# Establishing a Sustainable Information Security Management Policies in Organization: A Guide to Information Security Management Practice (ISMP)

Julius Olusegun Oyelami
Faculty of Computing
University Technology Malaysia
Skudai, Johor Bahru 81310
Email: Jooyelami2 [AT] live.utm.my

Norafida Binti Ithnin
Faculty of Computing
University Technology Malaysia
Skudai, Johor Bahru 81310

*Abstract*— **Increased in computer usage by organizations in respect to both internal and external connectivity and the wider use and popularity of the internet are offering many organizations of all types an unprecedented opportunity to enhance and aligned their IT operations by reducing paper processing, cutting costs, and sharing of information. However, the success of many of these efforts depends on an organization's ability to protect the confidentiality, integrity and availability (CIA) of their information in addition with data and systems it depends or relies on. Deficiencies in organization information security and management are becoming a global issue or challenges and raised growing concern among IT professional. Over the years and recently, there has been series of reports on information security issues and challenges in organizations and this, has been noted as wide high-risk area to many organization. This paper will describes sixteen (16) practices (P) related to information security and management organized under five (5) management principles (PP) that we identified during a research study we conducted on both private and governmental organization. These organizations have been identified having good reputations for information security programs and configured appreciable management policies in-place. Each of these practices contains and outlined specific examples of the techniques and control used by these organizations to increase their information security program's effectiveness. Data was collected from both the strong and weak organization and we also used the principle and practice from the strong organization as a yard stick to measure the strength of the weak organizations. The results of the study identified lack of direction, limited budgets and finances, lack of prioritization from senior officials and general ignorance to identify threat by the users. The result is also used to assist and support the weak organizations in strengthening their information security management programs at all levels.**

***Keywords***--- *Information Security Management and data protection policies.*

## I. INTRODUCTION

All organization must ensure the implementation of security practices within their operations to gain customers confidence and trust and also to protect their privacy and sensitive data of been stolen, sabotage or destroyed accidentally, [1] [2]. Learning from successful and leading organizations, clearly illustrates how these organizations are successfully addressing the challenges of fulfilling information security and management goal and objectives. These organizations establish a central management focal point; they promote information security awareness program, link information security policies to business risks, and develop practical risk assessment procedures that link security to business needs. To most organizations, electronic information and automated systems are essential to virtually all major operations and management. If organization cannot protect the integrity and availability of information and data, the confidentiality of that information and the ability to carry out their missions will be severely impaired or failed. However, despite the enormous usage and dependence by organization on electronic information and systems [3], [4] and [5] Information security audits revealed and identified that, organizations continue to disclose serious information security and management weaknesses. As a result, billions and millions of dollars in organization assets are at risk of losses, vast amounts of sensitive information and data are at risk of inappropriate disclosure to unauthorized person, and critical computer-based operations are vulnerable to serious and devastating disruptions.

Organizations have also identified and described it a potentially devastating implications of poor information security management program and policies from a broader perspective since then, organizational information security audit reports have continued to identify the widespread of

information security weaknesses that are taking place on organization operations and pose risk on assets. Although, many factor contributed to these weaknesses. Previous and recent researchers have found that, an underlying cause is poor security program and management. To help identify solutions to this problem, we study organizations with superior information security and management programs in other to identify management and security practices that could benefit organizations at all level of information security program and management practices.

This paper is designed to promote senior management and executives in information security policies and management and as well as decisions making in business policies and the awareness of information security issues and to provide information necessary to promote and establish information security management framework (ISMF) for more effective information security programs. The opening segments in this paper describe the problem and weak information security in private and governmental organization and describe the issue of information security management in the context of other information technology management issues. This paper describes sixteen (16) practices, organized under five management principles (PP) that we identified during a research study we conducted on both private and government organizations with reputations for having good information security programs and management policies. Each of these practices contains specific examples of the techniques used by these organizations to increase their security program's effectiveness.

Aim and Objectives

1. To identify leading organizations in information security management practices and control.
2. To promote information security policies and management practices for IT user's for decisions making and
3. To provide required information to promote and establish sustainable information security risk and management framework for more effective information security programs in organization.

