CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 33 - (Special Edition/2012)

CyberSecurity MALAYSIA
Agensi di bawah MOSTI

Rakyat Didahulukan, Pencapaian Diutamakan

MOSTI
Kementerian Sains, Teknologi dan Inovasi

BERHATI-HATI DENGAN PERAGUT IDENTITI

Sentiasa bijak. Sentiasa selamat

www.CyberSAFE.my

Pejabat Korporat:
CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888
Email: info@cybersecurity.my | Talian Khidmat Pelanggan: 1300-88-2999 | www.cybersecurity.my

A MESSAGE FROM THE HEAD OF CYBERSECURITY MALAYSIA

Dear readers,

We are pleased to present a special edition of the eSecurity Bulletin. This special edition is a compendium of articles that have been published in our previous eSecurity Bulletins over the years. These selected articles cover ISO/IEC 27001 ISMS implementation in various perspectives and issues, and other relevant information security topics.

We have seen a fair share of issues in cyber security that serves as good lessons for our way forward. In the past, the cyber threats appear to occur in foreign countries and being committed by foreign entities. Such threats however, are already here in our cyber space, where several incidents are both posed by foreign and local pranks. Identification of the sources of these threats can be very challenging due to anonymity and the borderless nature of the Internet.

There are gaps in cyber security that needs to be addressed immediately as cyber threats are expected to be subtler, sophisticated and damaging in more years to come, and they are always on the rise. International organized criminals are using the same innovations to refine their areas of expertise in committing crimes replacing traditional methods. The situation is further worsened by user's negligence and ignorance, which in turn has led to continued growth in financial impacts.

In 2012 we have seen hacktivism, malware infection, cyber crimes, and misuse of social media looming at the top of the threats list. We have seen how classified networks and industrial control systems were compromised. And we have seen how such attacks have resulted in marred reputations and credibility. Globally, we are also concerned of more aggressive cyber threats perpetrated by state actors and non-state actors. Such threats can refer to anything from cyber espionage, malicious software (malware) infection and system intrusion to high-scale cyber attacks with diverse political, economical and military motives. The threats are obvious and they are executed with technical complexity and sophistication.

It is indeed our concern to stay safe in our cyber space, with the desire to look good at the same time. We have to cooperate, collaborate, and combine our talents and ideas in order to formulate a viable and coherent cyber security approach. As such, we collectively, can earnestly begin confronting the cyber threats from a full security perspective.

I would like to thank and commend all contributors for their nobility of sharing invaluable knowledge with others and also for their continuous support towards our goal of enhancing online safety. Keep those keyboards clicking!

Happy reading!

Warmest regards
Zahri bin Hj Yunos
Acting Chief Executive Officer, CyberSecurity Malaysia

TABLE OF CONTENTS

READER ENQUIRY
Security Management and Best Practices, CyberSecurity Malaysia, Ministry of Science, Technology and Innovation (MOSTI) - E-mail: smbp@cybersecurity.my

PUBLISHED AND DESIGNED BY
CyberSecurity Malaysia (726630-U)
Block A, Level 8, Mines Waterfront Business Park, No 3,
Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan.

Information Security Management System (ISMS) Audit Evidence

By | Abd Rouf Mohammed Sayuti

Abstract

ISMS auditor often caught in a compromising and complex position of whether to believe evidence and oral description of a control implementation provided by an auditee, or look for evidence including observe the process himself or herself.

Standard 2310: Identifying Information from The IIA's International Professional Practices Framework (IPPF) for the Professional Practice of Internal Auditing requires internal auditors to gather "sufficient, reliable, relevant, and useful information to achieve the engagement's objectives". This article intends to provide insight on what is available in the ISMS audit evidence menu.

Introduction

Objective evidence is about evidence reliability and it can vary greatly. Firsthand evidence acquired by ISMS auditor or obtained from independent sources outside the audit area is considered more reliable. For instance, observing receptionist issuing visitor/contractor pass is more reliable than listening to his or her oral description of the issuance procedures and processes because the auditor can see whether the pass is issued correctly.

Objective Evidence

The key attribute of objective evidence is reliability. Many factors influence the reliability of specific types of ISMS audit evidence.

Physical Examination

The ISMS auditor's inspection on notebook computer screen saver password and lock are used to verify controls against unauthorized access and theft, respectively. Physical examination is usually a highly reliable form of evidence as *seeing is believing*.

However, the objectivity of physical examination depends on the examiner's qualifications. Certain IT asset, such as operational systems may require specialized expertise to identify correctly. ISMS audit team leader should consider engaging technical experts from outside or working with neutral internal technical experts to examine the equipments if ISMS audit staff lacks the requisite expertise. And while physical examination provides objectives evidence that an IT asset exists, it provides little evidence the asset is properly maintained by the administrator.

Inspection of Records

In perhaps the most common type of ISMS audit procedure, ISMS auditors reviews paper and electronic source records. For instance, reviewing operational system maintenance plan and information systems audit tool generated report to determine whether preventive maintenance conducted periodically and whether ISMS controls are functioning as intended.

The reliability of documentary evidence depends on its origin and the strength of the auditee's ISMS control. Records of external origin – those generated by or handled by external parties are generally more reliable than internally generated records. Internal record may be generated at will, but it is more difficult for an auditee to fabricate or alter an external record such as maintenance service report, and invoice from vendor.

Internal records generated under conditions of effective ISMS controls are more reliable than internal records generated when ISMS controls are weak because strong controls reduce the likelihood of errors in the records or minimize the likelihood of information falsification. And original records or secured digital copies such as in Portable Document Format (pdf) by Adobe Systems are preferable to photocopies or facsimiles.

Confirmations

ISMS auditor might obtain written responses from independent third parties such as vendors to verify accuracy or validity of the preventive maintenance records and from operational system end-users to verify

problem report lodged via memo, e-mail or helpdesk system.

Care must be taken to prevent auditee's influence on the confirmation response because a confirmation's reliability depends on the provider's independence. Although the auditee may prepare the confirmation request, it is best that ISMS auditor verify the recipient's address, control the mailing process, and receive the response directly. And if e-mail system is being used, direct the confirmation response to the ISMS auditor's own e-mail address.

Inquiry

ISMS audit related information from auditee's rarely can be considered conclusive evidence because of possible bias, error, or deception. ISMS auditors often use inquiry to obtain information about an auditee's ISMS processes and controls, but answers to inquiries should be substantiated with other ISMS audit procedures. For instance, ISMS auditor should inspect records and observe audited area's employees to verify that ISMS controls are operating as intended.

Reliability of evidence obtained by ISMS auditor through inquiry may be improved by asking the same question on several people. Information obtained from one person is less reliable in comparison to consistent information obtained from two or more people. ISMS auditor need to perform additional verification if answers to the same question are conflicting. Asking leading questions to auditee should also be avoided. Internal ISMS auditor should ask Documents and Records Controller to describe the ISMS procedures for identifying obsolete documents instead of asking the controller if obsolete physical documents have been identified and shredded.

Observation

Watching a process or procedure being performed by others is primarily intended to test whether ISMS controls are functioning as described. For instance, ISMS auditor often observed the company's employee for *close-door policy* during the normal office hours to determine whether the prescribed physical security policy is being followed. The limitation of observation is that employee may behave differently in the ISMS auditor's presence than they normally behave when the ISMS auditor is absent. The countermeasure to improve reliability of observation is by observing a process or a control implementation more than once, in more than one place or outside the normal office hours and making unannounced visits.

Reperformance

ISMS auditor re-performs ISMS controls procedure rather than watching an employee perform a procedure to see whether it was done correctly and to assess whether ISMS controls are functioning as intended. For instance, doors to restricted areas are equipped with biometrics access system to prevent unauthorized access. To test whether this control is working, ask randomly select employees to enter these areas. If none of them gained entry to the restricted areas, the ISMS auditor has evidence that the control is operating effectively. Oftentimes, reperformance is considered the most reliable evidence of an ISMS control's effectiveness due to the limitations of inquiry and observation.

ISMS Auditor Conclusions

Relevant and reliable ISMS audit evidence complements ISMS auditors' conclusions. In many cases, the procedures used to gather evidence determined the objectivity of the ISMS audit evidence. During ISMS auditors planning process, design methods that ensure objective evidence will be obtained. And assigned appropriately-qualified people to examine IT assets, request for original documents if available, scheduled multiple unannounced observations of key ISMS controls, and ensure confirmations are prepared and mailed or e-mailed under the ISMS auditors' control. In each ISMS audit conclusion, ISMS auditors must carefully assessed the credibility of evidence gathered to avoid basing audit findings on unreliable evidence. ▪

References

1. MS/ISO IEC 27001:2007 – Information Technology - Security Techniques – Information Security Management Systems – Requirements (ISO/IEC 27001:2005, IDT) Copyright 2007

2. The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing

3. Internal Auditor February 2009 Volume LXVI:I

Business As Usual – Optimising the Business Continuity Initiatives

By | Ida Rajemee Bt Ramlee

Business Continuity Today

In today's business climate, Business Continuity (BC) is a common term significantly embraced and adopted by most organisations. In a ever demanding and highly competitive environment to give the best services possible, having implemented Business Continuity Management (BCM) will definitely reflect stronger competitive edge and better positioning from the rest.

Within several sectors, statutory and regulatory compliance demand a comprehensive BC programme and plans. For instance, the Central Bank of Malaysia has published the BCM guidelines that became effective in January 2008. On a wider scope, BS 25999, a British Standard launched in 2007, regulates BCM programme implementation and management. Having these guidelines and standards, minimum BCM requirements can be enforced to ensure the continuity of critical business functions and essential services within a specified time frame in the event of a major disruption. Subsequently, this will promote customer confidence, ensure regulatory compliance and protect an organisations' reputation.

Based on the recent report published by Marsh's 2010 Europe, the Middle East and Africa (EMEA) Business Continuity Benchmark Report, the BCM maturity levels within an organisation can be measured by having BCM aligned to strategic business objectives. It is important to ensure that all resilience initiatives will align BCM with the overall organisational culture and in making strategic business decisions. This is represented in the chart below where as high as 66 percent of respondents agreed to this.

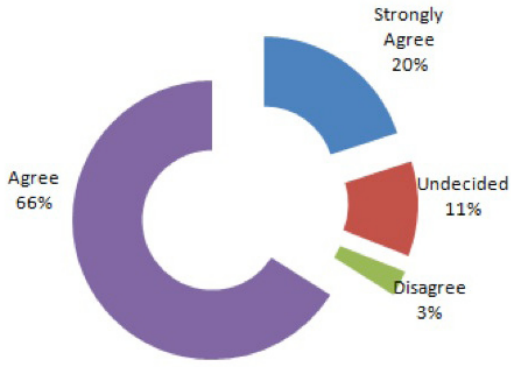


Figure 1: *BCM alignment to strategic business objectives.*

BCM now is no longer a jargon to most organisations concerned with providing continuous services with greater resilience for their customers. In order for this to become viable, a lot of effort and initiatives must be well planned, understood and embedded into an organisation's culture. This article seeks to explore the various main initiatives for organisations to have 'Business-As-Usual' (BAU) on unusual days.

Business As Usual – Ideal Recovery Value

During a crisis, services provided are anticipated not to be at its fullest capacity. Customers will be informed beforehand with a defined Service Level Agreement (SLA) prior to subscription. For instance if the Helpdesk System is down, services are still available but probably an analyst can only resolve 10 tickets in two hours instead of the normal capacity of 20 tickets per hour. In this situation, customers are able to accept and tolerate the fact that business is up but not at full capacity rather than not having the services at all. A lot of planning and initiatives directly related to Business Continuity must be in place and well thought out to ensure critical services are continuously available at acceptable levels. Referring to the article, Assessing your Organisation Business Continuity Capability and Maturity from CMÂ², it was stated that "Most company executives are exploring means of measuring the effectiveness of their BCM initiatives in terms of determining whether such initiatives will in practice, deliver true operational resilience when the unexpected occurs." CMÂ² also ranks organisation BCM capabilities based on a recoverability scale, grouped into five maturity levels as indicated in the table below:

MATURITY LEVEL	MAX SCORE	BRIEF DESCRIPTION
5	95% ≥ 100%	Recoverability is certifiable to BS 2599
4	61% ≥ 94%	Can recover all mission critical fucntions within agreed RTOs
3	41% ≥ 60%	Can recover some mission critical fucntions within agreed RTOs
2	21% ≥ 40%	Can recover limited business processes via informal...
1	0% ≥ 20%	Cannot recover or survive

Figure 2: *Organisation Business Continuity Capability and Maturity Matrix.*

The Recovery Time Object (RTO) as indicated in the above table and the Recovery Point Object (RPO) are two parameters determined during the Business Impact Analysis (BIA) phase. RTO is the time it takes to recover the specific critical business function within which applications and data that support a process, should be restored. It represents the recovery time of the system. On the other hand, RPO is the amount of data that can be lost before it affects the organisation. RPO presents the data quantity allowed to be lost when a disaster strikes or the point in time as determined by the business to which systems and data must be restored after an outage.

