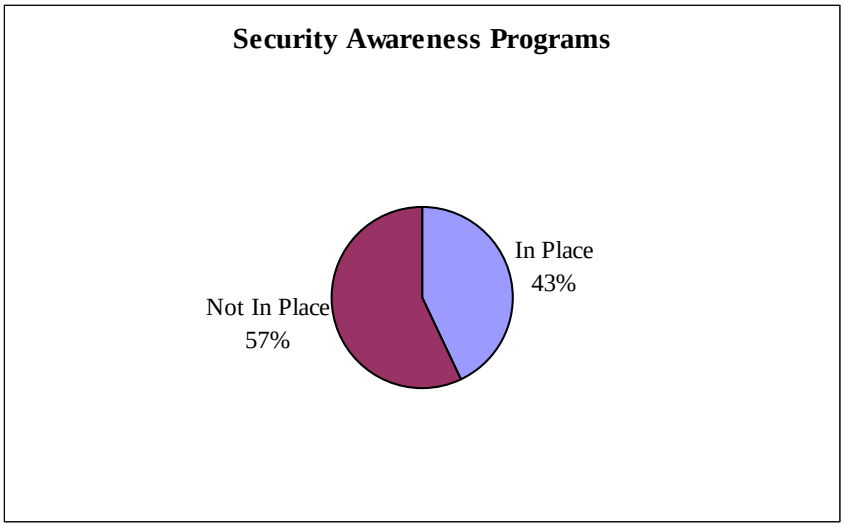

Figure 7-6: Analysis of existence of information security awareness programs

57% of the respondents confirmed that there were no such programs. It must be highlighted that information security projects can only be successful when all the necessary requirements such as framework, policies, procedures and training programmes are in place. The latter forms an integral part of any project. Without the support of proper security awareness programs, it will be almost impossible to succeed in mitigating security risks. This is one of the major factors that explain why companies in Mauritius are facing security problems and risks as stated earlier in this chapter.

In addition to the above findings, there was a high rate of respondents (63%) confirming a lack of regular training in areas of information security as shown in Figure 7-7 below.

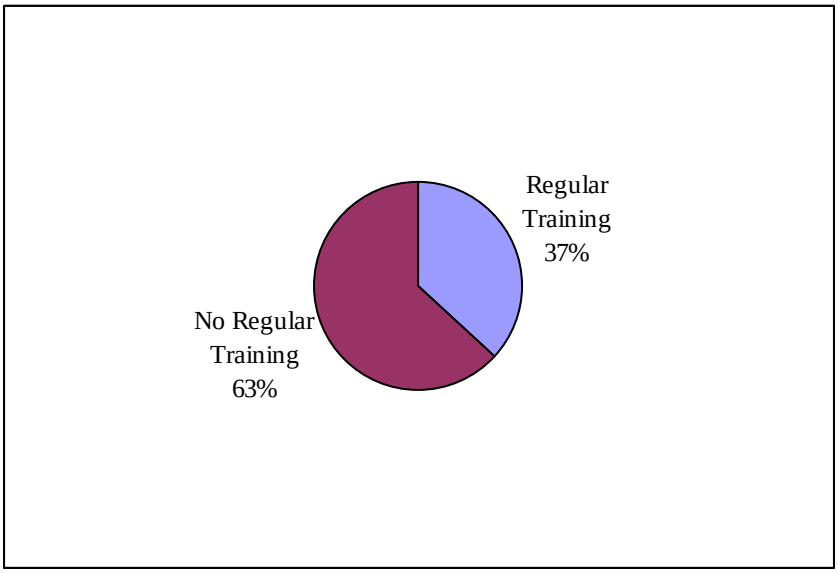

Figure 7-7: Analysis of training practices in information security

The fact that a significant portion of the respondents confirmed having no regular training in information security, it was very likely that the concerned organisations could face difficulties in combating security threats and risks since they were not well-equipped.

This in turn implies that top organizations in Mauritius are not investing enough in the development of their resources in areas of information security. This may eventually be detrimental to these organizations and put their existence at risk.

7.2.4.3 Measurement framework for the assessment of information security

Consider Figure 7-8 below. The majority of the participants (23 over 35 representing almost 66%) did not have any metrics or Key Performance Indicators (KPI) on the state, effectiveness and application of their information security policies.

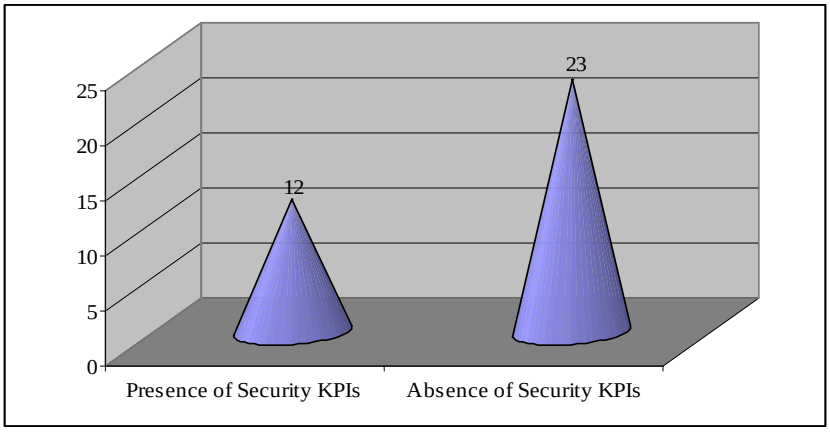

Figure 7-8: Existence of Security KPIs

Among those having security KPIs in place (34%), 20% of the respondents refused to give an indication of the indicators being used to monitor the effectiveness of their security policies. As regards the remaining 14%, it was noted that the security indicators were rather focused on measuring certain security incidents due to virus infiltration or access violation, but nothing concrete on the effectiveness of their security policies and measures, training campaigns and investment being made thereon.

Under such circumstances, it will be quite useful for organisations to monitor and measure the performance of their security implementation. The present situation does not allow the management to figure out the return on investment on security related projects. Not having such indicators can also mislead or create a wrong perception of the state of information security issues in the organisation.

7.2.4.4 Compliance with information security policies & procedures

As regards compliance with security policies, 43% of the respondents, out of those who were having security policies and procedures in place, confirmed that they were not systematically complying with the security policies and procedures in place as shown in Figure 7-9 below.

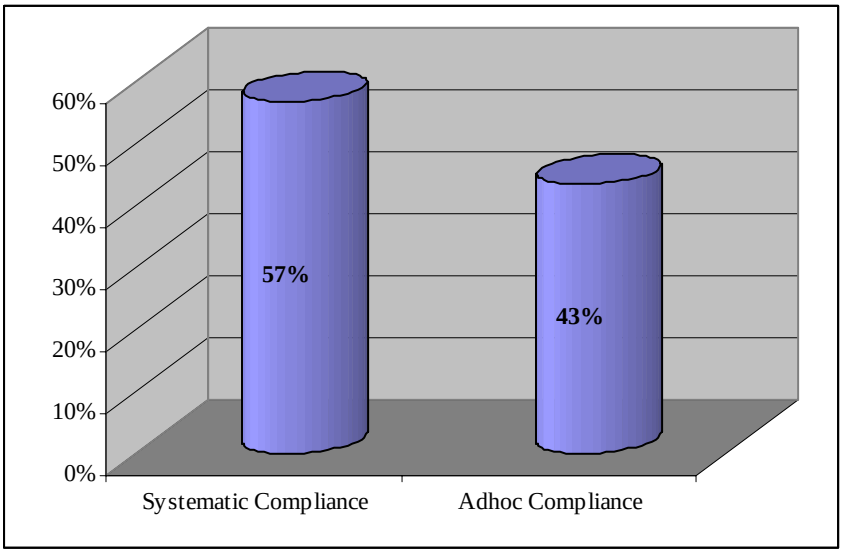

Figure 7-9: Analysis of compliance with information security policy

This rate is regarded as significantly high given the accompanied dangers and risks of ad hoc compliance with security policies and procedures. The best policies in place can easily fail if no one is adhering to them systematically. This finding supports the perception that Mauritian organizations are not systematically complying with security policies and procedures to a certain extent.

Consider Figure 7-10 as shown below. As mentioned earlier, it was also found that only 11% of the companies had effectively implemented established security policies such as BS 7799 and ISO.