## II. . FOCUS

This paper focuses on information security management program or practices from the weak organization perspective and the step by steps process or protocols a weak organization should follow in the context of securing and managing information as most of them had responded to these risks by re-orienting their information security management programs from relatively low-profile operations focused primarily on mainframe information security to visible, integral components of their organizations' business operations without a lasting solution. It also focuses on the aspect of strategic planning for an organization's overall information security management. An organization's success in information security management and other security-related implementation and efforts is likely to base on its overall ability to manage the utilization of information policies, control and management associated with information technology and adequate training for users.

## III. METHODOLOGY

Throughout the guide, our approach based on case study and data observation .We make several observations on a well-known governmental organizations, this observation is primarily based on their information security and management practices in order to benchmark them with the practices of the non-governmental organizations or otherwise known as private entities (private organization) we have studied. These observations based on the accumulated and data we have previously developed over a period of one and the half (1/2) years and on our recent discussions and interview with chief information security officer (CISO), IT managers and other IT officials who are knowledgeable and professional information security and management practitioner's. From the organizations we studied, we benchmarked data we collected from the successful organization as a yardstick with those weak organizations as they are struggling or striving to manage the same types of risks that faced the successful organization. Because of the similarities in the challenges they face, we believe that weak organization or entities can learn from the strong or successful organizations to develop their own and more effective information security management programs.

## IV. CASE STUDIES

### *A. Case Studies 1: Successful /Strong Organizations in Information Security Management*

To supplement our study on information security management audit work at various organizations and to gain a broader understanding of how information security management programs can be successfully implemented, we studied the management and security practices of two (2) organizations that we recognized having strong information security programs in place. The specific aim and objective of our review was to determine how such organizations have designed and implemented their information security and management programs in order to identify practices that could be applied at all levels of securing information and data. We also focused primarily on the management framework that these organizations had established rather than the specific controls that they had chosen, because previous research work had identified information security management as an underlying problem at most organization. Although powerful

technical controls, such as those involving in encryption, are becoming increasingly available to facilitate and enhance information security management, effective implementation also requires that these techniques must be thoughtfully selected and that, their use must be monitored and managed on a continuous basis. In addition, there are many aspects of information security, such as risk assessment, policy development, and disaster recovery planning that require coordinated management attention. To identify leading organizations, we reviewed professional literature and research information and solicited suggestions from experts in professional organizations, nationally known public accounting firms, and IT professional institute and agencies. In selecting organizations to include in our study, we relied primarily on recommendations from the British Computer Society (BCS), Institute of Information Technology professional (IITP) New Zealand and Information Security Audit and Control Association (ISACA) and public accounting firms because they were in a position to evaluate and compare information security programs at numerous organizations. In addition, we attempted to select organizations from a variety of business sectors to gain a broad perspective on the information security management practices being employed. After initial conversations and consent approval with few numbers of organizations, we narrowed our focus to four organizations, two that had implemented comprehensive information security management principles and another two that fairly or partially implemented information security programs. All were prominent nationally known organizations within the state. They included a private corporation and a governmental corporation; a regional electrical power company, a government university, a private nonbank financial institution, a computer vendor, and a chemical manufacturing industry. The number of computer users that was noted and observed within these organizations ranged from 2,500 to 8,000, and three had significant international operations. Because most of the organizations considered discussions of their information security management programs to be sensitive, private and confidential and they wanted to avoid undue public attention on this aspect of their operations, we agreed not to identify and expose these organizations by their trade names. We obtained information primarily through interviews with senior IT security managers and document observation and analysis conducted during and after visits to the organizations we studied. In a few cases, we toured the organizations' facilities and observed practices in operation. We supplemented these findings, to a very limited extent, with information obtained from others organizations.

### *B. Case Studies 2: Weak Organizations in Information Security Management*

The weak organizations we observed are non-governmental organization (or private entities). These two organizations don't want to be identified by name and they are working hard to establish a strong information security management practices. Our aim and objective of our review and observation into these organization was to determine how these organizations have been struggling to implement their information security management programs in order to identify practices and to meet up with the appropriate standard that could be applied at all levels of securing information and data structure. We identified that these organization have some measures of information security management program but, where not adequate enough to resolve most of the challenges confronting information security management as compared with the strong organizations. Observation revealed that, these weak organization where also confronted with same information security threats confronting the strong organizations. The weak organizations only have one to two principles and three to five practices among the five (5) principles and sixteen (16) practices identified with the strong organizations, positioning the strong organization to better advantage in formulating security policies and mitigating threats than the weak organization.