These two parameters provide guidelines on how fast critical business functions are recovered. For any resumption of critical business functions, the ultimate intention is to achieve RTO=0 and RPO=0. Having a 0 RTO in other words is translating that business is always available or possess 100 percent uptime on any critical business function, services or applications. Ultimately, this is the ideal value for RTO and RPO. However, these parameters are not mere figures determined by the BC implementation team. RPO and RTO must be confirmed by different operation demands after the risk analysis, as well as the minimum operating resources available to support the required critical business functions. To achieve 0 RTO and RPO may involve expensive failover servers, virtualisation to support business as well as data fault-tolerant and replication technologies.

Keeping in mind the value of RTO and RPO that need to be determined, how do organisations ensure 'Business-As-Usual' or the point at which the organisation is operating in a normal manner when a disaster strikes? RTO and RPO are the basis for identifying and determining possible strategies reflected in the business continuity to survive major incidents. By having BC programme and plans in placed, clients are assured that the organisations' critical business functions and critical services provided will be available even during a crisis.

The following topics will discuss on the main initiatives to be taken by organisation to ensure that returning to BAU is no longer a myth and what BAU entails.

Understanding Risks

"Business Continuity is responsible for managing operational risks associated with business disruptions in order to maintain operational resiliency. Any organisation with a risk-adverse focus should have comprehensive and effective business continuity plans." Quoted from the Disaster Recovery Journal – Executive Guide to Business Continuity, clearly indicates the importance of assessing risk within BCM. Amongst the common types of risk that may disrupt normal business operations include diseases, earthquakes, fire, floods, hurricanes, cyber attacks, sabotage, utility outages and terrorism.

During risk assessment, organisations will be able to understand the threats and vulnerabilities of all its critical business functions. Organisations should understand the impact that would arise if an identified threat became an incident and eventually cause business disruption. By understanding the risks, necessary counter measures can be taken with respective plans in place in order to reduce the likelihood of disruption, shorten the period of disruption or limit the impact of a disruption for key products and services. This can only be achieved if all BCM measures are adopted accordingly. On top of that, bear in mind that risk assessment is not a project-based initiative. It is an ongoing process, must be triggered by any emergence of new business processes, changes to the current business functions, and must be reviewed at planned intervals. This will help ensure that all identified risks with its associated risk treatment remained relevant and significant over a period of time.

Anchoring to Business Continuity Plans & Exercising

Exercises in BCM may vary depending on an organisation's needs and its operating environment. Types of exercises may range from the simplest one such as desktop reviews, walkthrough of plans and simulations to the most complex ones such as full simulation of BC Plans which involves incident management, crisis communication and activation of Disaster Recovery Center and relocating people to recovery sites.

Referring to the same 2010 EMEA Business Continuity Benchmark Report, it stated that the BCM plan main purpose is to recover critical business processes. The second largest reasons are to protect reputation and to protect revenue and profit. Having any BC Plans without testing it is as good as not having any plan at all. Exercises are compulsory and are a fundamental aspect of good BCM practice where plans can be validated. As reported in the BCM Report 2009: A Decade of Living Dangerously by Chartered Management Institute, 32 percent of respondents never rehearse their BC Plans.

For respondents that have their BC Plans tested, 75 percent agreed that the exercises had revealed shortcomings in the existing plans. With regards to this, not all exercises will bear fruitful outcomes to meet the intended testing objectives. Failed testing is also useful as it can be used to revamped, rectify and further improve the plans. It is good to have all test plans and scripts reviewed and approved for mutual understanding on what to be tested and achieved. In addition, well-written test scripts that reflects the common business scenario and environment shall include the scope of the test, its purpose and the respective personnel roles and responsibilities. These need to be taken into consideration for the exercises to be more realistic and significant. The business function owners, the BC implementation team as well as the management should all share the same test objectives and expectation. All exercised plans must be followed by observations reports and actions to be taken to resolve or rectify identified pitfalls.

For organisations with a lot of BC plans to support, a major concern is keeping the plan updated and reviewed regularly. It will be very unfortunate to find out that the plan is useless and although activated, it does not assist to resume critical business functions accordingly due to obsolete information. In order to avoid this, all critical business function owners should be given the responsibility to update the necessary details upon any invocation of changes to the business processes.

Top Management Support, Training & Awareness

Throughout the whole BCM implementation, top management officers are required to monitor and review its effectiveness and efficiency. This shall cover the organisation's BC policies, objectives and scope, and determine and authorise actions for remediation and improvement. Top management's commitment towards all BC initiatives is vital in ensuring a successful BC implementation. With top management buy-in, it makes it easier to get everybody else within the organisation to participate in business continuity activities.

The (EMEA) Business Continuity Benchmark Report indicated that 83 percent agreed that top management officers understands and provides full support as depicted in the chart below .

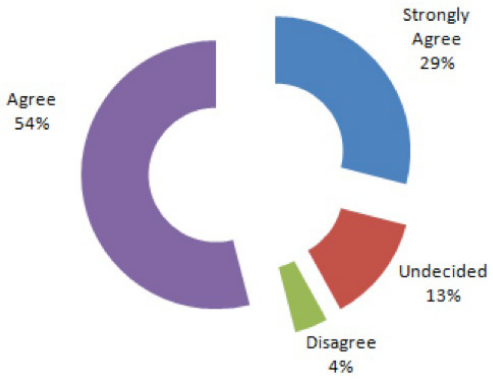


Figure 3: *Top management BCM understanding*

Based on this chart, it clearly showed that top management involvement for BCM related activities is very high and it is crucial for the top management to understand, review and agree to the contents of related BCM documentation. However, the lower percentage which constitutes the remaining 17 percent disagree and are undecided on the idea of making top management officers understand and provide support for BCM related activities within their organisations.

When this happens, the management may overestimate the actual recovery capabilities within their organisation. It may also trigger the possibility that the organisation's BC programme and plans are effective but the management fail to see the value and benefit of the whole BC initiatives.

Hence, to ensure total management comprehension, they need to be involved throughout the whole BC implementation. Management buy in can indirectly be obtained by involving them during BCM awareness

programmes along with other employees within the organisation. BCM Awareness programmes are vital in inculcating the importance of BCM for any organisation and must be an ongoing process. These programmes may significantly increase employees' knowledge and awareness to prepare them in responding to an event that caused an impact on the services provided, resources and the organisation as a whole.

By having these sessions planned regularly, employees will be communicated on their roles and support required from them to ensure service availability. All employees should have the basic understanding of BCM, and its importance to the company. Employees as well as the top management should also be heavily involved in the planning processes for their own business unit. For instance, a Business Impact Analysis (BIA) workshop followed by a Risk Assessment (RA), workshop attended by all business units within the organisation can speed up the BIA and RA process and will be of great assistance to the BC implementation team compared to having individual meetings or interviews with the respective business function owners. Consensus can also be obtained with unanimous decisions being made at the end of the workshop sessions.

Conclusion

The ultimate goal of having a BCM program is to ensure an organisation is able to survive any disruption, provide minimum critical operations and to return to BAU. With structured BCM programmes, availability of critical business functions and core services are assured and reduces the impact of incidents and faster recovery from incidents. An organisation without a strong BCM programme will in one way or another lose business or even be out of business.

As quoted from BS25999-2:2007 "Critical activities are underpinned by resources such as people, premises, technology, information, supplies and stakeholders." These resources are required in embarking on any BCM initiative and must be considered for strategic options to ensure resumption of organisations' critical activities. BAU depends upon these resources and its interdependencies as well as being the input to formulate and determine an organisation's BCM recovery strategies within the plans. All BCM programmes and initiatives are designed towards achieving a reduced impact of incidents and disruptions and faster recovery of incidents to assure that BAU is no longer a myth when disaster strikes and increases the organisation's ability to respond to a disruptive event. ▪

References

1. BS 25999 – 1 Business Continuity Management - Part 1 Code of Practice

2. BS 25999 – 2 Business Continuity Management - Part 2 Specification

3. 'A Decade of Living Dangerously : The Business Continuity Management Report' Patrick Woodman and Dr. Vidal Kumar, The Chartered Management Institute, March 2009

4. Lack of network scrutiny causes business continuity headaches - By Mark Holmes; line of business director for Network Integration, Dimension Data UK

5. Marsh's 2010 Europe, the Middle East and Africa (EMEA) Business Continuity Benchmark Report

6. Disaster Recovery Journal- Executive Guide to Business Continuity Special Report

7. The Business case for BCM, Business Continuity Institute

8. Assessing your Organisation Business Continuity Capability and Maturity http://continuitymauritius.com/index.php?option=com_content&view=article&id=98&Itemid=149

9. Study on the Design Principles of Data Disaster Recovery System for Hospitals http://ccsenet.org/journal/index.php/cis/article/viewFile/3428/3105-

10. Computer Technology Review -Disaster Recovery for the Masses - The Role of OS-Level Server Virtualization in Disaster Recovery by Carla Safigan

ISMS Certification: Mandatory policies and procedures

By | Noor Aida Idris

Introduction

Organisations that have plans for Information Security Management System (ISMS) implementation and certification must refer to the standard - *ISO/IEC 27001:2005 Information Technology – Security Techniques - Information Security Management Systems - Requirements*. This ISO standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organisation's overall business risks . The Information Security Management System (ISMS) provides an organisation the means to protect and manage their information based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.

Clause 1.2 of the ISO/IEC 27001:2005 states that organisations are not allowed to exclude any of the requirements specified in Clauses 4, 5, 6, 7, and 8 when they wish to claim conformity to this standard. Thus, organisations should understand, interpret and comply with these clauses when implementing ISMS, and eventually obtain the ISMS certificate. This paper will assist organisations to achieve ISMS certification by discussing one mandatory information security policy and five procedures which are stated in Clause 4 to Clause 8 of ISO/IEC 27001:2005. *(Note: organisations should take note that there are other information security policies and procedures that they may be required to produce before they can achieve ISMS certification).*

The policies and procedures which will be discussed in this paper are ISMS Policy, Documents Procedure, Records Procedure, Internal ISMS Audit Procedure, Corrective Action Procedure and Preventive Action Procedure. *(Note: the names given to the mandatory policies and procedures discussed in this paper are just examples. It should not be an issue if organisations have different names for their policies and procedures, as long as the objective and content of policies and procedures conform to the ISO/IEC 27001 standard).*

ISMS Policy

The first and only information security policy that organisations should produce for ISMS implementation and certification is ISMS policy; as this is stated in ISO/IEC 27001:2005 clause 4.3.1 (a). Policy is typically a document that outlines specific requirements or rules that must be met . An ISMS policy is probably the most important document that organisations have to produce when they wish to implement ISMS. This is because the ISMS Policy provides an organisation with the definition of information security; as such it is needed to govern organisations in managing information security within their environment (or their identified scope of ISMS). This ISMS policy should be defined in such a way that it will describe an organisation, the organisation's business characteristics, location, assets and technology. Additionally, an ISMS policy should:

1. Include a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security;
2. Take into account business requirements and information security compliance obligations defined in laws, regulations and contracts;
3. Align with the organisation's strategic approach to risk management in general;
4. Establish paradigms against which risk will be evaluated; and
5. Be endorsed by management.

The content of the ISMS policy needs to be produced properly so that it suits the organisation's style and workability. In general, a policy should have the following components :

- A statement of the issue that policy addresses.
- A statement about your position on the policy.
- How the policy applies in the environment.
- The roles and responsibilities of those affected by the policy.
- What level of compliance to the policy is necessary.
- What actions, activities and processes are allowed and which are not.
- What are the consequences of non-compliance.

The ISMS policy also should be disseminated and distributed and communicated to the intended staff and external parties (e.g. vendors, customers, if any). Finally, it is very important for the ISMS Policy to be reviewed regularly; to ensure the contents remains relevant, valid and accurate.

Documents procedure

The next focus will be the procedures. The first procedure that most (if not all) organisations should produce is a Documents Procedure. This is stated in 'clause 4.3.2 Control of documents'. This procedure is needed to ensure documents required by the ISMS are continuously protected and controlled. This procedure should provide descriptions and requirements for:

1. Approving documents for adequacy before it can be issued/used;
2. Reviewing, updating and/or re-approving documents;
3. Identifying changes and current revision status of documents;
4. Ensuring relevant version of documents are available whenever needed;
5. Ensuring documents to be legible and readily identifiable;
6. Making documents to be available to authorised users; and transferring, storing and disposing documents according to their classifications;
7. Identifying documents of external origin;
8. Controlling distribution of documents;
9. Preventing unintended use of obsolete documents; and
10. Applying suitable identifications to obsolete documents (if they are retained for any purpose).

Records Procedure

In addition to documents, records are equally important to organisations to

ensure conformity to ISMS requirements. They should remain legible, readily identifiable and retrievable. Thus, as part of ISMS implementation and certification, organisations should provide a Record Procedure as stated in 'Clause 4.3.3 Controls of records'. This procedure should define processes for:

1. Identification;
2. Storage;
3. Protection;
4. Retrieval;
5. Retention time; and
6. Disposal of records related to effective operation of the ISMS.

(Note: Documents and records discussed here may be input/output for any activities, processes or methods performed by an organisation to ensure the effective planning, operation, maintenance and control of its ISMS. They may be in any form or type of medium).

