An Investigation of Information Security Policies and Practices in Mauritius

O. Sookdawoor

School of Computing, University of South Africa, P.O. Box 392, UNISA, 0003, South Africa
Email: rsookdawoor@bai.intnet.mu

Abstract

Information is today regarded as one of the most valuable assets of an organisation. Without 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.

This paper aims at presenting the findings of the research that was conducted in Mauritius in 2005 while assessing the state of information security policies and 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 security issues while contributing to the development of the security community.

Keywords

Information security framework, information security policies, practices, established standards and compliance.

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 meets 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).

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

staff's day-to-day activities. Knowing the policies is only one half of the equation; staff 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.

Furthermore, one often finds organisations having sets of security policies and procedures but which 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.

2. IT 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). Other well-established standards have also contributed towards information security as a whole.

2.1 BS 7799, ISO 17799 & ISO 27001 Security Standards

In late 2000, the International Organisation for Standardisation (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 (Part 1) 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 BS7799. 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 1 below (ISO, 2002).

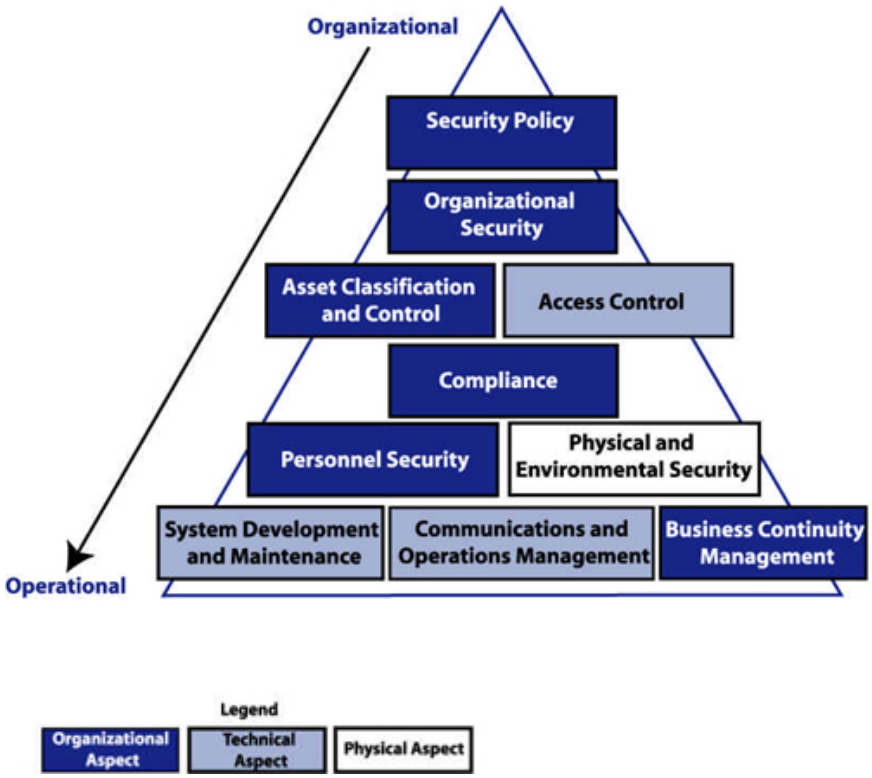

Figure 1: Areas covered by the BS 7799 / ISO 17799 standards

Consider Figure 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 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.
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.

In the year 2002, a revision of BS 7799 (Part 2) was published. It was earlier referenced as BS 7799:2002. 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).

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 security 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 (Juran, 1974). 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 as part of the ISO 27000 series. ISO 27002 and ISO 27004 are likely to be produced in the next few years

3. Security Findings on the International Scene

One can note, from the literature review, a growing emphasis on information security policy and its enforcement (OECD Guidelines, 2002; Proceedings of the OECD Workshop, 2001; IEEE, 2003; Ferris, 1994).

