NISER's ISMS Pilot Programme Experiences: Common Shortcomings in ISMS Implementation

Shamsuddin Abdul Jalil, Rafidah Abdul Hamid , Ariffuddin Aizuddin

Abstract: *Data needs to be protected and thus it is necessary to have an information security standard that can be adopted by Malaysian organizations to ensure data security. Thus, the National ICT Security & Emergency Response Centre (NISER) and SIRIM QAS International Sdn. Bhd. which is a wholly owned subsidiary of SIRIM Berhad has jointly conducted the Information Security Technical Expertise for ISMS (Information Security Management Systems) Pilot Program. It's objective is to enable local organizations to implement the best data protection methods. This paper aims to highlight the common shortcomings that were observed by NISER during the pilot programme implementation phase.*

Keywords*: ISMS, data, information, pilot programme, shortcomings, technical, management*

I. WHAT IS ISMS?

Protecting vital information is a huge challenge in all organisations today. Be it in paper or electronic form, data is the most critical element of any business and with more threats than ever before in both external and internal forms, it is no surprise that many organisations are implementing security procedures to ensure that their data remains private and not leaked or tampered by unauthorised parties.

Information Security Management Systems (ISMS) was initially the initiative from the UK Department of Trade and Industry in 1995 and its main objective was to provide a code of practice to information security practitioners. An ISMS is a systematic approach to managing sensitive company information so that it remains secure [1].

ISMS concerns itself with the security of information whether in physical or logical form and focuses on three areas: the confidentiality, integrity and availability of information or usually referred to as CIA. It encompasses of two parts: ISO17799 which is the Code of Practice for Information Security Management and BS7799-2:2002 which is the Specification for Information Security Management Systems with guidance for use.

II. WHY THE NEED FOR ISMS IMPLEMENTATION IN MALAYSIAN ORGANISATIONS?

The rising number of security breaches over the years have led to increasing security concerns among organisations throughout the world. In Malaysia specifically, the number of security breaches have continued to increase over the years and the breaches comes in different types and forms. The following diagram obtained from NISER's ISMS Survery in 2003 shows the different types of security breaches suffered by various organisations in Malaysia.