Internal ISMS Audit Procedure

The next procedure that organisations should have is an Internal ISMS Audit Procedure. 'Clause 6 Internal ISMS audits' states that organisations must conduct internal ISMS audits regularly. Thus, it is important that audit criteria, scope, frequency and methods for internal ISMS audit to be defined accordingly. This procedure should define responsibilities and requirements for:

1. Planning ISMS internal audits;
2. Conducting ISMS internal audits;
3. Reporting results of ISMS internal audits; and
4. Maintaining records for ISMS internal audits.

Corrective Action Procedure & Preventive Action Procedure

The last two procedures are quite related to each other and therefore many organisations usually combine them. A Corrective Action Procedure is needed to ensure organisations take actions to eliminate the cause of nonconformities with the ISMS requirements to prevent any recurrence. A Preventive Action Procedure is quite similar to Corrective Action Procedure, but having a different objective. The objective of this procedure is to eliminate the cause of potential nonconformities with the ISMS requirements in order to prevent occurrence. These 2 procedures are required based on 'clause 8.2 Corrective action' and 'clause 8.3 Preventive action'.

A Corrective Action Procedure should document the requirements for:

1. Identifying nonconformities;
2. Determining causes of nonconformities;
3. Evaluating the need for actions to ensure that nonconformity do not recur;
4. Determining and implementing the corrective action needed;
5. Recording results of action taken; and
6. Reviewing of corrective action taken.

And a Preventive Action Procedure should:

1. Identify potential nonconformities and their causes;
2. Evaluating the need for actions to prevent occurrence of nonconformity;
3. Determining and implementing required preventive actions;
4. Recording results of actions taken; and
5. Reviewing of corrective actions taken.

As a summary, table 1 below lists the mandatory policies and procedures:

Conclusion

Policies and procedures discussed in this paper are mandatory for organisations

Requirements in ISO/IEC 27001:2005	Mandatory Policy/ Procedure
4.3 Documentation requirements 4.3.1 General The ISMS documentations shall include: a) Documented statements of the ISMS policy ...	ISMS Policy
4.3.2 Control of documents ... A documented procedure shall be established to define the management actions ...	Documents Procedure
4.3.3 Control of records ... The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.	Records Procedure
6 Internal ISMS audits ... The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.	Internal ISMS Audit Procedure
8. 2 Corrective action ...The documented procedure for corrective action shall define ...	Corrective Action Procedure
8.3 Preventive action ...The documented procedure for preventive action shall define ...	Preventive Action Procedure

Table 1: *List of Mandatory Policy and Procedures*

that wish to be ISMS certified. However, there are other policies and procedures that needs to be developed (especially if controls in ISO/IEC 27002:2005 Code of practice for Information Security Management are selected). Examples of these are policies and procedures for data backups, password management, security testing of application systems, information security incident management response, business continuity management etc. Lastly, whichever policy or procedure that is in place, organisations should ensure that they are appropriately implemented and maintained so that the ISMS remains effective, efficient and successful. ▪

References

1. [1] ISO/IEC 27001:2005 Information Security Management Systems

2. [2] http://www.sans.org/security-resources/policies/

3. [3] Weise, J, 'Developing a Security Policy', December 2001

4. [4] ISO/IEC 27001:2005 Information Security Management System (Clause 4.3.1, Note 2 & 3)

5. ISO/IEC 27001:2005 Information Technology – Security Techniques - Information Security Management Systems – Requirements

6. ISO/IEC 27002:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management

7. Weiss, J. "Developing a Security Policy", Sun BluePrintsTM Online, December 2001.

8. http://www.iso27001security.com

Security Threats at The Gate: Challenges to SME

By | Sabariah Ahmad

Introduction

The emergence of information technology including the extensive use of the Internet has changed the way in which small and medium sized enterprise (SMEs) run their business. The massive adoption of the Internet has allowed SMEs to use information more effectively by allowing their customers, suppliers, employees and partners to access the business information they need, when they need it.

It works not only as a means for communication, but also for business promotion. While all these Internet-enabled services provide access to valuable business information to a bigger group of people efficiently and at a reduced cost, it also opens it up to potential risks and threats. Computer virus, loss of sensitive business information or data leakage, loss of privacy, down-time and loss of brand name reputation, if are not handled in an appropriate manner, can turn away new and existing customers. Furthermore, if these situations are not controlled quickly, it can cause significant loss and may lead to legal disputes.

The Challenges

Information security becomes imperative in balancing the opportunities offered by information technology and the potential risks that comes with it. However, it is a challenge for any SME in their quest to align e-business functions with security processes. A survey carried out among Malaysia's e-business users in early 2000 found that 70 percent of them believe that security is the most important barrier to e-business development. Many perceive the security risk of Internet-enabled services are quite high thus, are reluctant to engage it. Another survey concentrating on SMEs found that although the majority of them believe information security breach would be detrimental in achieving their business objectives, very few are putting security as a primary issue due to restrictions in resources from other business related priorities.

This paper aims to assist SMEs to prevent and effectively mitigate security threats and encourage its adoption so as to build the confidence among SMEs to do business online.

Security Threats that Affect SME

According to GFI Software, there are four categories of security threats that are likely to target SMEs as shown in figure 1 below. Each category branch out to multiple possible incidents or constitute part of the cause that contribute to these threats.

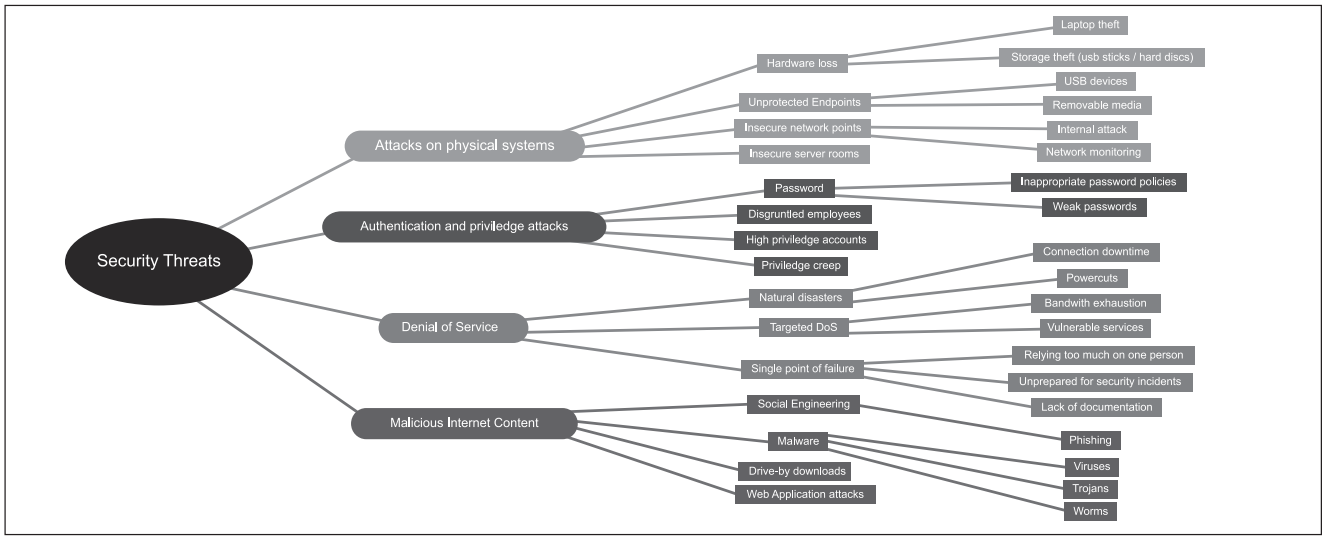


Figure 1: *Security Threat Map [source: GFI Software]*

Malicious Internet Content

The Internet is increasingly becoming an important tool for businesses and for SMEs as it is now the primary means of communication. However, many organisations were infected by malwares and SMEs are not spared. Malware is a term that refers to computer viruses, worms, Trojans and any other kind of malicious software. Malware can be introduced on the network by running the malicious executable code (EXE files) or even through basic software packages installed on desktop computers such as Internet Explorer, Firefox, Adobe Acrobat Reader or Flash.

Many SMEs networks cannot afford to employ prevention mechanisms such as network segregation and so this can be the factor for a worm to spread throughout an organisation. Additionally, most SMEs make use of servers for email, customer relationship management and file sharing. These servers tend to hold critical information that can easily become a target of an attack.

Denial of Service

Denial of service (DoS) is an attack that prevents legitimate users from making use of a service. Once a DoS attack is launched, it can lead to system downtime and may result in losing customers' confidence towards an organisation. One can only imagine the devastating situation when DoS attack forces websites accessed by millions of people to temporarily cease operation.

Apart from targeted DoS attacks, denial of service can also be caused by a single point of failure. Most small and some medium-sized enterprises have various single points of failures probably due to their attempt to minimise costs or just plain negligence. Having a single point of failure can result in lost of productivity and lost of business and this is very damaging for any organisation.

Authentication and Privilege Attacks

In most SMEs, it is unlikely to see work segregation such as network operation, system administration, security analysis or project management done by full-time dedicated personnel. This is due to the high remuneration these types of work demand. It is often found that only a single personnel, particularly a system administrator is assigned to do these tasks and is given the privilege to access important services or servers. With full access privileges, it gives the person an avenue to plan a logic bomb, create back-door accounts or leak sensitive company information that eventually compromise the stability and reputation of an organisation.

Another threat that compromise systems is password vulnerability. Hacker may use a programme that will utilise all variations of letters, numbers and special characters in an attempt to find a valid password. Although password policies can mitigate the risk, if it is too strict and poses a hassle, people will usually try to find other ways to get the information. Another point to note is that, password policy which are too strict in nature may be deployed to employees for authentication, but when it comes to customers, it must have a balance between security and usability as the customers will eventually take their business elsewhere.

Attacks on Physical System

Apart from threats from the Internet, loss of valuable business information can also take place due to stolen laptops or missing disks. DatalossDB[1], in their recent report, states that 20 percent of data loss is due to stolen laptops as shown in Figure 2. More often than not, this device contains important corporate documents and is used to log on to the company's network. This type of physical theft can happen to any business of any size and SMEs are not excluded.

The unprotected endpoints such as USB ports and DVD drives can be used to leak data undetected and introduce malware on the network. USB devices such as flash drives, iPods and other portable media players are commonly used by employees for legitimate applications and thus they become easy devices for data thief. Untoward incidents can happen due to negligence or possibly the work of a targeted attack. A disgruntled or dishonest employee can take large amounts of valuable business information out of the company.

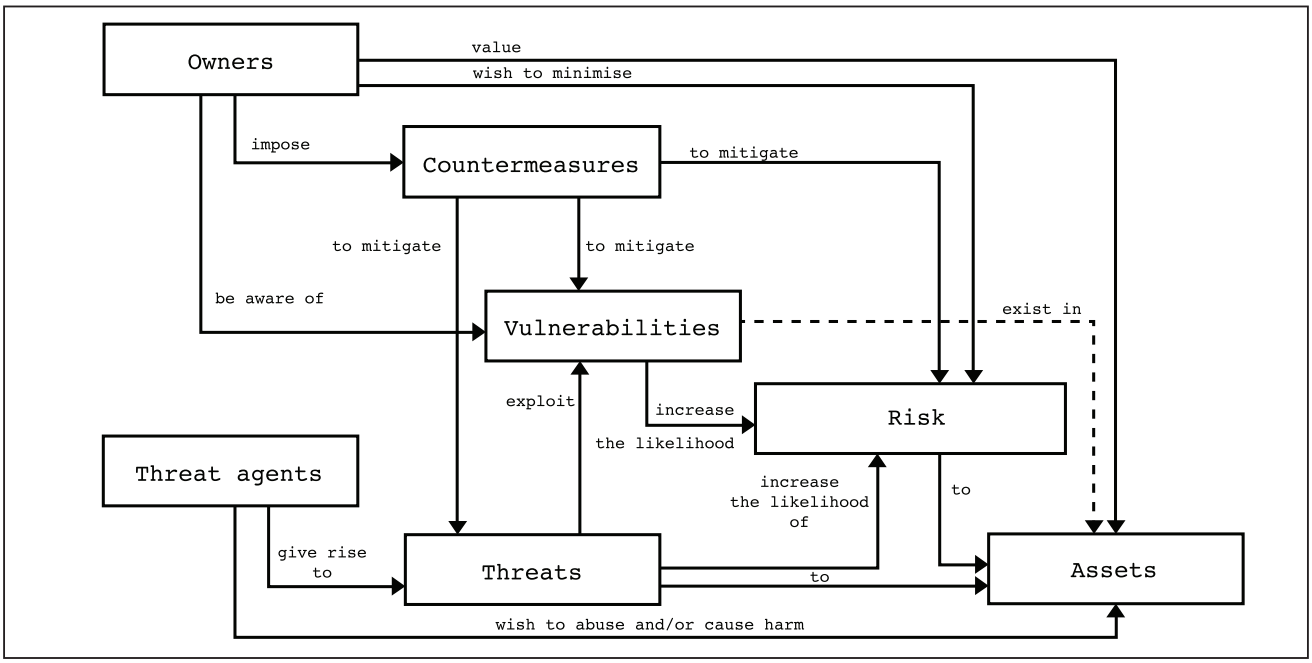


Figure 3: *Security Conceptual Framework*

How to Manage the Security Threats and Vulnerabilities

Implementing a security plan that provides the best possible response to threats and at the same time ensuring all resources are efficiently used pose a major challenge for SMEs. It is critical for SMEs to identify the vulnerabilities in their information systems in order to understand the threats that exploit them. Vulnerability is a weakness or in other words, the absence of security procedures, technical controls, or physical controls which will allow an attacker to reduce a system's information assurance.