Several studies have been undertaken around information security policy and practices on the international scene (CSO Research, 2004; SearchSecurity.com, 2001/2; DTI Information Security Breaches Survey, 2002; Deloitte Global Security Survey, 2004; CSO Online Survey, 2003; Computer Sciences Corporation, 2001). Findings were very enlightening for the information security community and practitioners. While in some areas, findings were alarming thereby necessitating urgent action, in other areas they gave some encouraging sign. The key lessons learnt have been categorised and summarised as per below:

3.1 Positive Issues

- There is a strong need for security training and awareness for employees and staff and the management's readiness to invest along these lines;
- There is a growing investment in security projects across the globe;
- Organisations around the world are concerned about security policy and compliance issues and efforts are being dispensed to address any gaps in compliance.

3.2 Negative Issues

- There is a problem of compliance with information security policy, standards and regulations across the world;
- 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;
- There is a lack of effort to measure and track security projects systematically using proper security Key Performance Indicators (KPIs);
- Where security policies exist, it was found that they were not maintained regularly to stay up-to-date with changing conditions;
- Some surveys revealed low participation or commitment of top management in certain areas of security implementation.

4. Investigation on the Local Scene

There were a few cases reported lately in Mauritius around information security practices (Mauritius News, 2003; Trust and Trustees, 2003; Mauritius News, 2005; Etienne, 2005).

There were concrete local cases where ineffectiveness of security policies, procedures and practices had been found. This demonstrated that even the topmost organizations as reported can face such problems in Mauritius. In other words, findings in Mauritius prove that it is not so different from countries around the globe with regard to security practices and policy compliance. It thus became 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 would not have been possible to confirm or generalize certain perceptions.

A field study was thus conducted in mid 2005 for a population comprising 100 major private organisations. A survey was devised and conducted for the selected sample using properly

supported methodologies, responses were compiled and analysed by using sound statistical techniques and results were interpreted. Again the findings have been very useful and enlightening to all security stakeholders. The key ones have been reported below under the relevant areas:

4.1 Responses Analysis

(a) 85% of responses were obtained and analysed in samples of 41 companies grouped by industry. Most of the professionals that were surveyed held a managerial position (60%) or senior technical role (23%);
(b) It came out that 91% of the respondents were male and 9% female;
(c) Only 3% of the respondents confirmed having an information security position or function in their respective companies;

4.2 Information security policy: Its presence, formulation and review

4.2.1 Findings

(a) Figure 2 below 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 Figure 2 below.

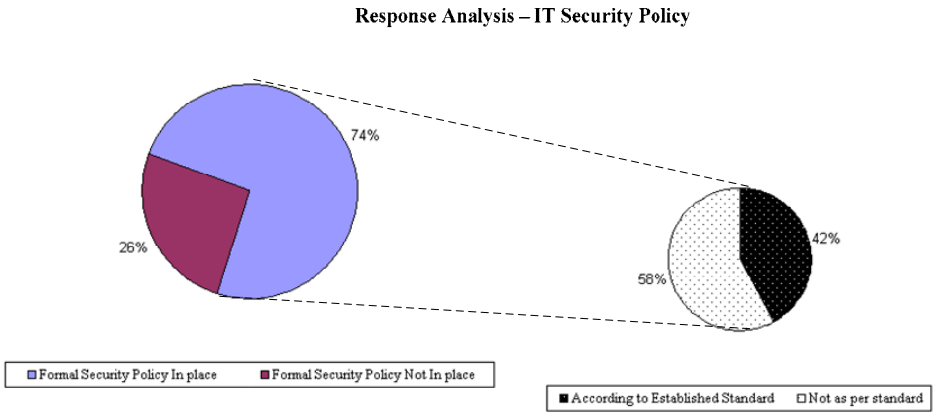

Figure 2: IT Security Policy Analysis

(b) 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 BS7799. 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.**
(c) Only 53% of the respondents confirmed the involvement of senior executives in the process of information security policy formulation;

(d) 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.

4.2.2 Observations

The high rate of non-standard security policies is a matter of concern for Mauritian organisations. 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 a security policy is one thing, having a properly defined and well-established security policy is another.