## V. Data Collection

During our observation into the information security management principles (ISMP) of successful or strong organization, table 1:1 depicted the ISMP conducted as shown below. After careful observation, we identified that, there are five standard principles and each of these principles (PP) is further categorized into 16 segments called practices (P). The first principle is the risk management principles ($PP_{1)}$ follow by the establishment of a central management focal point ($PP_2$), implementation of appropriate policies and related controls ($PP_3$), promoting awareness across the organization ($PP_4$) and monitoring and evaluation of policy and control effectiveness ($PP_5$). Table 1:1 below depicted the data we observe from the successful organization and mapped with the weak ones.

TABLE 1. ISMP of successful Organization

| | |
|---|---|
| Principle 1 | Assess risk and determine needs(**$PP_1$**) |
| Principle 2 | Establish a central management focal point (**$PP_2$**) |
| Principle 3 | Implement appropriate policies and related controls (**$PP_3$**) |
| Principle 4 | Promote awareness (**$PP_4$**) |
| Principle 5 | Monitor and evaluate policy and control effectiveness(**$PP_5$**) |

Key: Principles stand for PP

Further observation also revealed that, these principles (PP) implemented by successful organizations where further groups into sixteen practices (P). Table 2, table 3, table 4, table 5 and table 6 respectively depicted the sixteen practices identified from successful organization under five management schemes.

TABLE 2. Assess Risk and Determine Needs (**$PP_1$**)

| | |
|---|---|
| Practice 1 | Recognize Information Resources as essential organizational assets that must be protected |
| Practice 2 | Develop practical risk assessment procedures that link security to business needs and objectives. |
| Practice 3 | Hold program or business managers accountable |
| Practice 4 | Managing risk on a continuing basis |

**Key:** Practices stands for (P)

TABLE 3 Establish a Central Management Focal Point (**$PP_2$**)

| | |
|---|---|
| Practice 5 | Designate a central group to carry out key activities |
| Practice 6 | Provide the central group ready and independent access to senior executives |
| Practice 7 | Designate dedicated funding and staff |
| Practice 8 | Enhance staff professionalism and technical skills via training. |

TABLE 4. Implement Appropriate Policies and Related Controls (**$PP_3$**)

| | |
|---|---|
| Practice 9 | Link Policies to Business Risks |
| Practice 10 | Distinguish between policies and guidelines |
| Practice 11 | Support policies through the central security group |

TABLE 5. Promote Awareness (**$PP_4$**)

| | |
|---|---|
| Practice 12 | Continually educate users and others on risks and related policies |
| Practice 13 | Use attention-getting and user-friendly techniques |

TABLE 6. Monitor and Evaluate Policy and Control Effectiveness (**$PP_5$**)

| | |
|---|---|
| Practice 14 | Monitor factors that affect risk and indicate security effectiveness |
| Practice 15 | Use results to direct future efforts and hold managers accountable |
| Practice 16 | Be alert to new monitoring tools and techniques |

### *A. Data Analysis*

The Table 7 below depicted the data analyzed from both weak and successful or strong organization regarding there information security management principles. The data from the weak organization where cross map against the strong organization information security management practices (ISMP).

TABLE 7. Dataset A, Successful and weak principles

| **Principles(PP)** | **Successful Organizations** | | **Weak Organizations** | |
|---|---|---|---|---|
| | **$O_1$** | **$O_2$** | **$O_3$** | **$O_4$** |
| **$PP_1$** | √ | √ | × | × |
| **$PP_2$** | √ | √ | × | × |
| **$PP_3$** | √ | √ | × | × |
| **$PP_4$** | √ | × | × | × |
| **$PP_5$** | √ | √ | × | × |

**Key:** PP stands for principles
O stands for Organization

After careful study of the data Set A, we identified that strong organization have some adequate information security management principle strong enough to resolve information security management challenges by almost 80%, if not completely resolve, while the weak organizations are in a struggle to established basic principle (PP) in the context of protecting information and management standards.

Table 8 depicted data set B, these data is intend to analyze if the weak organization could have some practices (P) regarding information security management within their operation.