Managing both threats and vulnerabilities requires detailed understanding of security concepts and their relationship with each other. Cyril Onwubiko and A. Lenaghan from Kingston University, UK came up with Security Conceptual Framework as shown in Figure 3 to assist SMEs in implementing the right mix of protection controls to identify and mitigate both threats and vulnerabilities. This Security Conceptual Framework is adapted from The Common Criteria (CC) – ISO/IEC 15408. Assets in this framework refer to anything that is of value and importance to the organisation. In this context it refers to valuable business

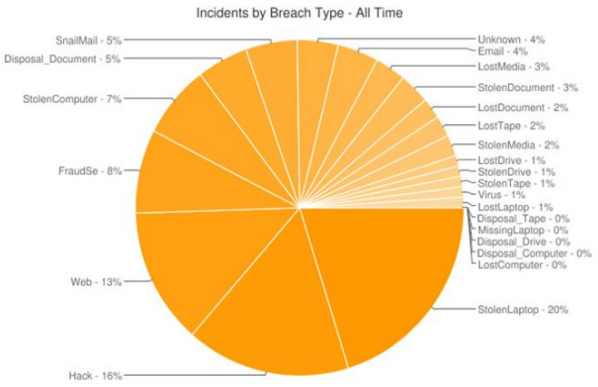


Figure 2: *Data Loss Incidents by Breach Type [Source: DatalossDB]*

Through this approach, SMEs can:

1. **Properly classify valued assets** – Using Asset Classification Schemes, assets are categorised as Insignificant, Minor, Major and Critical to determine their importance in an operation.
2. **Carefully identify vulnerabilities in classified valued assets** – Determine what should be protected and weaknesses that exist in or within those assets.
3. **Identify and mitigate potential threats imposed on assets** – Assess what can exploit these weaknesses.
4. **Appropriately evaluate associated risks** – Associate risks with vulnerabilities and potential threats that exploit those vulnerabilities.

5. **Adequately classify threats and their threat agents** – Decide on what can be imposed to prevent and mitigate identified threats.

The Security Conceptual Framework assists organisations to fully understand what is required to be protected (assets), what should be protected from (vulnerabilities, threats and associated risks) and how they can be protected (countermeasures). In short, this conceptual framework provides appropriate and efficient countermeasures to minimise risks to valued assets.

Checklist for Best Practices

While applying the Security Conceptual Framework to manage security threats and vulnerabilities, these are several best practices that SMEs can follow to better protect their assets.

Safeguard valuable business information

Understand what is required to be protected. Not every system and information resources need to be protected equally. Some are more valuable than the rest. Once they have been classified using Asset Classification Schemes, implement a complete protection solution to ensure they are safe.

Security Awareness

Security awareness programmes are important as employees need to know that while they are working and sharing information, they must be aware of the security issues that arise as a result of their actions. Besides telling the employees not to open emails from unknown senders, they also need to be told the risk of compromising information security to third parties. Any anomalies should be reported to an authorised person in charge of handling security incidents.

Policies

Develop a thorough and achievable security policy, implement it and update it at regular intervals. It must have the full support and commitment from the senior management. It needs to be communicated to each and every single employee and enforced accordingly.

Backup and Recovery Plan

Establishing a workable backup and recovery plan is critical to ensure business resilience for SMEs when faced with disasters. Not only backup has to be automated to avoid human error but it also has to be tested periodically. It is as good as having no backup system if restoration does not function properly or to expectations.

Deploy Content Filtering at the Gateway

Anti-virus can be part of the content filtering strategy where it can be installed at the email and web gateway. Often, email accounts are spammed with malicious email attachments that entice the receivers to run the malware code. By blocking the malware at the email gateway, the risk that a receiver mistakenly opens an infected file can be reduced.

Conclusion

In a world where information is currency, securing it from security threats becomes imperative. Ensuring the integrity, confidentiality and availability of information at all times is critical for the success of a business. When security systems are compromised, customers take their money elsewhere. By understanding the risks and employing the necessary safeguards, these threats can be eliminated or at least minimised. ▪

References

1) Norudin Mansor and Ahmad Faisal Amri Abidin, (2010), "The Application of E-Commerce Among Malaysian Small Medium Enterprises", European Journal of Scientific Research ISSN 1450-216X Vol.41 No.4 (2010), pp.591-605

2) GFI White Paper, (March 05, 2009), "Security Threats: A Guide for Small and Medium Businesses", www.gfi.com

3) C. Onwubiko and A.P. Lenaghan, (2007), "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises", IEEE International Conference on Intelligence and Security Informatics 2007

4) "Symantec 2010 SMB Information Protection Survey – Global Data", (June 2010)

5) Peter Lord, Mary Ann Davidson and Kristy Browder, (January 2002), "Managing e-Business Security Challenges", Oracle Corporation

6) Michael A. Regan, (16 August 2001), "The Computer Security Threat to Small and Medium Sized Businesses – A Manager's Primer", SANS Institute InfoSec Reading Room

7) "Economic Considerations of Website Password Policies" , (20 July, 2010) http://www.schneier.com/blog/archives/2010/07/website_passwor_1.html

8) "Data Loss Statistics", http://datalossdb.org/

9) "Secure e-business", www.tarrani.net/Security/securityebus.pdf

Steganography: Secure Information Hiding

By | Abdul Alif Bin Zakaria

Introduction

Network security has become a major concern due to increasing numbers of data transfer through the Internet. Confidentiality and data integrity are needed to protect us from unauthorised access. Digital audio, video, and pictures are exposed to infringement, causing music, film, book and software publishing industries to suffer tremendous losses. In this case, steganography can be applied to prevent this type of infringements from happening by providing copyright protection.

Steganography Overview

Steganography is a Greek word "Steganos", which mean covered or secret and "graphy" mean writing or drawing. Therefore, steganography means, literally, covered writing. In other words, steganography is the hiding of a secret message within an ordinary message and the extraction of it is carried out at its final destination. Steganography takes cryptography to the next level by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.

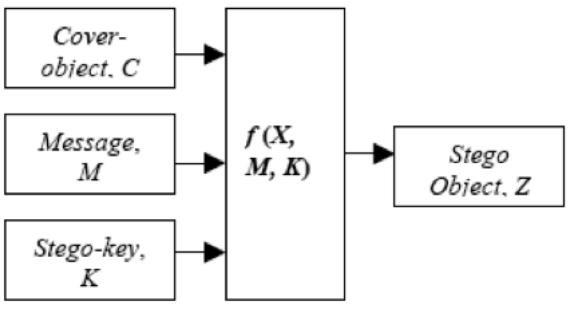


Figure 1: *Basic Steganography Model*
(Source: Information Hiding Using Steganography)

The basic model of steganography contains three main elements which are cover object, message and stego-key, which is shown in Figure 1. Cover object is also known as carrier in which a message is embedded and serves to hide the existence of the message. Message is the data in which the sender intends to keep it secret. It can be in the form of plaintext, ciphertext, image or anything that can be embedded in a bit stream such as copyright mark, a covert communication, or a serial number. Stego-key works as a type of password which will ensure that only a receiver who knew the key will be able to read the message from the cover-object. The cover-object with the secretly embedded message is then called the stego-object.

These are examples of carriers that reacts as cover object:

1. File and Disk that can hide and append files by using the slack space.
2. Image files where they can be both in colour and gray-scale (e.g. bmp, gif and jpg).
3. Network Protocols (e.g. TCP, IP and UDP).
4. Audio files that uses digital audio formats (e.g. wav, midi, avi, mpeg, mpi and voc).
5. Text files such as null characters, just like Morse code including html and Java.

Process of hiding information can be in many ways but in this article, we will discuss only one particular technique; by using an image file. We have to identify the redundant bit in the cover-object. Redundant bit can be changed or modified without damaging the quality of the cover-object. Message bit will be embedded into the redundant bit in the

cover-object. In this example a picture is used as the cover-object. Changes on embedded cover-object cannot be seen with the naked eye because the differences is too small. When the two pictures are compared, they almost look alike although there is embedded message in it.

Differences Between Steganography and Cryptography

Cryptography changes the structure of a message so that no one except the person who has the key can read the message. An attacker may intercept the message while data is being transferred because they were aware about the existence of the message. By attacking the algorithm or keys, it might authorise them to read the message.

Steganography is different from cryptography as it does not use algorithms to change the structure of a message. The main goal of steganography is to prevent an attacker from realising the existence of information by hiding the message. A key is needed to hide and reveal the message from the picture.

Although the two concepts are different, they can be applied together to add multiple layers of security. First, a message is encrypted using an encryption key to become a ciphertext. The ciphertext is then embedded into a picture and sent to a receiver. By doing this, an attacker might not have the chance to break the code or even if they have the opportunity, they need to work very hard to accomplish it.

Information Hiding Techniques

There are many methods of applying steganography. Here are several examples:

1. Least significant bit insertion (LSB)
2. Masking and filtering
3. Transform techniques

Least significant bit insertion is the easiest technique which embeds message bit into the least significant bit in the cover-object. Image size and message size must be determined by the system to allow the image to hold the embedded message. The ideal size of an image is 800 x 600 pixels which can embed up to 60 kilobyte messages. Any changes made to the picture are insufficient, as no one will realise the embedded message. Stego-image is sensitive to changes or manipulation. Scaling, rotation, cropping, addition of noise, or compression to the stego-image will demolish the message.

Masking and filtering techniques normally are limited for 24 bits and gray scale images. This technique hides information by marking the image just like paper watermark. Significant areas on the image are embedded with the information that needs to be hidden. The hiding concept in this technique is to make the information imperceptible by anyone. Only those who have authority will know the existence of the information.

Transform techniques embed the message by modulating coefficients in a transform domain, such as Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image or other variants.

Secure Information Hiding System (SIHS)

Information hiding systems has been widely used by many companies and institutions due to its reliability to provide secure communication transmission through the Internet. Applications on steganography are commercialised on

web sites and can be applied for learning purposes. In this topic, methods on the process of hiding information will be discussed for better understanding.

Since least significant bit insertion (LSB) is the easiest steganography technique, example of steganography methods will refer to this technique. A steganography website is recommended because it provides the application on these methods to hide messages in an image. Please refer to the web site link, http://mozaiq.org/encrypt for a clearer understanding on how steganography works.

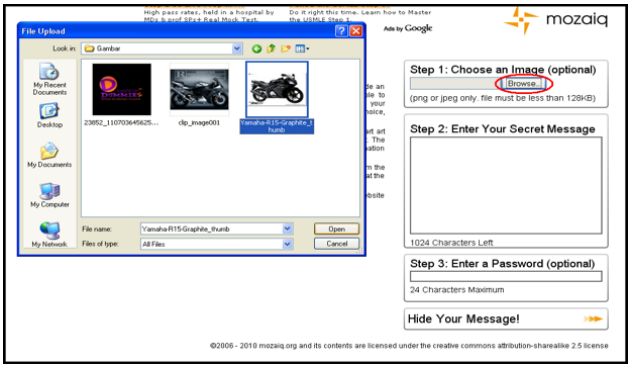


Figure 2: *Hiding Information Methods (Source: Mozaiq)*

The first step is to pick a cover object (image) to be embedded with the message, see Figure 2. The cover object size must be less than 128 kilobytes. This size restriction depends on the application or programme that was used. Every application has a different input requirement and condition.

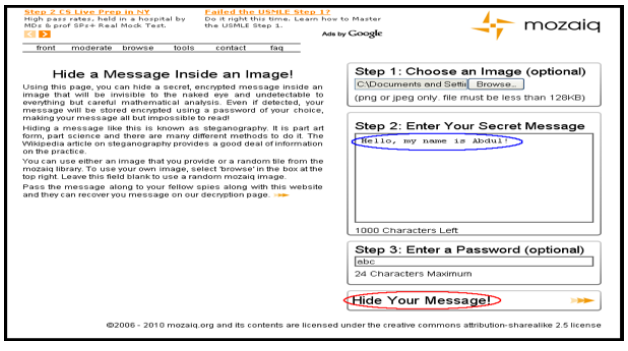


Figure 3: *Hiding Information Methods (Source: Mozaiq)*

All of the following steps below can be found in Figure 3. The second step is to write the secret message that needs to be sent. The message must be less than 1000 characters. The third step is to enter a password with a maximum of 24 characters. This password is also known as stego key. Stego key must be known by both sender and receiver in order to hide and reveal the secret message. After filling in the requirements needed, click “Hide Your Message”. This process is similar to encrypting a message in cryptography.

Figure 4: *Hiding Information Methods (Source: Mozaiq)*

The new image produced by embedding a secret message which is also known as stego object is shown in Figure 4. By comparing the image and stego object, it is hard to see any difference. This is to prevent an attacker from realising the existence of the information by hiding the message. Stego object has to be downloaded and can be renamed but cannot be altered (converting the image to another format, cropping, resizing, or drawing on the image). Any modification will destroy the hidden message.