Furthermore, 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 the majority 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.

4.3 Education & Training

4.3.1 Findings

57% of the respondents confirmed that there were no security awareness programs. There was also a high rate of respondents (63%) confirming a lack of regular training in areas of information security as shown in Figure 3 below:

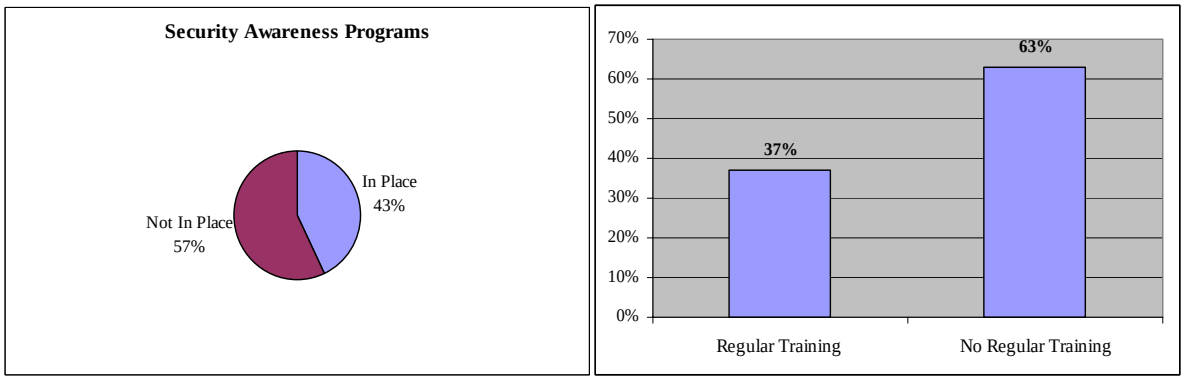

Figure 3: Analysis of Security Programs & Training Practices

4.3.2 Observations

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 reported in the press (Mauritius News, 2003/5; Etienne 2005).

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.

4.4 Measurement framework for the assessment of information security

The majority of the participants (23 over 35 representing almost 66%) did not have any metrics or key performance indicators on the state, effectiveness and application of their information security policies.

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 security issues in the organisation.

4.5 Compliance with information security policies and procedures

4.5.1 Findings

(a) Out of those who stated having security policies and procedures in place, 43% of them confirmed that they were not systematically complying with the security policies and procedures in place;

(b) Moreover only 11% of the companies had implemented established security policies such as BS 7799 and ISO as presented in Figure 4 below:

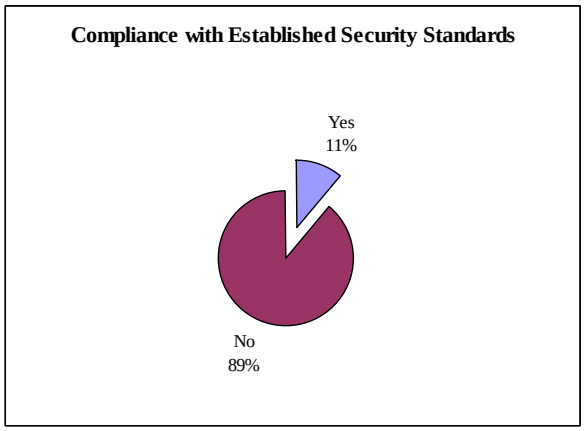

Figure 4: Analysis of compliance with established standards

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 5.