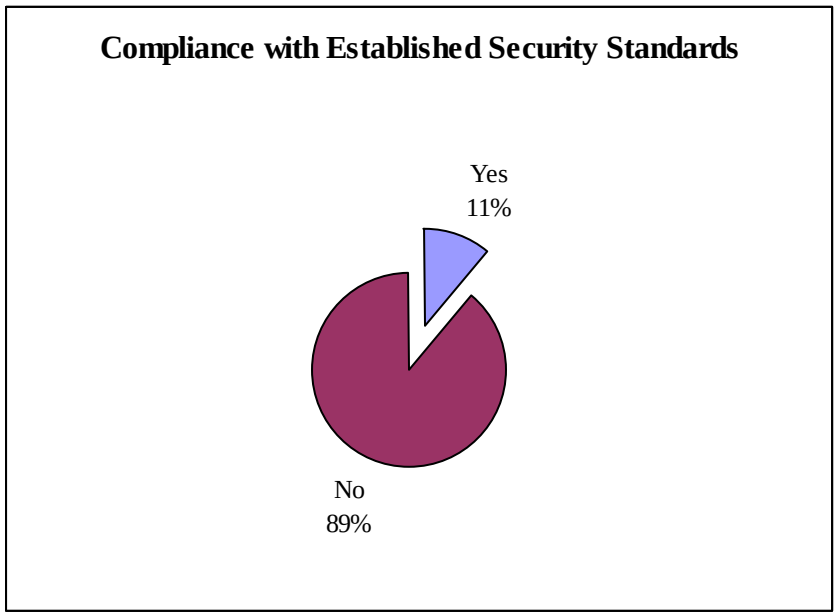

Figure 7-10: Analysis of compliance with information security policy

There is no doubt that there is a long way to go before reaching a stage where Mauritian firms can confirm that they have proper and effective security policies and procedures in place that could minimize their risk exposure. This low rate can also be explained by the fact that there is a large number of companies having poor or non-existing involvement of top management in information security strategy definition and policy formulation. There is a great need to raise the interest and attention of top management in this area so that proactive and corrective measures are put in place at the earliest possible time.

When analyzing the reasons why companies are not implementing/complying with established security policies such as BS 7799 and the like, a few, but common, responses were noted as represented below in Figure 7-11.

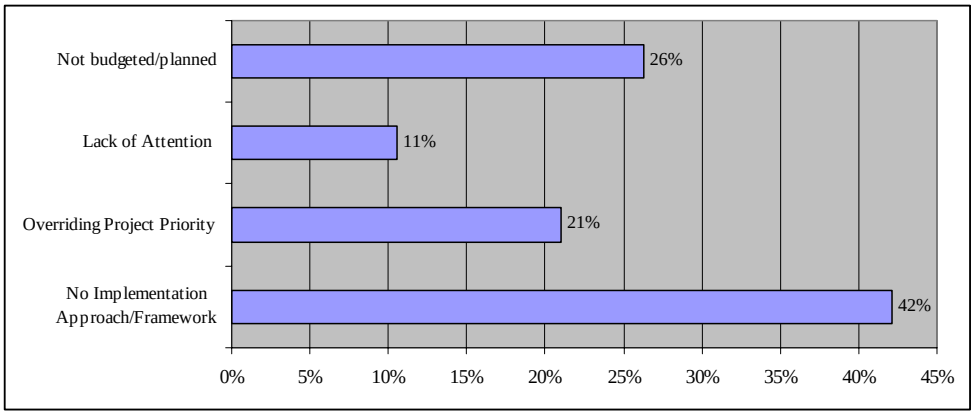

Figure 7-11: Analysis of reasons for non compliance with information security policy

Among those companies that confirmed having formal security policy in place, it came that very few have policies that are standard. The four main reasons why they have not complied with established stardards are:

(a) No implementation approach/framework

The majority of the respondents (42%) believe that they lack an approach and/or framework that will guide and facilitate the implementation process of a standard information security policy across the organisation. There is an indication that they do not really know how to go about it; reasons explaining why their existing information security policy are non-standard and used ad hoc.

(b) Overriding project priority

Another common reason for noncompliance with established security policies was earmarked. Basically projects other than security-related were receiving higher attention and priority within the organizations. Business and market related projects have so far obtained priority over this one.

(c) Not budgeted/planned

26% of the organizations reckon that they have not budgeted and/or planned the project of setting up a well-established and

standard information security till now. The investment has so far been driven towards operational projects.

(d) Lack of attention

11% of the respondents expressed a sensitive problem resulting in this noncompliance with established standards. There has been a lack of top management's interest in setting a standard security policy to the benefit of other projects. Revenue generating projects seem to receive more attention and priority of the top management among this group.

These responses give a clear indication that a comprehensive programme and framework will need to be put in place if there is an intention to address the situation. There is no doubt that implementing the right framework will not only act as a risk mitigation measure but also set the standards of operations in this fierce and competitive society.

7.3 Statistical Tests

Having analysed the responses obtained, it is now possible to conduct certain well-devised statistical tests to support the analysis conducted so far and confirm certain interpretations. Six hypotheses were enumerated in Chapter 6 and were meant to be tested in this chapter on the basis of the findings of the survey. The prime reason for conducting these tests was to confirm or refute certain perceptions on information security policies and practices. Despite having enlightened some of the doubtful areas in the previous section with concrete analysis, there is nevertheless a need to test these hypotheses by using appropriate statistical methods to strengthen the reliability of the interpretation.

The tests have been conducted with the help of a specialised statistical tool called Analyse-It by using data compiled in MS Excel spreadsheets (Analyse-IT, 2005). The variety of tests that it offers and the ease with which they can be performed is of great help to researchers.

7.3.1 Hypothesis Testing

7.3.1.1 Testing conformance with security standards

The null hypothesis (H_O) being:

"Mauritian organisations have implemented security as per established standards";

Test	Binomial test		
Alternative hypothesis	Response: No ≠ 0.5		
Performed by	O.Sookdawoor		
N	35		
	Have Implemented Security as per Established Security Standards		
Count	Response		
	No	Yes	Total
Total	31	4	**35**
Expected proportion	0.5		
Proportion	0.886		
95% CI	0.733	to 0.968	(exact)
p-value	<0.0001	(exact)	

Figure 7-12: Binomial Test on Hypothesis 6.4.1

Consider Figure 7-12 above. Binomial test was used to test the null hypothesis given above. This test is best used when data is of nonparametric nature and where only two possible options exist such as Yes/No as obtained for this question. It formally tests the difference between the proportion of categories in one sample against a hypothesised proportion (Siegel & Castellan, 1988).

Out of the 35 responses, it was found that only 4 respondents had implemented a security policy that complies with established standards while the remaining (31) did not have well established ones.

Researches often report a quantity known as the p-value as part of their research findings. A p-value is the probability of obtaining a value of the test statistics as extreme as, or more extreme than, that actually obtained given that the tested null hypothesis is true (Daniel & Terrell, 1995).

A **p-value** and a **confidence interval (CI)** are computed around the observed proportion (Armitage & Berry, 1994). A confidence interval of 95% has been used. The p-value and confidence interval both exploit the mathematical link between the Binomial and F- distributions and so are able to provide p-values with small and large sample sizes.

The interpretation of the result and decision of accepting or rejecting the null hypothesis depends on the **p-value**. A p-value of 0.05 is a typical threshold used in the industry to evaluate the null hypothesis (iSixSigma, 2005). Traditionally, researchers will reject a hypothesis if the p-value is less than 0.05. The general rule is that a small p-value is evidence against the null hypothesis while a large p-value means little or no evidence against the null hypothesis (Dallal, 2000). A p-value close to zero signals that the null hypothesis is false, and typically that a difference is very likely to exist (iSixSigma, 2005).

On the basis of the result of p-value (<0.0001) in the above test, the null hypothesis is unlikely to be true at the significance level used. It indicates that organisations have not implemented security measures as per established security standards.

7.3.1.2 Testing presence and application of security policies

The null hypothesis (H_O) being:

"Mauritian organisations have properly defined and implemented security policies"

Test	Binomial test
Alternative hypothesis	Response: No ≠ 0.5
Performed by	O.Sookdawoor

H_O: Mauritian organisations have properly defined and implemented security policies

n	35		
	Have properly defined and implemented security policies		
Count	Response		
	No	Yes	Total
Total	24	11	**35**
Expected proportion	0.5		
Proportion	0.686		
95% CI	0.507	To 0.831	(exact)
p-value	0.0410	(exact)	

Figure 7-13: Binomial Test in Hypothesis 6.4.2

Consider Figure 7-13 where another hypothesis is being tested by using Binomial technique given the collected data is again of non parametric nature with only two response possibilities. 24 respondents stated that they did not have properly defined and implemented security policies while 11 confirmed the contrary. This represents percentages of 69% and 31% respectively for absence and presence of properly defined and implemented information security policy.

A confidence interval of 95% has been used.

The computed p-value is 0.0410. Given the p-value is less than 0.05, the null hypothesis cannot be accepted at the chosen significance level. Hence it can be confirmed that there is a lack of properly defined and implemented security policies among Mauritian organisations. This is also supported by the results of the analysis exercise.