To decrypt or reveal the hidden message, you can choose “decrypt” in the “tools” bar at the top of the web page, which is shown in Figure 5. The process of decrypting (hide) the message is almost the same as encrypting it (reveal). Browse

the stego object, enter the stego key, and click “Reveal Your Message!” icon.

Figure 5: *Hiding Information Methods (Source: Mozaiq)*

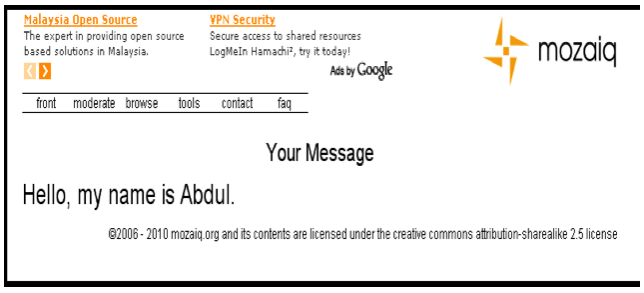


Figure 6: *Hiding Information Methods (Source: Mozaiq)*

Finally the secret message is revealed. It is interesting and can practically be used in any of our daily communication mediums. Elements needed to apply this programme are cover object (image), message, and stego key (key). Stego key must be kept secret and only be made known by those who have the authority on the message.

Conclusion

Information hiding can increase confidentiality of the information and provide privacy in our daily communication. Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Steganographic research is primarily driven by the lack of strength in the cryptographic systems on its own and the desire to have complete secrecy in an open-systems environment.

Laws were created by many governments which limit cryptosystems or even prohibit them from being used. This has been done as they fear law enforcement agencies will not gain any form of intelligence using wiretaps. This restriction caused the majority of the Internet community to use weak encryption algorithms that were thought to be unbreakable.

Many parties disagree with this form of enforcement and assuming these limitations are considered an assault on privacy. To add multiple layers of security, it is best to apply both cryptography and steganography together at the same time. Neither cryptography nor steganography were thought to be the “turnkey solution” to open system privacy, but by applying both technologies at the same time may provide an acceptable amount of privacy for Internet users. ▪

References

1. Mohammed, A.M. and Hussain, A.A. Information Hiding: Steganography and Watermarking

http://www.emirates.org/ieee/information_hiding.pdf

2. Muhalim, M.A., Subariah, I., Mazleena, S., Mohd, R.K. (2003). Information Hiding Using Steganography.

http://eprints.utm.my/4339/1/71847.pdf

3. Memon, N. Information Hiding, Digital Watermarking and Steganography

http://eeweb.poly.edu/~yao/EE4414/memon_F05_v2.pdf

4. Dunbar, B. (2002). A Detail look at Steganographic Techniques and their use in an Open-System Environment

http://www.sans.org/reading_room/whitepapers/covert/detailed-steganographic-techniques-open-systems-environment_677

E-Policy: Serve Your Company with Secure Environment

By | Amir Haris bin Zainol Abidin

Introduction

At the beginning of the twenty-first century, the places where government policy meets information security are multiplying. Now, Information and Communications Technology (ICT) has become one of the world's strongest and fastest growing. Although every country on the planet is connected to the Internet, many of them do not have a cybercrime law. The lack of a globally legal framework with respect to cyber criminal activities has become an issue which requires urgent attention of our country and all nations. Misuse of ICT facilities and application becomes an issue. One of many ways has focus on e-policy as the key.

The Emerging and Needs of E-Policy

Today, policy makers are coming from various backgrounds and agencies. The government should develop and spread principles designed to help policy makers ensure that legislative proposals do not affect e-commerce adversely, by providing an analysis of impact onto the local, national and international policy decisions and legislative proposals. Therefore, a unique network of senior policymakers, industry and thought leaders from around the world have created an Open ePolicy Group for that purpose. This group consists of global network e-policy experts with a mission to deliver tools and best practices to governments and enterprises to help them capture the benefits of open technologies in term of collaboration, cost and control. Open technologies (or Open ICT) refer to technologies and methodologies such as open standards, open source software, open architectures and open processes. The open concept has made e-policy unique when compared to conventional information security policy. Open e-policy is not owned by any entity, independent platform and publicly available.

Other than that, ePolicy Institute based at Columbus is another body to become a leading source of speaking, training and consulting services related to e-policy such as workplace email, instant messaging (IM), Internet, blog risks, and management. In Malaysia, government has showing tremendous effort towards development of information society. E-policy is the main key for that purpose and the implementation of eGovernment.

Since most of organizations today is equipped with the information technology, the need of e-policy could not been bore. Regardless whether organization is a publicly traded worldwide corporation, a mid-sized privately held operation, or a family-owned business, their rules to permit employees access to the computer systems and/or authorize the use of Internet, email and IM, they have actually put their organization's future, assets, and reputation at risk-. Employees' accidental misuse (and intentional abuse) of the Internet, peer-to-peer (P2P) technology, email and IM are some of examples that can generate potentially cost and time-consuming legal, regulatory, security and headaches for employers. Thus, e-policy is needed to mitigate and minimize the risks. Some scenarios will be discussed in next section.

Scenario

Scenario 1: People may be asking isn't it illegal for the employer to read their email? The answer is NO, it is not illegal. In fact, according to the federal Electronic Communications Privacy Act (ECPA), an employer-provided computer system is the property of the employer. The company

has every right to observe all email traffic and Internet surfing that occurs on the company's system. In other cases, most employers recognize some personal email use is warranted. While an e-policy may clearly state the company's email system is reserved for business use, the policy probably allows for brief communication between work and home. Email in office may be used to communicate in the case of personal emergencies for most organizations. The type of personal communication that is typically prohibited includes any correspondence that pulls people away from their job for extended periods of time. Generally what is prohibited is the posting of personal messages, such as campaigning for a political candidate, soliciting a charitable donation, or advertising a garage sale. An employer who wants to limit e-liabilities also will outlaw messages, personal or business-related, that are in any way offensive, menacing, or discriminatory.

Scenario 2: When software has been purchased, it includes purchasing a license to load the software onto one computer. It is not the software itself. Loading software that has a single user license onto other computers is illegal in action. The term for this is softloading. In addition to being ethically wrong, softloading puts the company at risk on a number of levels. People could carry a virus into the office via the software. If illegally duplicated software malfunctions, they will not be able to access technical support through the manufacturer's help line. And, if the software police come calling and find illegal software on their workstation computer (or other employees' computers), it is the company, not the individual employee, who will be held liable. Thus it is responsibility of all for minimizing potential licensing violation. Organization could appoint a software manager to monitor software installation, usage and license compliance. Adopt a written policy governing installation and copying of software, urge employees to report unlicensed software, educate employees about the risk of illegally copying software, and perform an internal audit/use metering software.

Scenario 3: There are literally billions of graphic illustrations and images in software programs and on the Internet. Many of these are in the public domain and may be copied freely, for example, to insert in Microsoft PowerPoint presentations. However, there are others with trademarked or copyrighted, and may not be copied or used without prompt permission of the copyright holder or trademark owner. It is employee's' responsibility to differentiate between public domain and copyrighted or trademarked graphic illustrations and images. The consequences to employee and the company of copying copyrighted video, games, and music are potentially very severe and could expose them to civil or criminal legal action. Therefore, e-policy content must specify any illustrations, documents, music files and video content (e.g. JPG, PDF, MP3, MP4, WMV, MPEG, etc.) must not be downloaded, stored or used on company ICT equipment unless the appropriate copyright protocols have been adhered.

How to Design and Implement E-Policy

Above paragraph is the example of the scenario and how e-policy could minimize the ICT risk. Those who are committed to preventing accidental and intentional Internet, P2P, email and IM abuse and reducing electronic risk are advice to put e-policy in place. To design and implement e-policy can be begun with three basic steps which are considered as best practices.

1. The first step is to set up clear and comprehensive written Internet, P2P, email and IM rules, policies and procedures for all compliers. These electronic policies are supposed to be easy for complier to access, understand and adhere to. This can be achieved with simple and not in vague language that may leave the policy open to individual interpretation. These policies should be updated annually or when necessary to ensure that rules, policies and procedures are always there and in place to govern new and growing risks such as blogging and other emerging technologies.

2. Secondly is to educate the complier. All written Internet, P2P, email and IM rules and policies should be supported with appropriate training. It is crucial to make sure all complier understand that policy compliance is mandatory. In some organizations, they make quizzes in regards with the policies to ensure complier is always aware about the content and compliances of the policies. Thanks to e-policy trainings and quizzes, people may find they are more compliant and the courts more accepting of the fact that they have made a reasonable effort to keep their organization free from discrimination, harassment, hostility, and other objectionable behavior.
3. For the third, empower with a combination of reward and disciplinary action on all written Internet, P2P, email, and IM rules and policies. Compliers who have fulfilled the policies requirement without fail should be rewarded as a token for their willingness to adhere to the policies. While disciplinary action should be taken to those who are inflexible to adhere to the policies. Both reward and disciplinary action are best handled by the management team who are responsible to ensure e-policies are adhered to. There is simpler method to achieve this if organizations doubt the motivation of the complier to comply with the policies. They could assign somebody or a department to install applications (or implement some methods) which works in concert with their Internet policies where they can block access to inappropriate sites and stay on top of complier online activity.

In addition to these basic steps, there is also e-policy maintenance in which the content should be updated accordingly and timely. The contents of a policy statement should rarely change and are such that they define particular actions from every employee in the organization related to the continuity of that policy. However, change in management, incident response and audit finding may cause amendment in e-policy content. The change in the content should be communicated to all compliers to ensure the e-policy is adhered and stay relevant.

It is a good practice for the compliers to sign and date each policy in writing for them to acknowledge that they have read it, understand it, and agree to comply with it or accept the consequences, up to and including termination. This is helpful when it comes to a workplace lawsuit, e-mail business records will be subpoenaed as evidence. As part of strategic e-mail management or usage policy program, "e-mail business record" for the organization could be define. Based on that definition, formal retention rules, policies, procedures, and schedules to business-related/business record e-mail can be applied consistently.

Conclusion

It is noted that there is much more things to put in the e-policy which can lead to good security practice in using the "e-related-stuffs". And all are aimed to goal of the e-policy which is to reduce potential liability, protect sensitive and proprietary business information and reduce waste of valuable corporate resources. Governments, policymakers and experts from around the world should share ideas and experiences about how best to address the emerging issues associated with of the development of a global information society, including the development compatible standards e-policy. The outcome will be vividly improving the commitment of all organizations and its family member towards the e-policy. ▪

References

1. Anderson, Ross, 2001, Security Engineering, E-Policy

2. Flynn, Nancy, 2006, ePolicy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure and Web Usage and Content

3. ITU, 2009, Understanding Cybercrime: A Guide for Developing Countries

4. Overly, Michael R., 2003, E-Policy

5. Flynn, Nancy, 2001, The ePolicy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies.

6. Schreiber, Mark E., 2000, Employer E-Mail and Internet Risks, Policy Guidelines and Investigation.

Software Product Liability from Information Security Perspective

By | Ahmad Ismadi Yazid B. Sukaimi

Introduction

Information is an asset that and like other important business assets, it is essential for a business entity and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversations. Management systems, based on a legitimate business risk approaches, to establish, implement, operate, monitor, review, maintain and improve information security must be in place.

This paper will discuss software ownership and responsibility issues from an information security management perspective clearly defining every form of responsibility. The responsibility of an owner is described under one of the ISO/IEC 27001 domains, the organisational aspects of information security and the control elements of dealing with external parties. In addition, perspectives from both Malaysia and the United States' will also be discussed.

Malaysia vs. US Landscape

Software vendors are likely to face increasing exposure to lawsuits alleging that software products did not perform as was expected when the real issues is really about software ownership. Many companies in Malaysia and US have been alerted with these issues and had incorporated certain disclaimers in their products in order to protect themselves from any security or physical incidents related to the usage of their software. Malaysia's premier online banking institution stated at their website [1] in particular that the bank shall not be liable for any loss or damage caused by any unavailability or improper functioning of the Mobile Banking-Service for any reason. This showed how serious they are in facing product liability issues. The same goes with a US based company, Microsoft [2] as stated at6 their website prohibiting software users from abusing their software in any manner that could damage, disable, overburden, or impair any of their servers, or the network(s) connected to any of their servers, or interfere with any other party's use and enjoyment of any services. Users are also warned to not perform any illegal attempt to gain unauthorised access to any of their services, other accounts, computer systems or networks connected to any Microsoft server or to any of their services, through hacking, password mining or any other means.

Definitions of Faulty Software

The ISO/IEC 27001 main objective is to ensure business continuity, minimise business risks and business interruptions, maximise return on investments and increase business opportunities. This can be achieved by increasing customer confidence in order to protect financial and intellectual properties to gain a positive reputation. Both Malaysia and the US are discussing the same main issue in deciding if software is considered "goods" or a "service". According to [6] Malaysia Consumer Protection Act 1999, the definition of "*product" means any goods and, subject to subsection (2), includes a product which is comprised in another product, whether by virtue of being a component part, raw material or otherwise. Under Section 3 of the [7] Malaysia Sale of Goods Act 1957 "goods" means every kind of movable property other than actionable claims and money; and includes stock and shares, growing crops, grass and things attached to or forming part of the land which are agreed to be severed before sale or under the contract of sale.*

Whereas under the [6] Malaysia Consumer Protection Act 1999, *"products" means*

products which are primarily purchased, used or consumed for personal, domestic or household purposes and includes products attached to or incorporated in, any real or personal property, animals, including fish, vessels and vehicles, utilities and trees, plants and crop whether on, under or attached to land or not, but does not include chooses in action, including negotiable instruments, shares, debentures and money.