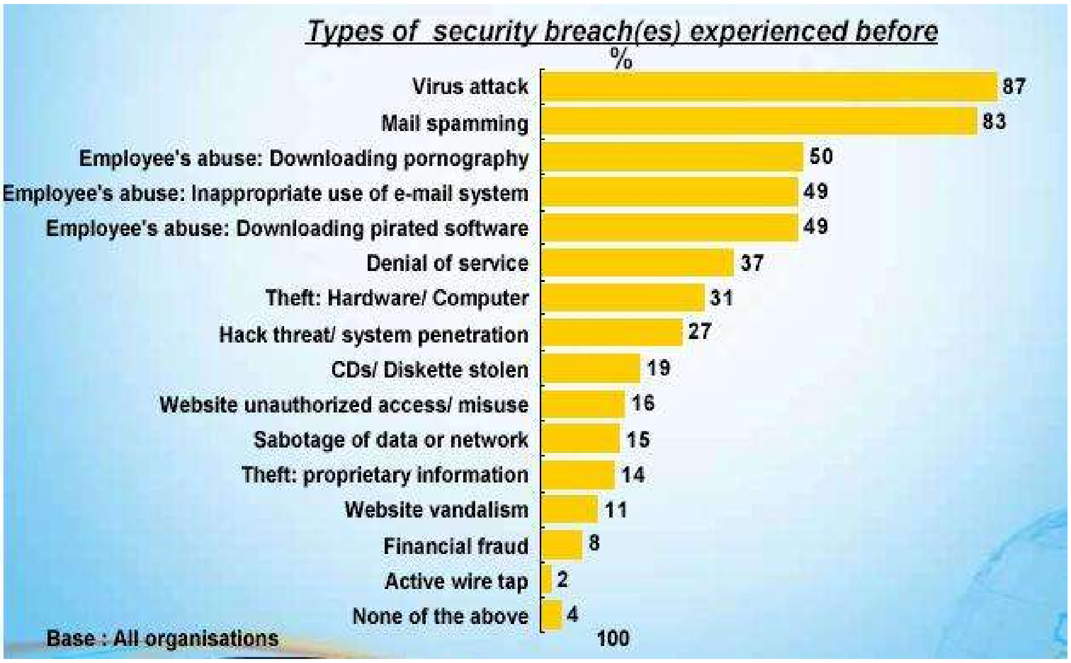

Diagram 1: Types of Security Breach(es) Experienced Before

Thus there is a more urgent need than ever to look at security from a holistic perspective, and to have a security management methodology to protect vital information systematically. This is where the need for ISMS comes in and the role that the coordinators of the pilot program plays are critical to ensure that ISMS implementation becomes more widespread and successful in the country.

III. NISER – SIRIM QAS ISMS PILOT PROGRAMME

National ICT Security & Emergency Response Centre (NISER) and SIRIM QAS International Sdn. Bhd. which is a wholly owned subsidiary of SIRIM Berhad jointly conducted the Information Security Technical Expertise for ISMS (Information Security Management Systems) Pilot Program. The certification is offered by SIRIM QAS and is based on the British Standards Institute's (BSI) BS 7799-2:2002.

Overall, the pilot program is expected to benefit the participating organisations tremendously in terms of improving their information security setup and ultimately it is expected that other organisations will follow suit and undergo a similar process to better protect themselves from information security breaches.

NISER's role in the pilot programme is to provide the expertise in ISMS for training and auditing; functioning from an advisory role. Thus, since NISER has been involved in different areas of the programme since it's commencement, NISER is in the best position to review the programme as a non-bias and independent source and provide comments that can be used as a guide or reference in the same topic for public consumption.

IV. COMMON SHORTCOMINGS IN ISMS IMPLEMENTATION

Since NISER together with SIRIM QAS have conducted a number of audits of the extent to which participating organizations have complied with the ISMS requirements, we have had the opportunity to observe a number of common shortcomings associated with ISMS implementation. Thus, the purpose of this paper is to raise them to the attention of interested parties, such as the participating organisations as well as other organisations interested or currently in the midst of implementing ISMS, in the hope that they will be seriously considered and addressed as consistently as possible. In this section, we will be looking at the identified shortcomings in detail.

On the whole, our findings mainly point to one conclusion: Among many participating organizations, there is a notable absence of a proper ISMS programme plan. Obviously, this underlying deficiency is a major drawback to the success of the programme itself.

This paper classifies our findings into two broad areas – technical and management.

A. Technical Shortcomings

a. Incomplete Risk Assessment Process

From our findings, we discovered that most of the organisations that have conducted the risk assessment process did not manage to do one that is comprehensive and consistent. The major concern faced in this area is that the implementor cannot link and justify the appropriate controls that are being implemented, the risks that they are mitigating and the different types of threat and vulnerability that they are protecting against. Most of the organizations also did not assess the realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with the assets, and the controls currently implemented. Besides that, some of the organizations also did not define the acceptable level of risks.

b. Incomprehensive Asset Listing

A comprehensive asset list is a must in order to carry out the risk assessment activity thoroughly. We discovered that most of the organisations did not manage to perform this task efficiently and thus they did not manage to perform the risk assessment process well. This means that they did not manage to mitigate the risks to all their available assets as identified within the ISMS scope and this leaves the organisation vulnerable to security breaches.

c. Lack of Assurance for Controls Effectiveness

Once the risk assessment process and risk treatment plan is approved, the identified controls will have to be implemented. The major issue here is the level of effectiveness of the implemented controls; to see whether they are able to efficiently mitigate the risks identified in the risk assessment process. While it is generally accepted that there are many factors preventing the proper implementation of the best identified controls such as the lack of budget, lack of expertise and others, it is usually recommended that the best possible control is chosen for the best results.

d. Improper Interpretation of Controls

Another of the most common shortcomings observed. We noticed that most of the participating organisations referred only to the BS7799-2:2002 Annex A when they require guidance to implement the recommended controls and left out the ISO17799 document alltogether. It should be noted that the ISO17799 provides more precise details on the actual implementation guidance of the controls and should be referred to regularly during the implementation process.

e. Scope Minimisation

There are some organisations that did not choose the core business as the certification scope as recommended by the standard and chose a less critical division or business function instead. This practice is not encouraged as it is more critical to secure the core business function rather than others.

f. Difficulties in Developing Comprehensive BCP Plans

The BS7799-2:2002 standard requires the organisation to have a single comprehensive Business Continuity Management (BCM) framework. Many of the organisations did not have such a framework in place and the most common reason being thrown about is the lack of expertise and manpower to develop it properly. We also discovered that some of the organisations that do have a BCM framework in place did not regularly test their BCP plan and this reduces the effectiveness of their BCM setup.

B. Management Shortcomings

a. Lack of Documentations

ISMS requires the organisations implementing it to focus a lot of effort in preparing relevant documentations. Every single task involved during the ISMS implementation phase will need to be documented as proof of completion or to be used as reference for the auditors and thus its importance should not be overlooked.

b. Failure to Define Specific Roles and Responsibilities in Information Security

Most of the organizations failed to define specific roles and responsibilities in terms of information security. Usually, the job descriptions only specify general roles and responsibilities. This is critical as only by specifically defining each personnel's responsibility in performing their duties to ensure information security, each individual in the organisation will know the exact areas and assets that they need to protect against security breaches.

c. Difficulties in Conducting Regular Management Reviews and Implementing Suggestions

Majority of the participating organisations that we have came across did not conduct regular and continuous management reviews on ISMS and this has contributed to the failure to implement ISMS effectively. As with any other large-scaled projects, ISMS requires regular meetings to be conducted and recorded.

d. Lack of a Comprehensive ISMS Project Plan

Many of the participating organisations have failed to have a proper plan for the ISMS project and this is obviously a big drawback to ensuring the project's success. It has become even more critical by the fact that the ISMS project is usually managed by personnel holding dual posts in the organisation.

e. ISMS regarded as a one-off project, rather than a continuous one.

Once the BS7799-2:2002 certification is awarded to the deserving organisation, the certification requires the organisation to be audited annually throughout the approved term. Thus it is only logical that the ISMS shall be considered as a continuous exercise rather than a one-off project as the organisation needs to show it's commitment of ensuring information security.

f. Failure to Obtain Enough Support from Top Management

It is critical that the project team present their ideas, plans, budget and other resources required on implementing ISMS clearly to the top management and obtain their approval and full support before embarking on the project. It is vital to ensure that the top management fully agrees to support the project right from the start since most of the major decisions regarding the project will need to be approved by them.

g. Difficulties in Conducting Internal Audit

Internal auditing plays an important role in securing ISMS implementation success since it ensures that the implemented procedures are done according to the required specifications. Many of the organisations that we came across do not have enough resources or expertise to conduct internal audits. This poses a problem as not only performing internal audit is a mandatory requirement for completing ISMS, but since it also acts as a corrective mechanism for the ISMS project, it is a big loss to the organisation if it is not carried out properly. It is important to note that the internal audits that are being conducted should be ensured to be both comprehensive and detailed.

h. Difficulties in Writing Proper Security Policies, Procedures & Guidelines

Most of the organisations do not have in-house expertise to write their own proper security policies, procedures & guidelines and this causes the organisation to be unable to implement effective security measures as required. This is the major reason on why some of the organisations did not have specific and complete policies. Inability to do so also causes the management team's effort in developing a security culture in the organisation to be a failure.

V. CONCLUSION

The ISMS Pilot Programme has been a good platform for all the parties involved to learn the proper methods of effective ISMS implementation. As expected, there are many positives that can be taken from the running of the programme. We hope that by highlighting the common shortcomings that were discovered during the implementation phase, the public will be able to learn from them and improve upon the currently used methodologies to ensure better ISMS implementation.

REFERENCES

[1] "What is an Information Security Management System?" Available at http://emea.bsi-global.com/InformationSecurity/Overview/WhatisanISMS.xalter