7.3.1.3 Testing compliance with security policies and procedures

The null hypothesis (H_O) being:

"Organisations are not systematically complying with or adhering to security policies and procedures in place";

Test	**Binomial test**
Alternative hypothesis	Response: Systematic Compliance ≠ 0.5
Performed by	O.Sookdawoor

H_O: Organisations are not systematically complying with or adhering to security policies and procedures in place

n	30		
	Systematic Compliance with Security Policy		
Count	**Response**		
	Yes - Systematic	Not - Systematic	**Total**
Total	13	17	**30**

Expected proportion	0.5		
Proportion	0.433		
95% CI	0.255	to 0.626	(exact)
p-value	0.5847	(exact)	

Figure 7-14: Binomial Test on Hypothesis 6.4.3

Consider Figure 7-14 where compliance behaviours are being tested using Binomial technique. The results were again compiled in MS Excel and tested using Analyse-It. Out of 35 respondents, only 30 stated having some form of security policies in place. Hence this test was conducted using the responses obtained from the relevant group of 30 respondents (n=30). 13 confirmed that they were systematically complying with their security policies

and 17 confirmed they were not. This represented 43% of systematic compliance and 57% of ad hoc and noncompliance with security policies.

A confidence interval of 95% has been used. The calculated p-value is 0.5847 for this hypothesis. Given the calculated p-value is larger than the threshold of 0.05, the null hypothesis cannot be rejected under these conditions.

One can therefore accept the statement supported by the null hypothesis for the chosen significance level and assert that Mauritian organisations are not systematically adhering to security policies and procedures in place.

7.3.1.4 Testing measuring practices of security KPIs

The null hypothesis (H_O) being:

"Mauritian organisations do not measure security KPIs";

Test	Binomial test
Alternative hypothesis	Response: Measure KPIs ≠ 0.5
Performed by	O.Sookdawoor

H_O: Mauritian organisations do not measure security KPIs

n	35		
	Measure KPIs		
Count	**Response**		
	Yes	No	**Total**
Total	12	23	**35**
Expected proportion	0.5		
Proportion	0.343		
95% CI	0.191	to 0.522	(exact)
p-value	0.0895	(exact)	

Figure 7-15 Binomial Test on Hypothesis 6.4.4

Consider Figure 7-15. The null hypothesis supports that Mauritian organisations do not measure security KPIs. 34% of the respondents confirmed that they were measuring their security KPIs while 66% confirmed not measuring such KPIs. Based on the computed p-value of 0.0895 using a confidence

interval of 95%, the null hypothesis can be accepted given the p-value is larger than 5%.

Thus one can conclude that local organisations are not measuring security KPIs on the basis of the parameters used above and result obtained.

7.3.1.5 Testing correlation between certain characteristics and security implementation/practices

The null hypothesis (H_O) being;

"There is no correlation between the respondents' experience in information security and the presence of security policies at their workplace".

Correlation test is being used for this case. It is a statistical technique which can show whether and how strongly pairs of variables are related; for example, establishing whether or not there exists a correlation between information security managers/practitioners' experience and presence of security policy at their workplace. In other words, is there any relationship between the years of experience of the respondents and implementation of security polices at their workplace? Testing this hypothesis will help to understand whether the respondents of a particular experience group(s) influence, in one way or another, the implementation of security policies at their workplaces. If a correlation exists, it will be interesting to establish the strength of the relationship.

The two variables in the hypothesis and between which the correlation test will be undertaken are:

- *the respondents' experience in security (X)*
- *presence of the security policy at the respondents' workplace (Y)*

Given that the data collected for these two variables are non parametric, Spearman's Rank Correlation technique is being used to

test the NULL hypothesis (Siegel & Castellan, 1988). Thus the data have been coded and ranked on the basis of their respective frequencies, ie, Rank 1 attibuted to the highest frequencies of the given variable, Rank 2 attributed to the second highest frequencies and so on. Where frequencies are equal, the rank has been averaged.

Consider Table 7-4 below:

	VARIABLES			
	Respondent's Experience in Security (X)		Presence of Security Policy at Workplace (Y)	
Experience in Security	Frequency (X)	Rank (X)	Frequency (Y)	Rank (Y)
Under 3 years	8	2.5	7	2
3-6 years	12	1	8	1
7-10 years	6	4	5	4
Over 10 years	8	2.5	6	3
None	1	5	0	5
TOTAL	**35**		**26**	

Table 7-4: Variable results (X) & (Y) for Spearman Ranks Correlation test

The responses that were obtained from the survey were tabulated in MS Excel using two pivot tables. The 1st pivot table provided the number of respondents by experience group as shown in column 2, “Frequency (X)”. The second pivot table provided the number of respondents that had security policy at their workplace by experience group. The results are shown in column 4, “Frequency (Y)” For instance when analysing the first row of data of Table 7-4, it can be noted that 7 out of 8 respondents had security policy at their workplaces and had an experience of less than 3 years in information security.

The frequencies for variable (X) and (Y) were then ranked as per Spearman Rank technique independently where rank 1 was assigned to the highest frequencies obtained, rank 2 to the second highest and so on. For example for variable (X), the experience group “3-6 years” had the highest frequency and thus was assigned rank 1. The subsequent ranks were then assigned on the same basis. As mentioned earlier, in

cases where frequencies are the same, an average rank has been calculated and allocated to the relevant experience group. For example, rank 2.5 has been allocated to experience group “Under 3 years” and “Over years” as they had similar frequencies(8)

	RANKS	
Experience in Security	**Respondent's Experience in Security (X)**	**Presence of Security Policy at Workplace (Y)**
Under 3 years	2.5	2
3-6 years	1	1
7-10 years	4	4
Over 10 years	2.5	3
None	5	5

Table 7-5: Ranked Data for Spearman’s Rank Correlation Test

Table 7-5, as given above, shows the respective ranks as obtained for the 2 variables (X) and (Y) by each experience group. For instance rank 1 was assigned to experience group “3-6 years” for variable (Y) as it had the highest frequency.

This table had to be prepared, on the basis of the results of Table 7-4 for the testing process. The values had to be tabulated in this format to adapt to the requirements of Anlayse-IT, the statistical software tool used for the Spearman’s Rank Correlation test. The columns 2 and 3 were used for the computation. The result that was obtained is shown in Figure 7-16 below.

analysed with: Analyse-it + General 1.71

Test	**Spearman Rank Correlation**
Alternative hypothesis	Respondent's Experience in Security (X) = Presence of Security Policy at Workplace (Y)
Performed by	O. Sookdawoor

n	5	
rs	0.97	
95% CI	0.66	to 1.00
p-value	0.0048	(t approximation, corrected for ties)

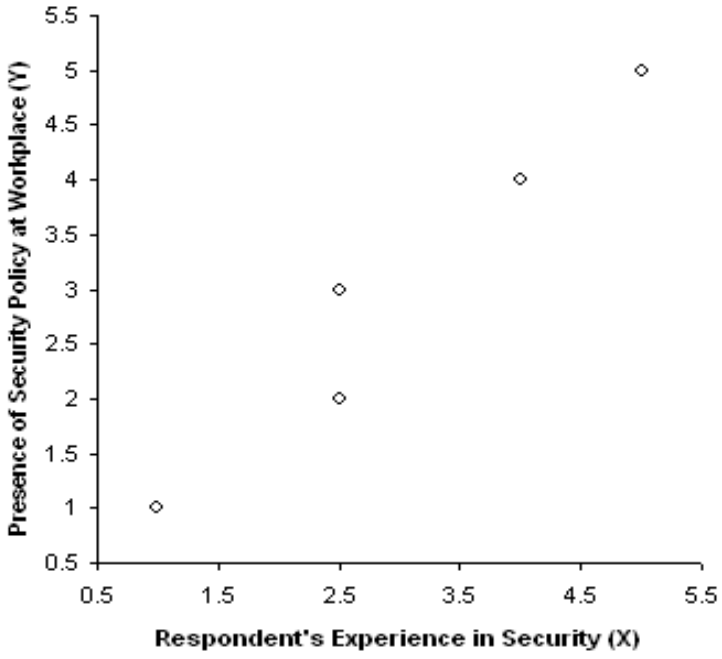

Figure 7-16: Results from Spearman's Rank Correlation Test

Consider Figure 7-16 as shown above. There were 5 cases (n) and a Spearman correlation coefficient was obtained for the two variables as given by **rs.** Spearman's Rank correlation coefficient is a technique which can be used to summarise the strength and direction (negative or positive) of a

relationship between two variables (Siegel & Castellan, 1988). A 95% confidence interval (CI) was again used.

The closer **rs** is to +1 or -1, the stronger the likely correlation. A perfect positive correlation is +1 and a perfect negative correlation is -1 (Box & Jenkins, 1976).