In Section 6 under [8] Malaysia Civil Law Act 1956 *"fault" means negligence, breach of statutory duty or other act or omission which gives rise to a liability in tort or would, apart from this Act, give rise to the defence of contributory negligence. The liability of a person under this Part to a person who has suffered damage caused wholly or partly by a defect in a product. Moreover, [7] Section 62 of the Sale of Goods Act 1957: Exclusion of implied terms and condition as to where any right, duty or liability would arise under a contract of sale by implication of law, it may be negatived or varied by express agreement or by the course of dealing between the parties, or by usage, if the usage is such as to bind both parties to the contract, it gives two conflicting views on the part of the liability of the software programmer.*

Software can be defined as goods or services, whichever conforms to the user and the manufacturer. Software product liability can be defined as any liability, negligence, malfunction, warranty issues and subsequence negative effect that arise from the usage of the software, which can affect the users' environment such as incidents, losses, fraud and other negative impacts, and can be penalised under the respective country laws. The responsible parties are the owner of the software, the manufacturer, the programmer, the salesman and anyone who were directly involved in selling or providing the software to the user.

Manufacturer responsibility

To protect their products, software manufacturers use disclaimers and agreements between users and themselves. Users are forced to sign or click a button agreeing to the terms stated before proceeding to install and use the software. Many times, users are too lazy to read the fine print and continue the transaction by clicking the 'Agree' button without fully understanding the legal terms and conditions stated by the manufacturers. According to [3] Levy et al, in US, there are several case studies where manufacturers are facing legal action on faulty software related incidents. A construction company alleged that a bug in a spread sheet programme caused the company to underbid a $3 million contract. The company sued the manufacturer of the programme for $245,000, claiming it had lost that amount as a result of the incorrect bid. To date, in Malaysia, we do not have similar cases being brought into our courts, even though we legal grounds with regards to faulty software.

There are provisions under Consumer Protection Act, section 71 that states clearly about the responsibilities of manufacturers in Malaysia, *where any damage caused wholly or partly by a defect in a product, the producer of the product whose using his name on the product or using a trade mark or other distinguishing mark in relation to the product, has held himself out to be the producer of the product persons and in the course of his business, imported the product into Malaysia in order to supply it to another person shall be liable for the damage.*

Users can also apply tort law and tort theory in both countries when dealing with manufacturers of defect software. Court judgments normally requires the losing party to compensate the victim financially. In principle, compensation in the form of damages and expenses will legally shift legally to the defendant. Since the software is the main reason for this issue, the liability is placed upon the owner of the software manufacturer. Tort distinguishes between two general classes of duties. The first is the duty not to injure 'full stop' and the other duty is not to injure negligently, recklessly, or intentionally. Software fault, is governed by fault liability where it flouts a duty not to injure negligently, recklessly, or intentionally, but can still be governed by strict liability if the user is physically affected.

An example of strict liability reasoning is described by [3] Levy in the case of

Brocklesby v. United State, where the court held a publisher of an instrument approach procedure for aircraft strictly liable for injuries incurred due to the faulty information contained in the procedure. Strict liability applied because the product was defective, even though the publisher had obtained the information from the government. Levy also described in his research of a second tort theory; that the vendor was negligent in developing the software. The plaintiff must show that the vendor had a duty to use a specific standard of care and that the vendor breached that duty. This can be shown if there is malfunction of the software, which results in a negative impact. The screenshot or log of the software can be the evidence for logging the incident.

In 2003 at the [9] State Superior Court in Los Angeles there was an allegation that Microsoft engaged in unfair business practices and violated California consumer protection laws by selling software riddled with security flaws. This allegation is really an opening statement that the software manufacturer can be held responsible for their products. More such legal actions are anticipated. The litigation, legal experts said, is an effort to use the courts to make software subject to product liability laws; a burden the industry has so far avoided and placed the blame on users.

Conclusion

It is clearly defined in both Malaysia and US laws that even though manufacturers provided their own disclaimers, users in both countries can still bring the manufacturer to court if they find any defects in the product. It is important to identify the exact and appropriate policy recommendations for software liability laws both in Malaysia and the United States. This is an important aspect from an information security perspective where the ownership and responsibility of the services are clearly defined. Users and manufacturers should make clear distinctions between safety-critical and normal software applications. The differences between regular and safety-critical applications such as exacting levels of care should be demanded from programmers, as their failure to do so may result in the injury or loss of life. The interest of the user and the manufacturer must be protected when dealing with software product liability issues so that it can be overcome and prevented from happening again in the future. ▪

References

[1] Maybank2u Liability and Indemnity. Available online at http://www.maybank2u.com.my/mbb_info/m2u/public/personalDetail04.do?channelId=&cntTypeId=0&programId=FO-Footer&cntKey=TNC03&chCatId=/mbb/Personal#liability. Retrieved on 23rd November 2011.

[2] Microsoft terms of service. Available online at http://www.microsoft.Com/about /legal/en/us/IntellectualProperty/Copyright/Default.aspx#E6. Retrieved on 23rd November 2011

[3] Levy et al. Tech. L.J. 1 (1989-1990).Software Product Liability: Understanding and Minimising the Risks.

[3] Raysman & Brown, 1988 Strict Product Liability for Software and Data, N.Y.L.J., Sept. 15, 1at 3, 3; Gemignani.

[4] Zammit & Savio, Tort Liability for High Risk Computer Software, 23 PLI/PAT 373, 375 (1987).

[5] Blodgett, Suit Alleges Software Error, A.B.A. J., Dec. 1, 1986, at 22.

[6] Laws of Malaysia Act 599 Consumer Protection Act 1999.

[7] Laws of Malaysia Act 382 Sale of Goods Act 1957.

[8] Laws of Malaysia Act 67 Civil Law Act 1956.

[9] Steve Lohr. 2003. Product Liability Lawsuits Are New Threat to Microsoft. Available online at http://www.nytimes.com/2003/10/06/technology/06SOFT.html. Retrieved on 23rd November 2011.

Implementing ISO/IEC 27001: Choosing an ISMS Consultant

By | Asmuni Bin Yusof

Introduction

In protecting their information assets, many organisations have planned to adopt the ISO/IEC 27001 standard to establish a framework to protect their information assets. The standard is also known as Information Security Management System (ISMS) which can be defined as a set of interrelated and/or interacting elements to establish the policy and objectives used to direct and control an organisation with regard to information security, in order to achieve those objectives. Organisations may be interested to adopt the standard due to many reasons such as regulatory compliance, to gain a stronger business advantage, to provide clear roles and responsibilities towards information security, etc. Due to certain complexities in implementing ISMS, organisations have the option to hire ISMS consultants who may assist them in getting the job done.

As in other industries, selecting the right ISMS consultant can be a daunting task. Many consultants claimed that they are worthy to be considered to assist clients in getting their company certified against the ISMS standard. What is the benchmark of a good ISMS consultant? This paper will discuss the traits of a good ISMS consultant which may help organisations to select a credible consultant to assist them in their journey towards ISO/IEC 27001 certification.

Should your company be certified in ISO/IEC 27001?

Before proceeding further, an organisation should ask themselves why they need to get certified against ISO/IEC 27001. Is it because they are abiding to the government's/ regulators' regulation of mandating such certification for their organisations? The true spirit of ISMS certification should be to provide a framework for managing information security issues in a systematic and continuous manner. As information and information systems are the lifeblood of almost all organisations, protecting information assets cannot be left to the IT department alone. It is inevitable that board of directors and top executives take an interest in the protection of information assets of their organisations. Ultimately, ISO 27001 should be utilised as a management tool or system to help you manage all information security risks and opportunities in the spirit of continual improvement.

The point I want to bring home, "Do not plan to get the certification as a means to get a badge on the wall that confirms your company is ISMS certified".

Issues in ISMS Consultancies

We see the mushrooming of ISMS consultancies throughout the country, claiming to possess vast experience in ISMS. In reality, their track records are quite difficult to verify. The services rendered by these consultants are not standardised and some organisations in need of their services are still not clear of what they should be expecting from those consultants. Probably, the criteria for an effective ISMS consultancy service has not been defined resulting in the vast differences in consultation costs/prices. Although overcharging is not desirable, under-pricing is also bad as it might compromise quality of

services rendered to clients. At the end of the day, an organisation will have to select a credible consultant/consultancy to assist them in getting the certification completed. They should dictate the selection criteria for choosing an ISMS consultant, and thus, ensuring best value for their money.

Expected Deliverables of an ISMS Consultant

A consultant should be able to establish ISMS in your organisation and set it ready for an ISMS certification. He/She should also equip your staff with sufficient skills to 'drive' the ISMS adoption. At the minimum, organisations should be expecting these items from their consultants:

- Identify information assets and provide recommendations on how to protect those assets
- Gap analysis
- Assist in a Risk Assessment exercise and propose a Risk Treatment Plan
- Preparation of Statement of Applicability
- Review existing Information Security Policies and procedures. Develop new policies and procedures if required
- Review existing IT infrastructure and organisation of information security in the organisation and highlight areas for improvement.
- Provide external and internal Vulnerability Assessment and Penetration Testing for critical systems and services
- Identif and recommend ISMS controls
- Guide to develop Document and Record Management capabilities
- Help to develop Incident Management and Response capabilities
- Help to develop Business Continuity Management capabilities
- Develop Internal Audit teams through training
- Provision of Security Awareness Programme Development and ISMS implementation workshops

The Consultant Company

How do we choose companies that are fit to render ISMS consultancy services? Preferably, their core business is in information security and they are ISO/IEC 27001 certified. We should expect the company to completely understand the value of ISMS and share their experiences in running information security programmes and provide 'tips' in dealing with auditors for Certification Bodies.

The company should also provide evidence in the form of client testimonials on successful ISO/IEC implementations of their previous ISMS projects.

Traits of a Credible Consultant

The followings are some of the traits of a good ISMS consultant:

1. **Being an Information Security Professional.** To be able to advice on information security matters, a consultant should have a good background on information security and should have some experience in planning and executing information security programmes in their company. To assist organisations to gauge the potential of a consultant, they should insist for a consultant with some internationally recognised information security certification such as Certified Information Security System Professional (CISSP), Certified Information Security Manager (CISM) and Certified Information System Auditor (CISA). You should demand these requirements as many important controls to protect information assets will involve analysing and proposing

1. the right technical controls. The validity of the certifications possessed by the holders can be easily verified from the certifiers.
2. **Experience in ISMS Implementation.** Preferably, a potential consultant should hold a certification on ISMS Implementation. It will be more worthy if the consultant has prior experience in implementing ISMS projects. The experience is much needed especially in consulting critical issues such as getting top management buy in, across-organisation commitments, identifying risks, business impact analysis, continuous development and improvement matrix. Inexperience consultants may not be able to deliver these crucial tasks.
3. **Certified ISO/IEC Lead Auditor.** It is paramount for an ISMS consultant to have credible information security auditing capability. He/she should be able to consider security controls in the perspective of a certification body. The consultant should possess a valid certificate in ISO 27001 Lead Auditor.
4. **Registered to Relevant Bodies.** To ensure that the chosen consultant is credible, an organisation may want to dictate that the consultant is registered to the relevant auditing or certification boards. You should expect the consultant is registered to the relevant auditing authorities such as the International Register of Certified Auditors, Professional Evaluation and Certification Board (PECB) and the International Register of Certificated Auditors.
5. **Knowledge of the Industry you are in.** Preferably, the potential consultant should have some knowledge of the industry you are in. For example if your company is in the communication sectors, a consultant should understand issues in running the communication business such as bandwidth and quality of service issues. For energy sectors, knowledge of industrial control systems should be necessary.
6. **Thorough understanding of the ISO/IEC 27001.** Although it is difficult to gauge the capabilities of a consultant through any tender selection process, you should be able to do so when you have the opportunity to meet the consultant. The potential consultant should possess a thorough knowledge of the ISO/IEC 27001:2005 standard and other ISMS related standards.

Conclusion

Selecting an ISMS consultant is not a trivial matter as it may affect the outcome of your ISMS certification. The consultant should have vast experience in information security and with substantial experience in ISMS consultancy. An organisation should determine the agreed deliverables to ensure a timely ISMS certification. An organisation should also get the best out of the consultancy services to ensure their ISMS drivers are ready to take over the 'steering wheel' when the contract ends.

An organisation should expect a substantial amount of knowledge transfer. Hence, someone from the organisation must have knowledge of ISMS so as to be able to at least check the performance of the consultant.

Remember, "The actual journey starts when your organisation achieve the ISMS certification" ▪

References

1. ISO/IEC 27001 – Information technology – Security Techniques – Information security management systems - Requirements

2. ISMS Implementation Guide, http://www.atsec.com/.../ISMS-Implementation-Guide-and-Examples.pdf accessed on 28 Feb 2012.