TABLE 8**.** Dataset B, Successful and weak practices)

| **Practices(P)** | **Successful Organizations** | | **Weak Organizations** | |
|---|---|---|---|---|
| | **$O_1$** | **$O_2$** | **$O_3$** | **$O_4$** |
| **$P_1$** | √ | √ | × | × |
| **$P_2$** | √ | √ | × | × |
| **$P_3$** | √ | √ | × | × |
| **$P_4$** | √ | × | × | × |
| **$P_5$** | √ | √ | × | × |
| **$P_6$** | √ | √ | √ | √ |
| **$P_7$** | √ | √ | × | × |
| **$P_8$** | √ | √ | × | × |
| **$P_9$** | √ | √ | × | √ |
| **$P_{10}$** | √ | × | × | × |
| **$P_{11}$** | √ | √ | × | × |
| **$P_{12}$** | √ | √ | × | × |
| **$P_{13}$** | √ | √ | √ | √ |
| **$P_{14}$** | √ | √ | √ | × |
| **$P_{15}$** | √ | × | √ | √ |
| **$P_{16}$** | √ | √ | √ | √ |

**Key:** P stands for practices
O stands for Organization

## VI. RESULTS

We identified weaknesses in both of the two private or non-governmental organization ($O_3$ and $O_4$) noted as the weak organization in their information security practices, but management attention has been carefully measured to ensure profitability and we also identified partial strength with this non-governmental organization information security but management attention has been lacking. We also identified that, private sector are reluctant to make the required investments in this area of information security due to, lack of direction, limited budgets and finances and the prioritization from senior officials and general ignorance to identify threat by the users. This could be concluded that, private organization does not have a positive and good culture towards information security due to limited training and awareness.

Having mapped the data collected from the successful organization ($O_1$ and $O_2$) the data analysis revealed that, both organization have common information security objective as follows: (1) Protect the confidentiality of sensitive personal and financial data on employees, clients, customers, and beneficiaries (2) Maintain customer, constituent, stockholder, or taxpayer confidence in the organization's products, services, efficiency, and trustworthiness (3) Avoid third-party liability for illegal or malicious acts committed with the, (4) Ensure that organizational computer, network, and data resources are not misused or wasted, (5) Avoid expensive and disruptive incidents, (6)Protect sensitive operational data from inappropriate disclosure (7) Organized computer or network resources (8) Avoid fraud, (9) Avoid a hostile workplace atmosphere that may impair employee performance and (10) Comply with pertinent laws and regulations. We also identified threat and possible or potential damage to the organization in the nearest future. Some of the threat identified are (1) attempts to access private information (2) malicious acts (3) sabotage (4) user error (5) and fraud while the potential damages identified are (1) sensitive data disclosed (2) integrity of data and reports corrupted (3) assets lost (4) critical operations halted (5) services and benefits interrupted and (6) taxpayer confidence lost.

## VII. RECOMMENDATIONS

Our recommendations intended to improve the information security management practices and principles for agency in information security practices and strengthen its leadership role. Initiatives that we suggested for the organization to consider incorporating in its strategic plan include developing information on the existing security risks associated with non-classified systems currently in use, developing information and data structure on the risks associated with evolving practices, such as internet usage, identifying best practices and principles regarding information security management programs so that they can be adopted by both governmental and private agencies, organization should also establish a methods for reviewing the adequacy of information security programs using interagency or IT professional consulting teams of reviewers, ensuring adequate review coverage of information security practices by considering the scope of various types of information security management audits and to periodically review and performed gap analysis to address any identified gaps in coverage, because, information security management program should be integrated as part of organization strategic. Organization must developed or identifying training needed by individual and this training should incorporate information security and awareness program that should focus on people and the training should be inculcate with psychology, social science, ethic and sociology (PSES) that will address cultural differences and values (CDV), this will enable individual to understand and embraced their differences. Lack of PSES within the information security and awareness training program will impede information security management practices and principle in the context of information security management and they should also identifying proven security tools and techniques for proper implementation.