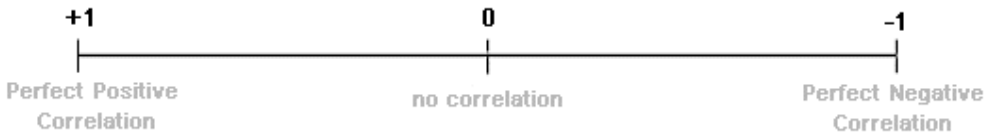

Figure 7-17: Correlation Values

The **rs** value of 0.97, as obtained above, suggests a fairly strong positive relationship between the two variables, that is, respondents' experience in security and presence of security policy at their workplaces.

This is also supported by the scatter diagram which depicts a positive linear correlation between the two variables.

Given these outcomes, it will be interesting to test the null hypothesis at a given significance level so as to determine whether the null hypothesis can be accepted or not. In this particular case, n = 5 and a 5% significance level is being used to determine the critical value of Spearman test statistics. The critical value is 0.800 when using these parameters (Daniell/Terrell, 1995).

Given the computed value of **rs** is equal to **0.97** and is greater than the critical value of 0.800 (at 5% significance level when n=5), the decision rule is to reject the null hypothesis at the 5% level of significance (Daniel, Terrell,1995). This is also supported by the p-value of 0.0048 which is very close to zero and less than 0.05 implying that the null hypothesis cannot be accepted.

Hence, it can be confirmed that a perfect positive correlation exists between the two variables, that is, the respondents' experience and presence of security policy at their workplaces. It can be concluded that experience in

information security has a direct bearing on the implementation of information security policy at the workplace. This has specifically been noted with the "3-6 years" experience group who are the main supporters of such practices.

7.3.1.6 Testing association between industry and security implementation/practices

The null hypothesis (H_O) being;

"There is a correlation between industry and security practices".

For the purpose of this test, security practices are based on whether organisations have defined and documented all the security requirements and policies. This demonstrates the level of commitment of the organisations to define and document all relevant security requirements and policies. This in turn indicates proper security practices in place.

The result obtained by industry with respect to this hypothesis is given below in Table 7-6:

		OBSERVED FREQUENCIES (O)	
Strata No.	**Industry**	**All Security Requirements and Policy are Defined & Documented?**	**All Security Requirements and Policy are Not Defined & Documented?**
1	Trade, Textiles & Manufacturing	10	7
2	Services	0	4
3	Transport & Communication	4	1
4	Tourism	1	1
5	Agriculture	2	1
6	Construction	0	0
7	Financial Services	2	2
8	Business Activities including IT	0	0
Total		**19**	**16**

Table 7-6: Observed frequencies by industry

Among the organisations that have responded to the survey, 19 of them have confirmed that all their security requirements and policies are defined and documented while 16 stated the contrary. These are compiled in the last 2 columns as grouped under the label "Observed Frequencies (O)". These were the data as obtained for each of the strata. For example, 10 organisations of the "Trade, Textiles & Manufacturing" (Stratum No.1) confirmed having defined and documented all the security requirements and policy while 7 stated the contrary for the same group.

For the purposes of this test, the results of strata 1 and 5 are being grouped under "Product-Oriented Industries" (non service oriented) and the rest of the strata have been grouped under "Service-Oriented Industries", given that their frequencies were less than 5 and will not meet one of the conditions of Chi-Square calculation (Viswanathan, 2004). The grouped strata also have common characteristics thereby making a logical sense to grouping them together. Hence the observed results, after grouping, will be as presented in Table 7-7 below:

	OBSERVED FREQUENCIES (O)		
Industries	**All Security Requirements and Policy are Defined & Documented ?**	**All Security Requirements and Policy are Not Defined & Documented?**	**TOTAL**
Product-Oriented	12	8	20
Service-Oriented	7	8	15
TOTAL	**19**	**16**	**35**

Table 7-7: Observed frequencies after grouping of certain strata

Table 7-7 above presents a summarised version of Table 7-6 where the results of the different strata have been grouped under two main strata as given in column labelled "Industries". Alongside these strata, the results from the respondents have been stated. For instance 7 service-based

organisations confirmed having the necessary security requirements and policy in a defined and documented format while 8 did not have these in place, as shown in row 2. The column labelled "Total" basically represents the sum of responses obtained from the respective sources.

Having compiled the observed/actual frequencies as obtained from the survey in the above tables, it is now necessary to work out the expected frequencies as per Chi-Square requirements. The calculated expected frequencies (E) are given below in Table 7-8:

	EXPECTED FREQUENCIES (E)		
Industries	**All Security Requirements and Policy are Defined & Documented ?**	**All Security Requirements and Policy are Not Defined & Documented?**	**TOTAL**
Product-Oriented	11	9	20
Service-Oriented	8	7	15
TOTAL	**19**	**16**	**35**

Table 7-8: Expected frequencies after grouping of strata in two main categories

Basically the computation of the Expected Frequencies (E) has been performed as follows:

The Expected Frequencies (E) for Product-Oriented stratum that have all the necessary security requirements and policy defined and documented = the total of the Observed Frequencies (O) as given in Table 7-7 for the same stratum (i.e. **20**) multiplied by the total of the column "All Security Requirements and Policy are Defined & Documented" (i.e.**19**) divided by the total of all observed responses obtained (i.e. **35**) thereby giving **11** (rounded) as Expected Frequency. The same logic is used to compute the values of E for the other corresponding cells such that the final frequency totals for O & E are same.

It is following this intermediate exercise that one can compute the Chi-Square Test of Independence for the given scenario.

The Chi-Square test of independence is given in Table 7-9 below:

	All Security Requirements and Policy are Defined & Documented ?		**All Security Requirements and Policy are Not Defined & Documented?**	
Industries	$(O-E)^2$	$x^2 = \sum\left(\frac{(O-E)^2}{E}\right)$	$(O-E)^2$	$x^2 = \sum\left(\frac{(O-E)^2}{E}\right)$
Product-Oriented	1.000	0.091	1.000	0.111
Service-Oriented	1.000	0.125	1.000	0.143
TOTAL		**0.216**		**0.254**

Table 7-9: Chi-square test of independence calculation

The results from the corresponding columns of Table 7-7 (for observed frequencies - O) and Table 7-8 (for expected frequencies - E) are used to compute the Chi-Square (X^2) value using the formulae given below:

$$x^2 = \sum\left(\frac{(O-E)^2}{E}\right)$$

For instance, value **0.091** (Table 7-9: 1st data row; 3rd column) has been obtained by subtracting **12** (Table 7-8: 1st data row; 2nd column) from **11** (Table 7-7: 1st data row; 2nd column), the result of which is powered by 2 and then divided by **11** (Table 7-7: 1st data row; 2nd column) for Product-Oriented stratum. The other figures have been computed by using the appropriate corresponding figures as explained above.

The sum of Chi-Square ($\chi 2$) calculated for the above values in Table 7-9, that is variables "All Security Requirements and Policy are Defined & Documented" and "All Security Requirements and Policy are Not Defined & Documented", is **0.470** (i.e. 0.216+0.254).

A 5% level of significance has been used for this calculation with a 1 degree of freedom. The critical value of $\chi 2$ at 5% level of significance for 1 degree of freedom is 3.84 as per Chi-square distribution table (Daniel & Terrel, 1995).

As the calculated value $\chi 2$ (**0.470**) is less than the critical value (3.84), the null hypothesis is accepted. Hence it can be confirmed that there is an association between industry and security practices in Mauritius.

7.3.2 Summary of Hypothesis Tests

Given that a series of hypothesis tests has been conducted by using different techniques as described above, it will be useful to present a summary of the findings. Table 7-10 below gives an illustration of these findings.

No.	Test	Null Hypothesis (H_0)	Statistical Technique Used	H_0 (Accepted - ✓) (Rejected - ✗)
1.	Testing conformity to security standards	Mauritian organisations have implemented security as per established standards	Binomial Test	✗
2.	Testing presence and application of security policies	Mauritian organisations have properly defined and implemented security policies	Binomial Test	✗
3.	Testing compliance with security policies and procedures	Organisations are not systematically complying with or adhering to security policies and procedures in place	Binomial Test	✓
4.	Testing measuring practices of security KPIs	Mauritian organisations do not measure security KPIs	Binomial Test	✓
5.	Testing correlation between certain characteristics and security implementation/practices	There is no correlation between the respondents' experience in information security and the presence of security policies at their workplace	Spearman Rank Correlation Test	✗
6.	Testing association between industry and security implementation/practices	There is a correlation between industry and security practices	Chi-Square Test	✓

Table 7-10: Summary of Hypothesis tests

7.4 Summary

The aim of this chapter was to highlight the key findings of the research work which was undertaken in Mauritius. Data was compiled, coded and tabulated in such a way that it could be used for analysis and interpretation. While in some cases simple two-dimensional analysis was undertaken, in other cases pivot tables were used to support elucidation. These techniques have helped the interpretation process of the sample data. Moreover, relatively more complex statistical tests were used with the support of specialized tools with a view to testing the hypotheses that were put forward. These tests helped in clarifying certain perceptions that were earlier formulated.

Among the different findings, one can note that a large majority of the organisations (89%) have not implemented properly defined information security policies that comply with established standards. The findings gave a clear indication that the level of information security practices is yet to be improved in Mauritius. Very few organizations have invested in the implementation of information security policies and procedures locally. Among those that have implemented security policies, it can be noted that a significant portion of companies is not complying with them systematically. When this was further analysed, it came out that a majority of them was facing difficulties in undertaking such projects, that is, they lacked the support of an approach and framework that could help them to implement and ensure compliance with established standards. This gap is felt among the majority of those who did not have proper security policies in place.

Bearing this in mind, there is a need to close this gap by devising an implementation approach/process and framework that can be used by organizations that do not know how to go about such projects. This should not attempt to replace any standards but rather complement to attain such goals. This can in itself be a project for future work.

The objective of the next chapter will be to recapitulate the main aim of this research work and questions that were put forward while specifying how this study has been able to address them. The findings as obtained during the research

will be used to conclude the state of information security practices in Mauritius as well as ascertain the main hypotheses. This will in turn contribute towards a more informed local security community.

Chapter 8: Conclusion

8 CONCLUSION

8.1 Introduction

This chapter is the last part of the research work. The research topic was challenging and required significant effort to meet the objectives set initially. The aim of this chapter is to present the findings in relation to the research work. An attempt at answering the relevant research questions will also be undertaken in this section.

Information security in itself is vast in scope and a single research project is barely enough to address all concerns of the community. While selecting the research topic, it was obvious that it should be one that can bring value to the local security community and specifically help in filling gaps in the area of information security practices. This was in itself a motivating factor in undertaking this challenge.

There were also certain perceptions on information security practices that necessitated an in-depth study so as to reach a valid and well-supported conclusion in the local context. Field work was thus undertaken so as to gather factual data that could serve in determining the acceptability of accompanying hypotheses. Relevant statistical tests were conducted on the data to support the interpretation exercise.

This chapter will thus highlight the main findings and conclusions while eliciting certain areas of future research work for the security community.

8.2 Research Overview

Mauritius is among the fast developing countries in Africa and is even being seen as a model player in certain areas by a number of countries. Diversifying from a sugar based economy to manufacturing, tourism, financial services and now to an ICT hub has been a great challenge. The focus of the current generation is to turn the country into the ICT model player in the region.

However, to support such initiatives, it is crucial that there is a general move across industries and companies in applying best practices in the domain area. Information security has been the main area necessitating focus and consolidation these days; that's the reason why this research was framed around this topic.

8.2.1 Research Aim

The aim of this research was to identify whether Mauritian organizations that are heavily dependent on IT have proper and reliable security policies in place which comply with international norms such as BS 7799 and the like.

Information security policies and procedures constitute as an underlying necessity for best practices, and also enables to secure organizational assets; another reason why the study specifically focused on this aspect.

Almost 90% of the companies that were surveyed were heavily dependent on IT. Among this group, several sets of data were collected and analysed. Today it can be confirmed that only 11% of the local organisations have implemented security policies that are compliant with established standards such as BS 7799. This in turn implies that the majority of the organizations are not complying with international norms but merely implementing ad hoc and not necessarily right practices.

Among those that had information security policies and procedures in place, there were nevertheless 43% of them that were not systematically complying with their security policies and procedures. The questions that were put in the research proposal for those that were not complying with international standards were:

(a) What are the implications?

(b) What are the business risks and exposures?

(c) What could be the impacts?

(d) What is the extent of deviation from these established norms?

The study, as it stands today, helps to respond to these questions. When it was noted that a great majority of the companies have not implemented well established and standard information security policies at workplace (89%), it gives an immediate signal that there is a need to draw the attention of the community on the implications, risks and possible impacts.

Typical implications, risks and impacts are:

- Danger of losing organizational assets whether in the form of material or data. While certain assets have monetary value, others are simply as valuable as the former ones. Data security is among those assets that require best practices and controls to ensure its integrity, confidentiality and availability. The absence of proper information security policies and procedures is simply an enabling factor for such risks to materialise; the impacts of which could be exponential nature. Some organizations might have to face severe financial losses while others losses their goodwill on the market.
- Organisations can easily end up having ad hoc and unstructured practices that are not conducive to business development and consolidation of their market position. Having non-standard policies and practices leave room for security threats to materialise more easily both from internal and external sources. Organisations can lose their competitive edge if such events occur. People recently witnessed the adverse impact of such risks at certain companies in Mauritius as expressed in the earlier chapters.

So what can be done to mitigate or contain such risks? The answer is obvious. Organisations in Mauritius will need to give information security the attention it deserves. Top management must steer such projects and invest towards safeguarding their assets by starting to adopt and implement best practices. In the same way as someone will insure their property and motor vehicles to protect them against certain risks to avoid

losses, one needs to adopt similar attitude and practices towards information security. Adopting, implementing and continually reviewing the right set of information security framework and policies constitute an insurance for the organization in general.

Business drivers will need to ensure that investment in such projects is budgeted consistently as for any other items if they really want to make a difference.

The change required in the local environment revolves around the culture and belief in information security standards and practices. This needs to flow from the top to the bottom of the organization if the intention is really to make Mauritius the ICT hub of the region.

When one sees that only 53% of the respondents' top management were involved in such projects, 63% of the respondents stating lack of training in this area and 66% not measuring security related performance indicators, then a significant turnaround programme needs to be undertaken in the local community if one wants to succeed in risk management.

A change in attitude, culture and belief with sustained motivation to adopt best practices will definitely enhance the present state of information security issues locally. Researches, security institutions, government bodies and the like will need to synergize and engage in programmes that can help in transforming the present mindset to get information security in the agenda of all organisations. However such efforts must be dispensed towards adopting best and standard practices rather than confining to basic and ad hoc procedures.

It was also found that 42% of the respondents do not really know how to go about implementing such projects within their organisations; a reason why they believe standard security policies and procedures have not been implemented.

Though several approaches exist such as BS 7799 implementation framework & IMSM, a need for a supplementary and complementary approach/framework can add up value in the process for the local

community. Such process or approach should take into account the cultural aspects and practices of the local organisations so that it easily adapts to their needs and management philosophies.

Another set of questions was put forward in the initial chapter; questions that were specifically directed to those cases that were conforming to international norms, that is, companies having information security policies as per established standards. A coherent analysis was meant to be made under the following key areas:

- **How far their implementation is reliable and complies with norms and standards (Ex ISO 17799, etc)?**
- **What is their general risk exposure?**
- **What improvement can still be made over the long run?**

Today, the findings demonstrate that only a small group of organisations (11% of the population) have adopted and implemented policies as per established standards. But how far the implementation and compliance are reliable for organisations that have adopted them? Though there are 11% of organisations that have implemented international standards such as BS 7799, there is nevertheless certain work that still needs to be undertaken to improve further.

Among this small group, one out of the four respondents stated that the organizations are not complying to it systematically. Complying with such policies on an ad hoc basis carries the same risk as those that simply do not have such policies in place.

Furthermore, again one out of four organisations confirmed the absence of key performance indicators as well as lack of regular training in information security.

Typical risks as elicited above, such as incurring financial losses due to loss of organizational assets, data, goodwill and market share exist for companies that simply adhere to the policies on an ad hoc basis. Not measuring the effectiveness of security implementation on a regular basis

can prove to be as dreadful as not having security in place. Accordingly, not investing towards security training can be very hazardous for an organisation that may have invested massively in its business.

There is no doubt that for information security to be successful, there is a strong need to fully and systematically comply with the established policies.

Therefore the concerned organisations have to embrace another challenge of ensuring the established information security policies are adhered to systematically by all stakeholders, the performance of information security programmes consistently being measured and getting the top management to drive the implementation and review process on a continual basis.

An organisation and its assets can never be safe if security policies are not complied with. Coupled to it, organisations must implement proper systems, controls and metrics to record, assess and measure the effectiveness of information security programmes. This should be included as part of the management dashboard. Investment towards information security training should be given similar interest as for training in any other business areas. Learning the right way of doing things can only help to better the operations and safeguard the organisations' assets.

Again top management has a crucial role to play in these situations. As part of good governance principles, top management must ensure that these issues are in their agenda. Measures should be put in place to ensure established policies are systematically being adhered to and that the effectiveness of their implementation is being assessed. Efforts should be dispensed towards getting the stakeholders to understand the implications of having a halfway implementation of an information security framework. Regular security workshops and seminars could help in reshaping the organizational culture towards a more security-conscious organisation. It is only under such circumstances that the interest of all stakeholders can be protected.

Hence there is a need to sustain effort towards compliance, reviews, audit and training programmes so as to reap full benefits and returns from such projects. Management has an important and yet mandatory role to play in ensuring such elements are not left aside at the expense of other business related projects.

8.2.2 General Perception on Information Security in Mauritius

There was a general unsubstantiated feeling that there was no adherence to standardized security policies in Mauritius. This research has confirmed that this is true based on the outcomes of the data analysis and statistical test. 11% of the organisations have implemented standard information security policies, 9% fully adhering to them. However, this is regarded as very low especially for a country like Mauritius which has as ambition to become the model player in the African region. There is no doubt that the stakeholders have a long way to go in transforming this reality.

In support to the above generalised perception, other hypotheses were set forward and statistically tested with the collected data. The following facts can now be confirmed:

- *Organisations in Mauritius lack properly defined and implemented security policies;*
- *Local private organisations are not systematically complying or adhering with security policies and procedures in place;*
- *Mauritian organisations are not measuring security KPIs;*
- *There is a strong positive correlation between the respondents' experience in information security and the presence of security policies at their workplace;*
- *There is a correlation between industry and information security practices in Mauritius.*

Again these become key pointers for the local security community to learn and address in a very near future if the aim is to become the model in the region while safeguarding the organisations' existence.

8.2.3 How Mauritius differs from other countries?

This question was also set as part of the research objectives initially. Following the background study conducted internationally and locally, one now has a comparative view of practices in the area of information security.

Basically there was an absence of secondary data in Mauritius to support the comparative analysis. With this research this gap has been filled.

Most developing countries are injecting significant finance and effort in information security and are being supported by increasing commitment from their top management (Deloitte & Touche & Tohmatsu, 2004). The same commitment is not felt in Mauritius in the information security area.

Based on global findings, it could be noted that major developing countries are sustaining their investment in security awareness programmes and skill development. 63% of the Mauritian respondents admit they lack such training.

A unique attribute has been found with Mauritius. Many developing countries have not had a similar development history as Mauritius, that is, developing from an agricultural based economy, to manufacturing, tourism, financial services and now to an ICT based economy. This is a very specific condition that is somewhat unique to Mauritius.

There is also high diversification of culture and ethnic characteristics in Mauritius as compared to some other developing countries. There is also a high level of literacy in Mauritius as compared to other countries in Africa, Asia or Latin America. These stand as comparative characteristics for Mauritius vis-à-vis other developing countries.

To sum up this section factually, Table 8-1 below provides a clear comparison of security practices between Mauritius and the rest of the world.

Findings in relation to information security policies and practices	**Rest of the World**	**Mauritius** Note4	**State & (Gap)** Note5
Do not Review/Measure IT Security Policy	60% Note1	57%	Better
Compliance with in place security policy	50% Note1	43%	Poorer (7%)
Top management involvement in information security related projects	56% Note1	53%	Poorer (3%)
Presence of documented security policy in place	59% Note2	54%	Poorer (5%)
Security programmes in place	50% Note2	43%	Poorer (7%)
Absence of information security KPIs	66% Note3	66%	Same
Access to information security training	50% Note3	37%	Poorer (13%)

Table 8-1: Summary of survey results

Note1: Based on Research conducted worldwide by CSO Research 2004

Note2: Based on Research conducted in UK by DTI 2002

Note3: Based on Research conducted by Deloitte Global Security Survey in 2004

Note4: Based on Research conducted as part of this dissertation

Note5: Comparing the state of information security practices and gaps between Mauritius and the rest of the world. "Poorer" implies that the state of information security policies and practices in Mauritius is poorer than the rest of the world. "Better" implies that the state of information security policies and practices in Mauritius is better than the rest of the world. "Same" implies no difference in information security practices. The gap that exists between Mauritius and the rest of the world is indicated in bracket.

Table 8-1 above clearly highlights that the state of information security policies and practices is poorer in almost all areas when comparing Mauritius with the rest of the world. Gaps also exist in the majority of cases when comparing with the international surveys. While in some cases the extent of variation is high, in other cases it is fairly low. In areas where Mauritius has poorer information security practices, efforts must be made urgently to at least reach the stage in which the developing countries are, but with a further objective of realising better practices in the near future.

8.3 Future Research

The present research was of a limited scope in which it was not possible to address all concerns of the security community. However, the findings as obtained in this study have enlightened everyone in such a way that it is now easy to earmark areas of improvement and those necessitating immediate actions on behalf of every stakeholder. From a research perspective, there is still room to devise a supportive approach or framework that can complement existing ones so that Mauritian organisations can easily implement those established standards. The easier and more accessible such processes are, the more people will go for them. This is simply not a statement but rather a fact since almost 42% of the respondents highlighted that they do not know how to go about implementing standards security policies and practices; an adaptive process or approach or framework to the local context can help to alter the situation along with a change in management's attention, interest, commitment and practices in information security related projects.

This is an area of future work which can be undertaken as a separate research project.

8.4 Summary

To sum up, this research aims at contributing to the improvement of information security practices in the local context. However, it can also serve as a basis to enlighten the security community of other territories so that stakeholders may make the most out of it and help everyone to improve further.

In general, the following ingredients are required by local organisations to bring the present state of information security policies and practices to an enhanced level:

- A need for standard information security policy that has as objective to properly reflect the business goals;
- A need for clear management commitment and support in undertaking such projects for the welfare of the organisations, economy and community;
- A need for proper distribution, sustained education and guidance on security policy to all employees and parties involved in the organisation;

- A need for a sustained awareness campaign to draw the attention of all employees and stakeholders on the risks associated with lack of proper security practices;
- A need for a comprehensive strategy on security risk analysis, risk management and security requirements;
- A need to shape up the attitude, culture and management practices of all stakeholders towards information security;
- A need for an approach to security implementation which is consistent with the organization's own culture;
- A need for a comprehensive measurement system to evaluate progress, performance and effectiveness of security implementation;
- A need for a sound review and control structure to act as guardians to ensure systematic compliance with standard information security policies and practices;
- A need to compensate or reward best practitioners of and good initiative taken towards information security fairly.

With these in mind, everyone can give a helping hand to better the state of information security across the world.

Appendix

A. Questionnaire

QUESTIONNAIRE

"*An Investigation of Information Security Policies and Practices in Mauritius*"

Research

In

MAURTIUS

2005

Confidential

Introduction

- **Questionnaire**
  - *Questionnaire completion will take around 30 mins;*
  - *All information collected will be presented in an analytical manner thereby not disclosing any company specific information that could affect the organisation's goodwill;*

Section A: Basic Personal Information

For each of the questions below, please tick (✓) the appropriate one.

1. **Please specify your gender group.**

   Male [ ]
   Female [ ]

2. **Which of the following corresponds to your age group?**

   Under 21 [ ]
   21-30 [ ]
   31-40 [ ]
   41-50 [ ]
   51-60 [ ]
   Above 60 [ ]

3. **Which of the following reflect most your current your job profile/ title/ role?**

Chief Information Officer	[ ]	IT Manager	[ ]
Chief Security Officer	[ ]	Network/Systems Manager	[ ]
Systems Administrator	[ ]	IT Security Officer	[ ]

   Other (Please specify) _____

4. **For how many years have you worked in the IT sector?**

   Under 3 years [ ]
   3-6 years [ ]
   7-10 years [ ]
   Over 10 years [ ]

5. **For how many years have you worked in IT Security related projects/assignments?**

   Under 3 years [ ]
   3-6 years [ ]
   7-10 years [ ]
   Over 10 years [ ]
   None [ ]

Section B: Company Background

For each of the questions below, please tick (✓) the appropriate one.

6. Which of the following categories describes best your organisation's activity?

Manufacturing	[ ]	Banking/Finance	[ ]	Health	[ ]
Insurance	[ ]	Education	[ ]	Retail	[ ]
Communication	[ ]	Travel & Tourism	[ ]	Services	[ ]
Transport	[ ]	Other (please specify) _____			

7. How many employees does your organisation employ?

Less than 25	[ ]
25-50	[ ]
51-100	[ ]
101-500	[ ]
More than 500	[ ]

8. How many IT Professionals work in your company?

Less than 5	[ ]
5-10	[ ]
11-20	[ ]
More than 20	[ ]

9. How would you rate your organisation's dependence on IT?

Very High	[ ]
High	[ ]
Low	[ ]
Not at all	[ ]

10. How would you rate the level of IT literacy in your organisation?

Very High	[ ]
High	[ ]
Low	[ ]
Poor	[ ]

11. How would you rate the level of IT Security measures in your organisation?

Very High	[ ]
High	[ ]
Low	[ ]
Poor	[ ]

Section C: Security Policy

For each of the questions below, please tick (✓) the appropriate one.

12. (a) Does your organisation have a formal IT Security Policy in place?

Yes [ ] No [ ]

(b) If yes, when was it first introduced in the company?

Recently (0-3years) [ ]

Long time back (for more than 3 years) [ ]

Don't know [ ]

13. Has your security policy been defined according to an established standard?

Yes [ ] No [ ]

If yes, which one? _____

14. Were appropriate parties involved in the development of the security policy?

Yes [ ] No [ ]

If yes, provide a list of stakeholders involved in the development of the security policy?

_____

15. Is there a defined review process for the security policy in your organisation?

Yes [ ] No [ ]

If yes, what are the key elements that you review?

_____

Section D: Organisational Security Practices

For each of the questions below, please tick (✓) the appropriate one.

16. (a) Is there a formal forum or structure in place to oversee and represent information security in your organisation?

Yes [ ] No [ ]

(b) If yes, what is the frequency of meetings?

Weekly [ ] Monthly [ ] Quarterly [ ] Yearly [ ] Ad hoc [ ]

17. Are comprehensive security awareness programs in place?

Yes [ ] No [ ]

18. Does the organisation provide regular and structured training to its employees on information security & policy?

Yes [ ] No [ ]

19. Is there a defined process in place to coordinate the implementation of information security policy, measures and programs?

Yes [ ] No [ ]

20. Are all relevant security requirements and policy specifically defined and documented in your organisation?

Yes [ ] No [ ]

21. (a) Are there specific key performance indicators or metrics in place to measure the success of and compliance with security policy in your organisation?

Yes [ ] No [ ]

(b) If yes, what are those key performance indicators? Please specify.

_____

22. Are responsibilities for accomplishment of information security requirements and programs clearly defined?

Yes [ ] No [ ]

23. (a) Is there an overall security officer in charge of information security?

Yes [ ] No [ ]

(b) If yes, to whom does this person report to? Please specify.

_____

24. Has a capability been established that provides specialized information security advice to the organisation?

Yes [ ] No [ ]

25. (a) Has an independent review of information security practices been conducted on the feasibility, effectiveness, and compliance with written policies?

Yes [ ] No [ ]

(b) If yes, when was it conducted?

This year [ ] Last year [ ] In the past [ ]

Section E: Compliance

For each of the questions below, please tick (✓) the appropriate one.

26. (a) Does your organisation comply with its security policy and procedures?

Yes [ ] No [ ]

(b) If yes, how would you qualify compliance with the security policy, requirements and procedures in place in your organisation?

Systematically compliant [ ]
Compliant on an ad hoc basis [ ]

(c) Does the security policy in place comply with established security standards such as BS 7799?

Yes [ ] No [ ]

(d) If your organisation does not comply with established security policy, are there specific reasons hampering its compliance? Please specify.

_____
_____

List of References

1. AAKER, D.A., KUMAR, V., DAY, G.S., 1998. *Marketing Research*, John Wiley & Sons Inc.

2. AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, 2002. *SAS70 Auditor's Report.*

3. ANALYSE-IT SOFTWARE LTD, 2005. [Online]. Available from http://www.analyse-it.com/ [Accessed on 29th June 2005].

4. ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE (ACSAC), 2003. *Themes and Highlights of the New Security Paradigms Workshop 2003, IEEE Computer Society.*

5. ARMITAGE, P., BERRY, G., 1994. *Statistical Methods in Medical Research* (3rd Edition).

6. ARSHAM, H., 2004. *Statistical Thinking for Managerial Decision Making* [Online]. Available from http://home.ubalt.edu/ntsbarsh/index.htm [Accessed on 11th November 2004].

7. BARMAN, S., 2002. *Writing Information Security Policies*, New Riders Publishing.

8. BOX, G.E.P., & JENKINS, G.M., 1976. *Time Series Analysis, Forecasting and Control*, Holden-Day: San Francisco.

9. BRITISH EUROPEAN STANDARDS, 2005. BS 7799/ ISO 17999. [Online]. Available from: http://www.british-europeanstandards.org/BS7799_standards.htm [Accessed on 17th May 2005].

10. BRITISH STANDARDS INSTITUTION, 2004. Latest News. [Online]. Available from: http://www.bsonline.bsi-global.com/server/index.jsp [Accessed on 04th April 2005].

11. BRITISH STANDARDS ISO/IEC, *Information Technology: Code of Practice for Information Security Management (ISP 17799).*

12. BUSINESS PARK OF MAURITIUS LTD, 2004. *Mauritius: A Paradise in the Indian Ocean.*

13. C & A SYSTEM SECURITY LTD, 2002. *Information Security: The COBRA Method.* [Online]. Accessed from: http://www.securitypolicy.co.uk/securitymanagement/ [Accessed on 16th May 2004].

14. C & A SECURITY SYSTEMS LTD, 2002. Introduction to COBRA [Online]. Available from: http://www.securitypolicy.co.uk [Accessed on 16th May 2004].

15. CARIGUE, R. & STEFANIU, M., 2003. *Information Security Governance Reporting*, BMO Financial Group, Canada.

16. CENTRAL STATISTICS OFFICE, 2003. 2003 *Statistics on Mauritius*, Government of Mauritius.

17. CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL, 2005. [Online]. Available from: http://www.cissp.com/Exam/exam.asp [Accessed on 04th April 2005].

18. CONTROL DATA SYSTEMS, INC., 1999. Why Security Policies Fail [Online]. Available from: http://www.cdc.com [Accessed on 02nd July 2005].

19. CRC JOURNALS, 2001. *Information Security Risk Analysis*, 2001 CRC Press LLC.

20. CRISIS MANAGEMENT AND DISASTER RECOVERY GROUP, 2002. *Theory and Resources for Disaster Recovery and Crisis Management* [Online]. Available from: http://www.crisis-management-and-disaster-recovery.com . [Accessed on 10th June 2005].

21. CROSBY, PHILIP, B., 1979. *Quality is free*, New American Library, New York, USA.

22. CSO ONLINE.COM, 2004. *The Best Practices of Highly Secure Organisations*, 2004 Global Information Security Survey, CSO Magazine, September 2004.

23. DALLAL, G.E, 2000. *Nonparametric Statistics.*

24. DANIEL, W. W., & TERREL, J. C., 1995. *Business Statistics for Management & Economics*, 7th Edition, Houghton Mifflin Company, U.S.A.

25. DEEKS, J., FOSTER, M., GREENBANK, T., VORLEY, G. and SEYERLE, J. 2002. *BS15000 IT Service Management and BS 7799 Security Management - White Paper on BS15000 IT Service Management and BS 7799 Security Management*, 19th February, 2002.

26. DELOITTE & TOUCHE & TOHMATSU, 2004. *2004 Global Security Survey*, Global Financial Services Industry.

27. DISASTER RECOVERY WORLD, 2002. *The Business Continuity Planning & Disaster Recovery Planning Directory* [Online]. Available from: http://www.disasterrecoveryworld.com/ [Accessed on 23rd February 2004].

28. EL SEGUNDO, 2001. *CSC Survey Reveals Inadequate Information Security Practices Among Companies Worldwide*, Computer Sciences Corporation (CSC) [Online]. Available from: http://www.csc.com [Accessed on 27th February 2005].

29. ETIENNE, P., 2005. *Cyber criminal neutralizes broadband network*, L'EXPRESS.

30. FEDERAL BUREAU OF INVESTIGATION (FBI) & SECURITY INSTITUTE, 2001. *Computer Crime and Security Survey – (ISO/IEC 17799 Security Standards Guidelines for Best Practice).*

31. FERRIS, J.M., 1994. Using Standards as Security Policy Tool, Department of the Treasury, Washington, D.C.

32. FIELDLER, A. E. NOWECO, 2003. *Necessity of Management of Information Security - the Standard ISO 17799 as international basis.*

33. FOWLER, F. J. Jr., 1984. *Survey research methods*. Thousand Oaks, CA: Sage.

34. GASSP, 1995. *International Information Security Foundation, Generally Accepted System Security Principles Committee.*

35. GORSUCH, R. L., 1983. *Factor Analysis* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

36. GUADAGNOLI, E., & VELICER, W. F., 1988. *Relation of sample size to the stability of component patterns, Psychological Bulletin.*

37. HAMMER, M. and CHAMPY, J., 1993. *Re-engineering the Corporation*, Nicholas Berkley Publishing, London, UK.

38. HARTER, P., ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, 2001. *Information Security in a networked World, Proceedings of the OECD Workshop,* Tokyo.

39. HATCHER, L., 1994. *A Step-by-Step Approach to Using the SAS® System for Factor Analysis and Structural Equation Modeling*. Cary, N.C.: SAS Institutte, Inc.

40. HILBERT, P., 2005. *Panne Internet : Les dessous d'un sabotage,* L'EXPRESS.

41. HOLLAND, M., 2002. *Guide to citing Internet resources* [online]. Poole, Bournemouth University. Available from: http://www.bournemouth.ac.uk/library/using/guide_to_citing_internet_sourc.html. [Accessed on 25th May 2004].