3. ISO/IEC 27001 for Small Businesses Practical Advice

Benefits of ISO/IEC 27005:2011 Information Security Risk Management

By | Noor Aida Idris, Lt Col Asmuni Yusof (Retired)

Introduction

The increasing numbers of cyber security incidents has resulted in managing information security as one of the top agendas in many organisations. Organisations have to keep up-to-date with information security risks introduced by new and advanced technologies, in addition to their own reliance with such new technology since organisational information now resides in a digital world as well as in physical mediums.

Information security management was introduced to ensure organisations were able to secure their most valuable information assets, which concerns critical business information. By proactively protecting information assets and managing information security risks, organisations can reduce the likelihood and/or the impact on their information assets from a wide range of information security threats. Today, there are various mechanisms being practised by different organisations in managing information security. Among which is via information security management systems based on ISO/IEC 27001: 2005 Information Security Management Systems (ISMS) - Requirements.

ISO/IEC 27001 is one of the published standards in the ISO 27000 family that provides the general requirements for implementing information security management systems. This standard provides organisations with means for protecting their information (in terms of confidentiality, integrity, availability) and providing clients, partners and regulators, assurance of compliance to an internationally recognised set of information security requirements. It is a risk-based approach that provides a holistic and structured way in managing information security for organisations.

Risk management is an important concept through information security management. Information security risk management is needed to ensure the confidentiality, integrity and availability of information assets (CIA) is preserved by organisations. According to (Humphreys, 2008), risk management is the key to information security governance by an organisation and to the protection of its information assets. If the organisation is unaware of the risk(s) it faces, it will not deploy or implement security controls; thus fail to protect its most critical assets. Several guidance are available to assist organisations manage their information security risks, one of it is ISO/IEC 27005:2011 Information Security Risk Management. The objective of this paper is to convey benefits of implementing information security risk management based on ISO/IEC 27005:2011 Information Security Risk Management.

Introduction to ISO/IEC 27005:2011- Information Security Risk Management

ISO/IEC 27005 contains description of information security risk management processes and activities, which provide guidelines to organisations to manage their information security risks. This

standard, which was first introduced in 2005, has been revised recently and re-published in 2011. The standard is one of the standards which play a significant role for the successful implementation of ISMS.

Benefits of ISO/IEC 27005

In the authors' opinion, there are several key advantages when organisations refer to ISO/IEC 27005 for implementing information security risk management. Firstly, this standard can be used by any type of organisation. Secondly, this standard supports the requirements of information security risk assessment specified in ISO/IEC 27001. And thirdly, this standard, which has been revised to align with three other risk management standards, can be used by organisations that wish to manage their information security risks in similar fashion to the way they manage other risks.

This standard is applicable to any type of organisation

One of the attractions of ISO/IEC 27005 is the risk management processes described in the standard which is applicable to all organisations, no matter the size or type. As a matter of fact, the information security risk management processes defined by the standard can be applied not just to the organisation as a whole, but to any discrete part of the organisation (e.g. a department, a physical location, a business service or a critical function), any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

Information security risk management described in ISO/IEC 27005 consists of five processes which are: context establishment, information security risk assessment, information security risk treatment, information security risk acceptance, information security risk communication and consultation and information security risk monitoring and review. These five processes are illustrated in Figure 1.

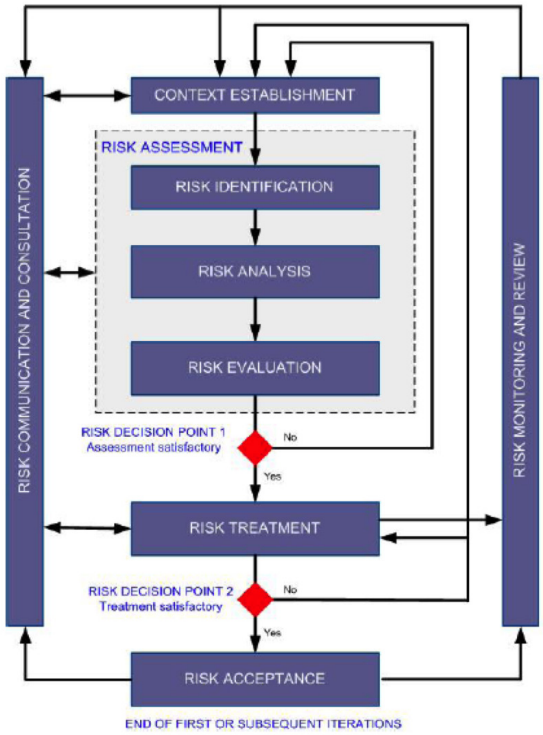


Figure 1: *ISO/IEC 27005 Information Security Risk Management Processes*

The standard supports risk assessment requirements specified in ISO/IEC 27001

Another key benefit offered by the ISO/IEC 27005 standard is that it supports the information security risk assessment requirements specified in ISO/IEC 27001. Thus, organisations that wish to be certified against ISO/IEC 27001 certification may refer to ISO/IEC 27005 when implementing the information security risk assessment.

The mapping of clauses in ISO/IEC 27005 with risk assessment requirements in

ISO/IEC 27001 is discussed in detail below:

a) Clause 7 – Context establishment

In ISO/IEC 27005, the context of risk management for an organisation is established first. In establishing context for risk management, both external and internal context for setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organisation operating the information security risk management. The context establishment process is in line with ISO/IEC 27001:2005 clause 4.2.1 c) Define the risk assessment approach of the organisation.

b) Clause 8 – Information security risk assessment

The context establishment process is followed by a risk assessment process. There are three sub processes included in a risk assessment process which are risk identification, risk analysis and risk evaluation. Risk assessment process determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritises the derived risks and ranks them against the risk evaluation criteria set in the context establishment. The information security risk assessment process is in line with ISO/IEC 27001:2005 clause 4.2.1 d) Identify the risks and e) Analyse and evaluate the risks.

c) Clause 9 – Information security risk treatment

Next is the risk treatment process. The information security risk treatment process involves planning to treat the identified risks. There are 4 options available for risk treatment: risk modification, risk retention, risk avoidance and risk sharing. Selecting the risk treatment options should be based on the outcome of the risk assessment, the expected cost for implementing these risk treatment options and the expected benefits from these options. The information security risk treatment processes is in line with ISO/IEC 27001:2005 clause 4.2.1 f) Identify and evaluate options for the treatment of risks.

d) Clause 10 – Information security risk acceptance

The decision to accept the risks and responsibilities for decisions are made and formally recorded in the information security risk acceptance process. This process is important to ensure that the upper management is aware of the risks and also on the plans to treat the risks. The information security risk acceptance process is in line with ISO/IEC 27001:2005 clause 4.2.1 g) Select control objectives and controls for the treatment of risks and h) Obtain management approval of the proposed residual risks.

e) Clause 11 – Information security risk communication and consultation

The risk communication and consultation process involves activities to achieve an agreement on how to manage risks by exchanging and/or sharing information about those risks between the decision-makers and other stakeholders. The information security risk communication and consultation process is in line with ISO/IEC 27001:2005 clause 4.2.4 c) Communicate the actions and improvements to all interested parties

with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

f) Clause 12 – Information security risk monitoring and review

On-going monitoring and review of current information security risks are important because risks are not static. New threats and vulnerabilities may arise at any point in time; likelihood or consequences may change abruptly without any indication. Thus, constant and continuous monitoring on the risks is necessary to detect these changes. By conducting regular monitoring and review may also ensure that the risk management context, the outcome of the risk assessment and risk treatment plans remain relevant to the organisation. The information security risk monitoring and review process is in line with ISO/IEC 27001:2005 clause 4.2.3 d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks.

Easy alignment with other risk management standards

Another advantage for organisations that choose ISO/IEC 27005 when implementing information security risk management is that they can align the way they manage other risks, such as enterprise-wide risks, with information security risks. This is due to ISO/IEC 27005 being revised recently to reflect changes in three risk management standards which are:

- ISO 31000:2009 - Risk management - Principles and Guidelines;
- ISO 31010:2009 - Risk management - Risk Assessment Techniques; and
- ISO Guide 73:2009 - Risk Management Vocabulary.

As an example, organisations that have adopted ISO 31000 for managing their enterprise-wide risks may find that they can manage their information security risks in a similar fashion. Thus, lesser time and resources may be used when embarking on the journey of adopting ISO/IEC 27005 for information security risk management and implementing ISMS based on ISO/IEC 27001.

Conclusion

Information security risk management is one of the requirements in ISO/IEC 27001 ISMS. As stated earlier, ISO/IEC 27005 is an essential companion for implementing ISMS based on ISO/IEC 27001. The advice and guidance contained in the standard is useful for any organisation intending to manage their information security risks effectively. The three advantages described in this paper can be enjoyed by organisations managing their information security risks based on ISO/IEC 27005.▪

References

1. ISO/IEC, "Information Technology – security techniques – information security risk management systems", ISO/IEC 27005 International Standard, 2011.

2. ISO/IEC, "Information Technology – security techniques – information security management system – Requirements", ISO/IEC 27001 International Standard, 2005.

3. International Organization for Standardization website, www.iso.org, accessed on 23 March 2012.

4. ISO27001 Security website, www.iso27001security.com, accessed on 23 March 2012.

5. Humphreys, E. 2008. Information security management standards: Compliance, governance and risk management, information security technical report 13 (2008) 247–255.

6. Humphreys E. 2010. Information Security Risk Management – Handbook for ISO/IEC 27001, BSI Standards.

Economic Benefits Through Information Security Standards

By | Mohd Nazer Apau, Sabariah Ahmad

Introduction

Within the next eight years, Malaysia aims to be an industrialized and self-sufficient nation in all aspects of life – economic prosperity, social well-being and political stability. To achieve the objectives outlined in Vision2020, the government introduced the Economic Transformation Program (ETP) towards boosting the country's Gross National Income (GNI) to US $523 billion by 2020.

Traditionally, land, labour and capital were considered the main contributors to economic growth. With the information communications technology (ICT) era upon us, Malaysia outlined a Digital Malaysia Master Plan, leveraging the nation's strength in ICT to accelerate and sustain economic needs. New trends like cloud computing, virtualization, mobility, peer to peer file sharing, Web 2.0 and third-party outsourcing have been recognized as effective business enablers.

However, the digital world brings with it new challenges, vulnerabilities, risks and threats which need to be investigated and mitigated. One of the effective approaches to managing these is to adopt robust information security standards.

Emerging Threats that can Impede Economic Growth

According to MyCERT statistics, there are an increasing number of reported cyber incidents (15,218) which include content related incidents, cyber harassments, denial-of-services, fraud, intrusion, malicious codes, spam and other vulnerabilities. The trend is uphill: reported cyber incidents in 2011 (January-December) surpassed 2010 (January-December) figures by 7,128.
Cyber crime, targeting economic sectors, is also on the rise, overtaking traditional crime in its business impact. According to the Symantec 2010 Enterprise Security survey, 75 percent of global organizations suffered cyber attacks and lost an average of US$2 million in 2010. In the UK, £30 billion a year was lost through fraud. The financial services industry alone suffered £3.8 billion losses on credit and debit card fraud[1].

Managing information security is obviously a complex and challenging responsibility because it involves skilled people, the proper processes and the right technology (PPT). And, it works within the framework of the culture and belief of the organization. If the PPT component is not properly integrated, there will undoubtedly be failure in managing information security.

The Role of Standards and the Contribution to Economic Growth

Standards play an important role in managing cyber threats and driving economic benefits. Standards are defined as published documents which describe specifications and procedures which ensure that a material, product, method or service is fit for its purposes and consistently performs in the way it was intended[2]. Studies have shown the positive influence of the use of standards in economic growth. In Germany, the use of standards attributed 1 percent of the Gross National Product[3]; in Australia, a 1percent increase in the use of standards is associated with a 0.17 percent increase in productivity[4]; in the United Kingdom, standards have contributed 2.5 percent per year to its GDP (between 1948 and 2002)[5].

Standards provide a benchmark for efficiency and effectiveness for consumers, clients, traders and developers. Products and

services will surely improve in quality if they conform to standards, and that also gives an assurance of consistent quality. It also means they meet national and international requirements. It allows local companies to gain new market access.

There are more benefits, including local consumers being willing to give local products and services a try as they perceive it to be on par with foreign products and services, and local customers enjoying these products and services at lower prices.

All in all, incorporating standards promotes and even strengthens the local market, maximizes business potential and increases customer trust.

It is expected that Malaysia can gain RM 8.8 billion in its GNI in 2020 by strengthening the local ecosystem and complying with standards in cyber security.

Applying Information Security Standards in the Malaysian Economy

When examining Malaysia's national information security practices, the ETP Performance Management and Delivery Unit (PEMANDU) recognized three important issues that warranted attention:

1. The potential exposure of the Critical National Information Infrastructure (CNII) to cyber threats,
2. The lack of compliance to information security standards, in particular, the information security management system (ISMS i.e. ISO/IEC 27001), and
3. The weak ecosystem of the local industry to support CNII requirements.

Recognizing this, the Cyber Security, Safety and Awareness Act was discussed and deliberated in PEMANDU's Strategic Reform Initiative to boost global competitiveness.

This Act is to be applied in conjunction with the National Cyber Security Policy (NCSP), managed by the National Security Council, and implemented with an action plan under the Cyber Security Technology Framework Thrusts.