## VIII. CONCLUSION AND DISCUSSION

From the literature review and with all indication, it has been noted that, some organization has put in place adequate information security management policies, practices and principles to address the technical and the non-technical aspect of information security management, It was also noted that, researchers and International organization of standardization (ISO) have identified several frameworks, standards and models such ISO27001, information security management maturity model (ISM3), information security management system (ISMS) for quality information security management, ISO9001 and information technology infrastructure library (ITIL) for effective and quality management requirements and to align information technology with business continuity, COBIT, OCTAVE as well as information technology laws and regulation such as data protection [6] to protect the use of personal data, the computer misuse [7] to protect wrongly use of computer and the privacy and electronic communication regulation [8] to regulate information security management towards information sharing. In the literature review, personal information protection and electronic document act of (2000), the common law of confidentiality and the freedom of information act [9], access to information act [10] and the cyber intelligence sharing and protection act [11] and the protocol in information sharing framework where also identified as a way to secure, managed and regulate information security during usage and sharing across entities.

These aforementioned frameworks, standards, models, laws and regulations are meant for effective information security and management and to address information breaches and threats that might confront data and information during information sharing. Researcher have also identified that, culture, behavior, lack of trust are factor impeding information in the context of information security management and most of the researchers seems not to have a solution, as information security management concomitantly reflect human behavior. After critical analysis and review of all articles, a gap was observed, and this gap focus on lack of information security awareness and training [12] to address the loop holes in people behavior and some curriculum in information security education do not have the required element or modules to address human behaviors in the context of information security management towards information sharing.

## IX. FUTURE WORKS

Although we attempted to be as thorough as possible within the scope of our study, we identified and recognized that more work in this area need to be done; this will include a more in-depth study and data collection regarding individual practices and understanding of the subject matter. We also recognized and identified that the practices of information security management require customization at individual organizations depending on factors such as the existing organizational strengths and its weaknesses. Although we believe that the information security management practices described in this paper is fundamental enough in improving an organization's information security practices and management, they should be considered in the context in a broader spectrum of Information security management issues and challenges but an important factor is the effectiveness in implementing these principles and to link them in a cycle of operational activity that would helped and ensure that information security policies addressed current risks on an ongoing basis. The single most important factor in prompting the establishment of an effective security program was a general recognition and understanding among the organization's most senior executives of the enormous risks to business operations associated with relying on automated and highly interconnected systems. However, risk assessments of individual business applications provided the basis for establishing policies and selecting related controls. The areas of human science that focuses on psychology, social science and sociology need to be study to enhance human behavior towards cultural values; this could ignite positive behavior towards information security and may increase the awareness of users concerning these risks and related policies to effectiveness of controls and awareness activities that could be monitored through various analyses, evaluations and audits. This aspect of research may span a new information security paradigm in the future.

## REFERENCES

[1] M H. Fleming, “Homeland security studies and analysis institute”. Measuring cyber security information sharing (2012) pg203-416
[2] J. J. Sung, J. Back-Kyoo. “Journal of Leadership and organization studies” (2011) Vol.10, 7-8
[3] Electronics communication act of (2000)
[4] Privacy and electronics communication act of (2003)
[5] Personal protection and electronics document act of (2000)
[6] Data protection act of (1998)
[7] Computer misuse act of (1990)
[8] Privacy and electronics communication regulation of (2003)
[9] Freedom of information act of (2000)
[10] Access to information Act of (1985)
[11] Cyber intelligence sharing and Protection act of (2011)
[12] J. O. Oyelami, N. Ithinin, “People are the answer to security establishing a sustainable information security awareness training (ISAT) program in organization”. International Journal of Computer Science and information security (2013) 11(8):1-8

*About the Authors*

**Oyelami Julius Olusegun** Is Currently is a postgraduate research student at the department of information system, faculty of computing, University Technology Malaysia (UTM), and a member of information assurance and security research group (IASRG-UTM), His research interest are in information security management, social networking, information systems, Information sharing and knowledge management System. He is a professional member, Association for Computing Machinery (ACM), British Computer Society (BCS) and the Institute of Information Technology Professional New Zealand.

**Norafida Binti Ithnin** is an Associate Professor of computer science, currently a senior lecturer and head of information systems department in University Technology Malaysia (UTM), faculty of computing. She received her B.Sc degree in Computer Science (Computer Systems) form University Technology Malaysia (UTM), Kuala Lumpur, Malaysia in 1995 and her M.Sc degree in Information Technology (Computer Science) from University Kebangsaan Malaysia (UKM), Bangi, Malaysia in 1998. She earned her PhD degree in Computation from UMIST, Manchester, United Kingdom in 2004. Currently, her main research interests are security management and graphical password. She is a member of ACM and others.