42. IEEE COMPUTER SOCIETY, 2003. *Proceedings of the 19th Annual Computer Security Applications Conference 2003.*

43. IGNOU, 2002. *Quantitative Analysis for Managerial Applications,* New Delhi, SOMS.

44. INFORMATION SECURITY POLICY WORLD, 2001. *Security Online Support Information Security Policies.*

45. INTERNATIONAL ORGANISATION FOR STANDARDIZATION, *Banking and Related Financial Services – Information Security Guidelines (ISO/TR 13569).*

46. INTERNATIONAL ORGANISATION FOR STANDARDIZATION, ISO 1999 & *ISO 17799 Standard publication.*

47. INTERNATIONAL ORGANISATION FOR STANDARDIZATION, ISO 27001, 2005. *The ISO17799 & ISO 27000 Newsletter - The Information Security Standard.*

48. ISIXSIGMA, 2005. *P-Value* [Online]. Available from: http://www.isixsigma.com/dictionary/P-Value-301.htm [Accessed on 06th October 2005].

49. ISO, 2004. *BS 7799-ISO 17799 Security Standards – For a better Information Security Management.*

50. JURAN, J.M., 1974. Quality Control Handbook, McGraw Hill, USA.

51. KOTHARI, C.R., 1985. *Research Methodology Methods & Techniques*, Wiley Eastern: New Delhi.

52. KRAUSE, M., TIPTON, H., 1999. *Handbook of Information Security Management*, Auerbach Publications.

53. LEEDY, P., 1993. Practical Research: Planning & Design, 5th Edition, Macmillan Publishing Company.

54. LONG, D., 2003. *Spearman's Rank Correlation Test* [online]. Available at: http:// www.cs.cmu.edu [Accessed on 06th October 2005].

55. L'EXPRESS, 2005. *Cyber criminal neutralizes broadband network.*

56. L'EXPRESS, 2005. *Panne Internet : Les dessous d'un sabotage*

57. MARSH, N., 1996. *Statistical Glossary.*

58. MAURITIUS NEWS, 2005. *The Mauritius Commercial Bank Scandal: The disappearance of the Deposit Account of 800 million rupees.*

59. MAURITIUS CHAMBER OF COMMERCE AND INDUSTRY, 2003. Mauritius Statistics.

60. MAURITIUS QUALIFICATION AUTHORITY, 2004. *Course Directory*, Mauritius.

61. MICROSOFT CORPORATION, 2005. *Microsoft Office Online* [Online]. Available from: http://office.microsoft.com/en-gb/FX010858001033.aspx [Accessed on 13th August 2005].

62. MIMOSO, M., SEARCHSECURITY.COM, 2002. *Survey respondents see challenges with company security policies* [Online]. Available from: http://searchsecurity.techtarget.com [Accessed on 27th February 2005].

63. MURPHY, L., 2004. *Survey preparation: Survey Sample & Response Rates.*

64. MUSTAFI, C.K., RAO, S.S., 2003. *Research Methodology for Managerial Decisions*, Indian Institute of Management, Unique Press (P) Ltd.

65. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), 2004. *An Introduction to Computer Security*, NIST Handbook (NIST Special Publication 800-12).

66. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), 2005. Common Criteria. [Online]. Available from: http://niap.nist.gov/cc-scheme/index.html [Accessed on 25th February 2005].

67. NCES, 2005. *Statistical Standards* [Online]. Available from: http://nces.ed.gov/ [Accessed on 16th July 2005].

68. NUNNALLY, J. C. 1978. *Psychometric Theory* (2nd ed.). New York: McGraw Hill.

69. ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, 2004. *OECD Global forum on information systems and network security: Towards a global culture of security.*

70. PELTIER, T.R., 2001. *Information Security Policies, Procedures & Standards*, CRC Press Company.

71. PERRYMON, JOSH. ALLSTATES TECHNICAL SERVICES, 2002. *Information Security Auditing / Implementation Procedures*: *White Paper on Information Security Auditing / Implementation Procedures*, November 2002.

72. PFLEEGER, C.P., 2000. *Security in Computing*, 2nd Edition, Prentice Hall.

73. PRICEWATERHOUSE COOPERS, 2004. *Information Security Breaches Survey 2004*, UK.

74. RAOSOFT, INC. 2005. *Sample Size Calculator* [Online]. Available from: http://www.raosoft.com/ [Accessed on 07th June 2005].

75. RESOURCES FOR SECURITY RISK ANALYSIS, ISO 17799 / BS 7799 SECURITY POLICIES & SECURITY AUDIT, 2004. *Security Risk Analysis, BS 7799, Security Policies and Security Audit Solutions* [Online]. Available from: http://www.securityauditor.net/ [Accessed on 02nd March 2005].

76. RISK ASSOCIATES, 2002. *Applying Information Security Policies & Computer Security Standards* [Online]. Available from: http://www.securitypolicy.co.uk/secpolicy/ [Accessed on 02nd March 2005].

77. RIVIERE, L., 2004. *Top 100 Companies*, Business Publications Ltd, Mauritius.

78. RIVEST, R. L., SHAMIR, A., ADELMAN, L. M., 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, 21(2):120-126, February 1978.

79. RSA Security Inc., 2005. Content Library [Online]. Available from: http://www.rsasecurity.com/content_library.asp [Accessed on 02nd March 2005].

80. SAFERPAK, 2005. *Surveys- Response Rate* [Online]. Available from: http://www.saferpak.com [Accessed on 08th June 2005].

81. SAS, 2002. *Developing an effective Security Policy to safeguard the Enterprise: White paper on IT Security Management, 2002.*

82. SCHNEIER, B., 2000. *Secrets & Lies*, Wiley-VCH Verlag GmbH.

83. SEARCHSECURITY.COM, 2001/2. *Survey on Corporate security policies - Security Policies in the Workplace* [Online]. Available from: http://searchsecurity.techtarget.com/tips [Accessed on 27th February 2005].

84. SECURITY INSTITUTE, 2001. *FBI and Computer Crime Security Survey*.

85. SECURITY RISK ANALYSIS & ASSESSMENT, AND ISO 17799 / BS 7799 COMPLIANCE. *The Ten Sections of ISO 17799* [Online]. Available from: http://www.riskworld.net/7799-2.htm [Accessed on 09th March 2005].

86. SECURITY RISK ASSOCIATES, 2001. *The Benefits of Security Risk Analysis* [Online]. Available from: http://www.eon-commerce.com/riskanalysis/benefits.htm [Accessed on 27th February 2005].

87. SECURITY RISK ASSOCIATES, 2001. *Security Risk Assessment & Risk Analysis: How & Why* [Online]. Available from: http://www.eon-commerce.com/riskanalysis/index.htm [Accessed on 27th February 2005].

88. SEDDON, D., 2002. *Security Policy: Underpinning information security, DTI Information Security Breaches Survey 2002*, Published in National IT Decision Makers' Yearbook.

89. SIEGEL S., CASTELLAN N.J. (Jr), 1988. *Non-parametric Statistics for the Behavioral Sciences*, 2nd Edition, McGraw-Hill Book Co., New York.

90. SLATER, D., CSO ONLINE.COM, 2003. *Security Immaturity*, CSO Magazine, April 2003.

91. STEINER, 2004. *Steiner Marketing* [Online]. Available from: http://www.steinermarketing.com [Accessed on 14th November 2004].

92. THE BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING PRACTITIONER'S DIRECTORY, 2004. *The Business Continuity*

Directory [Online]. Available from: http://www.business-continuity-and-disaster-recovery-world.co.uk/ [Accessed on 10th June 2005].

93. THE INFORMATION SECURITY POLICIES WORLD, COMPUTER SECURITY POLICIES DIRECTORY, 2001. *Security Online Support (SOS) Information Security Policies* [Online]. Available from: http://www.information-security-policies-and-standards.com/ [Accessed on 27th February 2005].

94. THE ISO 17799 DIRECTORY: SERVICES & SOFTWARE FOR ISO 17799 AUDIT, ISO 17799 COMPLIANCE & SECURITY RISK ANALYSIS, 2004. *General ISO Information* [Online]. Available from: http://www.iso17799software.com/ [Accessed on 02nd March 2005].

95. THOMPSON, S., 2002. *Sampling*, Wiley.

96. TRUST & TRUSTEES, 2003. *Huge fraud at Mauritius bank, Compliance & Regulation News* [Online]. Available from: http://www.trusts-and-trustees.com/crn/news/ [Accessed on 02nd July 2005].

97. VISWANATHAN, P. K., 2004. *Glimpses into Application of Chi-Square Tests in Marketing* [Online] Available from http://www.vishstat.com [Accessed on 17th November 2004].