With this, the government has introduced a number of information security standards policies, including the implementation of the ISO/IEC 27001:2007 in all CNII. The framework also encourages all security products and systems to be certified with standards requirements, such as Common Criteria (ISO/IEC 15408). Banking sectors and retailers for example, are to comply with Payment Card Industry Data Security Standard (PCI DSS).

The following are some examples and benefits of how information security standards are currently applied in Malaysia:

ISO/IEC 27001 as ISMS De Facto Standard

ISO/IEC 27001:2005 is considered as the de facto standard in managing information security. This standard is aligned with ISO 9001:2000, the Quality Management System and also with ISO/IEC 2000:2005, Information technology – Service management.

Business resiliency (i.e. incident handling, disaster recovery and business continuity) is a vital ingredient and these are specifically addressed in the de facto ISMS standard.

Japan has 3,840 entities certified with ISMS [6]. Malaysia, on the other hand, only has 55 entities that are ISMS certified, including RHB Bank Berhad, Kumpulan Wang Simpanan Pekerja (KWSP), JARING Communications Sdn. Bhd., Malaysian Administrative Management and Planning Unit (MAMPU), Prudential Services Asia, Malaysian Electronic Payment System (MEPS) and Telekom Malaysia (TM).

Towards improving this, the government has mandated all CNII to be ISMS certified by 2013. On the same score, the Malaysian government, through MAMPU, has mandated critical government sectors to achieve ISMS certification.

Information Security Assurance through Trusted Security Products – ISO/IEC 15408

The ISO/IEC 15408 is an international standard for computer security certification (known as Common Criteria). The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme was introduced in 2009 with the formation of a national Certification Body.

In September 2011, Malaysia was accepted as the Certificate Authorizing Participant Member by the Common Criteria Recognition Arrangement (CCRA), a first for ASEAN and for a developing country. With this recognition, Malaysia, through its MyCC Scheme, is able to issue Common Criteria (ISO/IEC15408) certificates on ICT products. As a result, Malaysia is recognized by all 26 CCRA member countries worldwide.

Through the Second Economic Stimulus Package, the Malaysian Government has provided special grants for local companies to have their ICT products certified under the MyCC Scheme. More than twenty products have been certified including access control devices and systems, data protection and biometric devices and a range of other systems.

Payment Card Industry - Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) represents a set of security practices to ensure the safe handling of payment card data. The standard was mainly established by major card companies, i.e. American Express, Discover, MasterCard and Visa.

This standard comprises 12 distinct requirements which helps build and maintain a secure network, protect (cardholder) data in transit or at rest, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test the organization's IT infrastructure, and maintain an information security policy.

Conclusion

The implementation of information security standards by itself will not remove cyber threats, but will however, with the correct implementation as suggested through the standards, assist in identifying and handling the risks.

The use of standards leads to direct and indirect economic benefits as the goal of standardization is to arrive at a universal specification (control), provide inter-operability, reduce costs in terms of process R&D and customer / market acceptance, safeguard assets and many other relevant reasons.

While we have won several world-renowned accolades in applying information security standards, we still have steps to make in ensuring more companies and government agencies recognize the myriad of benefits stemming from its discipline.

The economic benefits will be more pronounced as information technology becomes increasingly pervasive in every aspect of life and business. ▪

Note: This article was published in Microsoft's Future e-magazine on 8 March 2012

References

[1] http://www.which.co.uk/news/2010/01/fraud-costs-uk-30bn , 22 Jan 2010

[2] Standards and the Economy – Centre for International Economics: July 2006

[3] Standards and the Economy by DIN German Institute for Standardization e. V. : April 2000

[4] Standards and the Economy – Centre for International Economics Canberra & Sydney: July 2006

[5] The Empirical Economics of Standards, Department of Trade and Industry Economics Paper no.12 : June 2005

[6] http://www.iso27001certificates.com

Guidance for Internal Information Security Management System (ISMS) Audit – Clause 6 of ISO/IEC 27001:2005 ISMS Requirements

By | Noor Aida Idris

Introduction

The increasing numbers of cyber security incidents have made managing information security as one of the top agendas in many organisations. According to statistics obtained from Malaysia Cyber Emergency Response Team ((hereafter referred to as MyCERT), 15,218 cyber security incidents (excluding spams) were reported in 2011. The figure increased by 88 percent from 2010, where only 8,090 incidents were reported. Until September 2012, a total of 7,905 incidents and 93,439 spams have been reported. Adding to our concern, these numbers are only for reported cases; the number for unreported cases is still unknown and may be a large number as well.

In order for organisations to reduce and manage these cyber security incidents, information security management is introduced. By proactively protecting information assets and managing information security risks, organisations can reduce the likelihood and/or the impact on their information assets from a wide range of information security threats. Today, there are various mechanisms being practiced by different organisations in managing information security. Among which is via information security management system based on ISO/IEC 27001: 2005 Information Security Management Systems (ISMS) - Requirements.

ISO/IEC 27001:2005 ISMS – Requirements is an international Standard published by the International Organisation for Standardisation. The Standard specifies requirements of an information security management system that an organisation can develop and operate to protect its information assets and manage its information security risks. In addition, ISO/IEC 27001 is a certifiable Standard. Thus, an organisation can approach a certification body (CB) to carry out an external audit of the implemented ISMS in order to obtain ISO/IEC 27001 certification.

Internal ISMS Audit

One of the requirements being specified in ISO/IEC 27001 is Clause 6 internal ISMS audit. The internal ISMS audit must be conducted to determine whether the control objectives, controls, processes and procedures of an organisation's ISMS:

1. conform to the requirements of this International Standard and relevant legislation or regulations;
2. conform to the identified information security requirements;
3. are effectively implemented and maintained; and
4. perform as expected.

As internal ISMS audit is compulsory; organisations will need further guidance on how to conduct an internal ISMS audit. The objective of this paper is to provide guidance for organisations to fulfil the internal ISMS audit requirements. The paper will focus on three Standards that were published recently – ISO 19011:2011 Guidelines for Auditing Management Systems, ISO/IEC 27007:2011 Guidelines for Information Security Management Systems auditing and ISO/IEC TR 27008:2011 Guidelines for Auditors on Information Security Controls. These three Standards provide valuable information that can guide organisations in planning, conducting and managing an internal ISMS audit. Organisations are recommended to refer to all three Standards collectively when they plan, conduct or manage their internal ISMS audits.

ISO 19011:2011 Guidelines for auditing management systems

The objective of this Standard is to provide guidance on the management of an audit

programme, on the planning and conducting of an audit of a management system, as well as on the competence and evaluation of an auditor and an audit team. This Standard is applicable to any organisation that need to conduct internal or even external audit of any management system. Examples of management systems includes information security management systems (ISMS), quality management systems (QMS), and environmental management systems (EMS)
This Standard was first published in 2002. The second edition, published in 2011 had been technically revised. Among the main revision that were included in the second edition was the scope of the Standard being broadened from the auditing of quality and environmental management systems to the auditing of any management systems.
One of the key features of this Standard is that it introduces the concept of risk to management systems auditing. The approach adopted relates both to the risk of the audit process not achieving its objectives and to the potential of the audit to interfere with the auditee's activities and processes. However, it does not provide specific guidance on the organisation's risk management process, but recognises that organisations can focus audit efforts on matters of significance to the management systems.

The essence of the ISO 19011:2011 Standards are:

Clause 4	describes the principles on which auditing is based. There are six principles that are outlined in the Standard and that can help users to understand the essential nature of auditing;
Clause 5	provides guidance on establishing and managing an audit programme, establishing the audit programme objectives, and coordinating auditing activities;
Clause 6	provides guidance on planning and conducting an audit of a management system;
Clause 7	provides guidance relating to the competence and evaluation of management system auditors and audit teams;
Annex A	illustrates the application of the guidance in Clause 7 to different disciplines;
Annex B	provides additional guidance for auditors on planning and conducting audits.

Note: As with common structure of international Standards, Clause 1 defines the scope of the Standard; Clause 2 provides normative references; and Clause 3 sets out the key terms and definitions used throughout the Standard.

ISO/IEC 27007:2011 Guidelines for information security management systems auditing

This Standard which was published in 2011, provides guidance on the management of an information security management system (ISMS) audit programme and the conduct of the internal or external audits in accordance with ISO/IEC 27001:2005 ISMS - Requirements, as well as guidance on the competence and evaluation of ISMS auditors. ISO/IEC 27007 is applicable to any organisation that need to understand or conduct internal or even external ISMS audits or to manage an ISMS audit programme. ISO/IEC 27007 reflects and largely makes references to the previously mentioned Standard, ISO 19011. Unlike ISO 19011 that provides guidelines for auditing and managing any management system, this Standard provides additional guidance which is specific to ISMS. Thus, ISO/IEC 27007 should be used in conjunction with the guidance contained in ISO 19011.

As an example, clause 7.2.3.3 of ISO 19011 provides guidance on "discipline and sector specific knowledge and skills of management system auditors". However, clause 7.2.3.3.1 of ISO/IEC 27007 provides additional guidance which is specific for ISMS auditors. Amongst which, an ISMS auditor should have knowledge and skills in the area of information security management methods that include information security terminologies,

information security management principles and their applications and information security risk management methods and their applications. In addition, ISMS auditors need to have general knowledge in information technology and information security techniques as applicable (e.g. physical and logical access control techniques; protection against malicious software; vulnerability management techniques, etc.), or access thereto; and current information security threats, vulnerabilities and controls, plus the broader organisational, legal and contractual context for the ISMS (e.g. changing business processes and relationships, technology or laws).

The gist of ISO/IEC 27007:2011 Standards are:

Clause 4	Focus on principles of auditing; however the principles of auditing that are applied are the same as those in ISO 19011:2011 clause 4. Thus the section does not re-describe the principles on which auditing is based, rather it makes reference to ISO 19011:2011
Clause 5	Provides guidance on managing an audit programme. These guidelines are additional to the ones described in ISO 19011:2011 and are quite specific to the ones related to ISMS
Clause 6	Provides guidance on planning and conducting an audit of a management system. Again, these guidelines are additional to the ones described in ISO 19011:2011 and are quite specific to the ones related to ISMS
Clause 7	Provides guidance relating to the competence and evaluation of management system auditors and audit teams. Similar to clause 5 and 6, these guidelines are additional to the ones described in ISO 19011:2011 and are quite specific to the ones related to ISMS
Annex A	Illustrates the practice guidance for ISMS auditing

Note: As with common structure of international Standards, Clause 1 defines the scope of the Standard; Clause 2 provides normative references; and Clause 3 sets out the key terms and definitions used throughout the Standard.

ISO/IEC TR 27008:2011 Guidelines for auditors on information security controls

This ISO/IEC TR 27008:2011 provides guidance to organisations on reviewing the implementation and operation of information security controls, including technical compliance checking of the controls, in compliance with an organisation's established ISMS Standards.

Unlike the previous ISO/IEC 27007 which was mainly focused on auditing an ISMS, this Standard is not intended for management systems audits. This Standard's focus is on providing guidance to ISMS auditors on auditing information security controls which are mostly described in Annex A of ISO/IEC 27001. Examples of the controls described in the Annex A are asset management, human resources security and communications and operations management.

An organisation's information security controls should be selected based on the result of a risk assessment, as part of an information security risk management process, in order to reduce risks to acceptable levels. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the organisation's specific security and business objectives are met. Organisations may refer to the ISO/IEC TR 27008 as a starting point for defining procedures for auditing and/or reviewing information security controls. Naturally, organisations may have to customise their information security controls review and/or audit based on their unique requirements, security objectives, risks, etc.

The ISO/IEC TR 27008 is applicable to all organisation types and sizes, including public and private companies, government

entities, and not-for-profit organisations that wish to conduct information security controls reviews and technical compliance checks. This Standard was published in 2011.

The main contents in the Standard are:

Clause 6	Provides an overview of information security control reviews
Clause 7	Elaborates on the methods for auditing information security management systems controls. There are three methods that are described in detail which are 'examine', 'interview' and 'test'. Each method will be discussed in detail via two sub topics which are 'general' and 'attributes'
Clause 8	Discusses on the activities that will normally involve in auditing information management systems controls
Annex A	Provides a set of practical guides for technical compliance checking by using typical technical controls depicted from ISO/IEC 27002
Annex B	Provides information on how to obtain initial information gathering for human resources and security, policies, organization, physical and environmental security; and incident management

Note: As with common structure of international Standards, Clause 1 defines the scope of the Standard; Clause 2 provides normative references; and Clause 3 sets out the key terms and definitions used throughout the Standard.

Conclusion

The three Standards, ISO 19011, ISO/IEC 27007 and ISO/IEC TR 27008, provide useful guidance to organisations that need to conduct an internal ISMS audit and fulfil one of the requirements in ISO/IEC 27001. They are intended to be used collectively to meet the objectives of establishing, conducting and managing an ISMS audit programme. Each Standard has its purpose and should be used as a companion for the others, and not to replace one another. The table below shows a summary of the three Standards. ▪

References:

1. ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems – Requirements

2. ISO 19011:2011, Guidelines for auditing management systems

3. ISO/IEC 27007:2011, Information technology -- Security techniques -- Guidelines for information security management systems auditing

4. ISO/IEC TR 27008:2011, Information technology -- Security techniques – