NISER'S ISMS PILOT PROGRAMME EXPERIENCES: COMMON SHORTCOMINGS IN ISMS IMPLEMENTATION

By The National ICT Security and Emergency Response Centre (NISER)

The progress of data protection standards implementation in Malaysia is slowly gathering pace and its importance is becoming more and more apparent to organisations around the country.

This is the view held by NISER (National ICT Security and Emergency Response Centre) which is currently staging an audit on data protection methods in local organisations. The audit came at the heels of a pilot project called the Information Security Management Systems (ISMS) that NISER jointly conducted with SIRIM QAS International Sdn. Bhd.. NISER's role in this programme is to provide technical assistance in ICT Security to SIRIM QAS in terms of the development of the programme as well as providing training and auditing services.

The BS7799-2:2002 standard has been adopted in the pilot programme for certification purposes. The BS7799-2:2002 is the de-facto standard for data protection and is well accepted in international communities and thus was the standard chosen for the ISMS pilot programme. NISER and SIRIM QAS is currently still in the process of completing the audit process for the participating organisations.

Preliminary considerations

First off, according to En. Shamsuddin bin Abdul Jalil, a policy analyst at NISER, organisations should have a comprehensive ISMS plan and assign to specific people the exact areas that they should be responsible for protecting against security breaches. In reality, very few such plans are available, making it hard to gauge the plan's implementation success. The inability for the personnel to segregate and dedicate their duties to perform the ISMS tasks on top of their daily job activities has contributed to the delay or failure to implement ISMS properly.

Besides that, support from top management, it was found, falls below expectations. This raises the question of commitment: has management grasped the size of the impact of a serious security violation on sensitive company information? An attack is a very real threat that can happen at any moment. If organisations are seriously concerned about data security, then the people at the top should involve themselves with their project teams right from the start, scrutinizing their ideas, plans and budgets.

Then again, policies, procedures and guidelines need to be expertly scripted. After all, the ISMS requires documenting every implementation phase as proof of completion and as a reference point for employees, auditors and other relevant parties. The majority of the organisations in the pilot programme do not have sufficient/appropriate security policies, procedures and guidelines in place. Among the reasons are that because they do not have

knowledgeable and experienced staff capable of writing appropriate policies and also because they did not manage to carry out the risk assessment process comprehensively and thus they were not able to come up with the appropriate policies, procedures & guidelines based on the risk assessment results. In a few other organisations though, such documentations already exist but the quality of writing leaves much to be desired.

"Putting all that aside," said En. Shamsuddin, "most of the major issues found are at the technical level."

Technical shortcomings

First, the selection of the certification scope. It may seem as a trivial issue but it requires no further reinforcement that selecting an organisation's core business for the ISMS project is crucial to the success of its implementation. Anything less – and some organisations have chosen far less critical divisions – will certainly lead to the hazards of misreading danger signs as they occur.

Secondly, the risk assessment process. According to En. Shamsuddin, throughout the audit process, it was discovered that a number of organisations have managed to complete the risk assessment process in a comprehensive and effective manner and there were also some organisations that did not manage to do so well in that area. One of the reasons, he said, lies in inadequate asset listing. A comprehensive listing meticulously identifies assets most prone to security violations so that plans can be developed to mitigate risks occurring to them. It is essential for carrying out a thorough risk assessment. Clearly, organisations with a less well-endowed listing actually make themselves vulnerable to security attacks. Another issue, according to him, is regarding the choice of risk assessment methodology. Organisations need to ensure that the methodology that they choose to use is in accordance to the BS7799-2:2002 requirements.

That is not all. Once a risk assessment process is approved, controls need to be set up. The major issue here is whether such controls are competent enough to mitigate the identified risks efficiently. They could be if the people developing the controls are able to link them to the variety of sources from which risks may come. Then risk mitigation should become more efficient.

However, this is not happening. Most organisations, surprisingly, have not fully assessed the impact that external and internal threats can have on data protection while some have not even defined an acceptable level of risks that they can take should a security breach occur.

ISO 17799 or BS 7799-2:2002?

There is also a common misunderstanding on the use of the ISO17799 and BS7799-2:2002 standards. The ISMS certification is based against the British Standards Institute's BS7799-2:2002 which is the specifications for ISMS with guidance for use, not ISO17799, which is the code of practice for Information Security Management. As it is, quite a number of organisations chose to use exclusively the BS 7799-2:2002 without

referring to the ISO17799 standard. The issue here is that many organisations did not use the ISO17799 standard as mandated by BS7799-2:2002 as ISO17799 actually provides more precise guidelines on the implementation of the controls.

Conducting internal audits

So, is there life after the award of a certification? There is indeed more work. Said En. Shamsuddin, "Certification requires a continuous audit of the organization. There will be at least one audit on the ISMS set-up done by the certification body annually during the certification period and this is known as the surveillance audit. So, it is only logical that the ISMS to be considered as an ongoing exercise in information security rather than a one-off project." Thus it becomes very important for organisations to have a strong internal audit team to perform comprehensive ISMS audits so that they can be assured that the measures that they have put in place to secure their organisations are working as expected. In reality however, many organisations do not have sufficient resources to conduct internal audits. This can be a thorny issue as internal auditing is compulsory under ISMS. Besides that, the other major issue regarding internal audits is that they are often incomplete and does not cover all the areas required under ISMS.

Finally, regular reviews. Some of the participating organisations lack continual management reviews. It is a question of commitment. Said En. Shamsuddin, "This is actually detrimental to the very idea of data protection itself. Participating organisations should understand that constant reviews can put them on the track to successful data protection implementation. However, such reviews are few and far between." It is also discovered that for some of the organisations that do conduct regular reviews, most of the time these review meetings are not attended by the right personnel e.g. Top management, key ISMS driver/implementer etc. and thus the execution of the decisions made resulting from the meetings are not carried out appropriately.