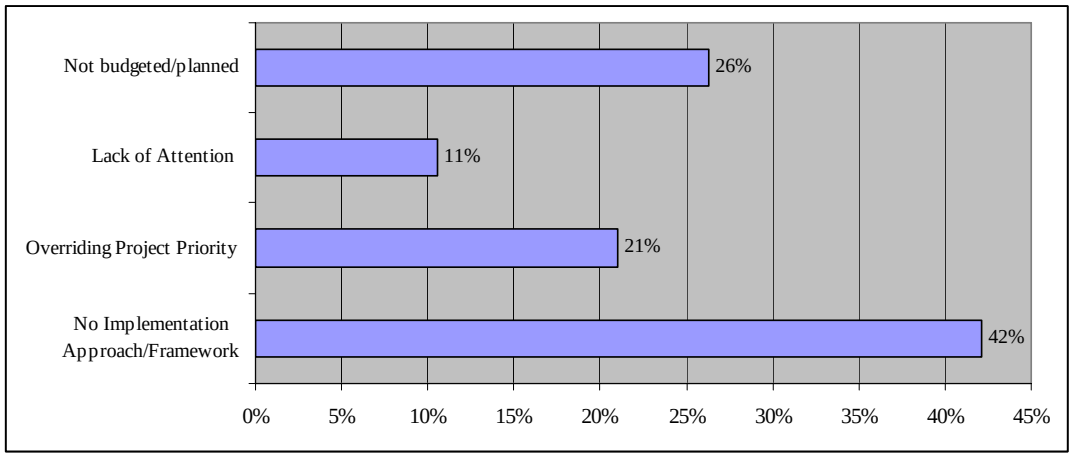

***Figure 5: Analysis of reasons for noncompliance with information security** policy*

Four prime reasons were noted for the non-adherence to information security policy namely:

1. No implementation/ framework;

2. Not budgeted or planned;
3. Overriding project priority;
4. Lack of management's attention.

4.5.2 Observations

There are high business risks associated with adhoc 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. The low compliance rate to established security standards is also a concern to be addressed by the concerned organisations.

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.

These responses also give a clear indication that a comprehensive programme and framework will need to be put in place if one intends 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.

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.

4.6 Summary of hypothesis tests

A number of statistical tests was conducted to support the interpretation exercises and clarify on certain perceptions. A summary of these tests and outcomes is given in Table 1 below.

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 1: Summary of Hypothesis tests

The results of the hypothesis tests have given clear confirmation on where statements can be confirmed and generalised for the whole population and where they cannot be. It must be noted that these tests hold true for the chosen significance level (5%).

5. Similarities & Differences

It will be interesting to compare the findings of the local context with that of the global ones. This can show how information security practices in Mauritius compares to the global trend. This is given in Table 2 below.

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 2: 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 in Mauritius in 2005 to support this paper
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 2 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 a near future. In other words, Mauritian organisations have to engage in a sustained improvement programme to become a role model in this area.

6. Conclusion

This paper 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 information security practitioners 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:

- The need for a standard information security policy that has as objective to properly reflect the business goals;
- The need for clear management commitment and support in undertaking such projects for the welfare of the organisations, economy and community;
- The need for proper distribution, sustained education and guidance on security policies to all employees and parties involved in the organisation;
- The need for a sustained awareness campaign to draw the attention of all employees and stakeholders to the risks associated with lack of proper security practices;
- The need for a comprehensive strategy on security risk analysis, risk management and security requirements;
- The need to shape up the attitude, culture and management practices of all stakeholders towards information security;
- The need for an approach to security implementation which is consistent with the organization's own culture;
- The need for a comprehensive measurement system to evaluate progress, performance and effectiveness of security implementation;
- The need for a sound review and control structure to act as guardians to ensure systematic compliance with standard information security policies and practices;
- The need to compensate or reward best practitioners of and good initiative taken towards information security fairly.

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

7. References

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

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

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

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

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 02nd March 2005].

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

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

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

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

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

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

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

ISO, 2004. *BS7799-ISO 17799 Security Standards – For a better Information Security Management.*

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

MAURITIUS NEWS, 2003. *The Mauritius Commercial Bank Scandal: The disappearance of the Deposit Account of 800 million rupees.*

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, 2002. *Guidelines for the security of networks and information systems: Towards a culture of society.*

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

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

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

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

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

TRUST & TRUSTEES, 2003. *Huge fraud at Mauritius bank, Compliance & Regulation News* [Online]. Available from: http://www.trusts-and-trustees.com/crn/news/news_mar06_03.html [Accessed on 02nd July 2005].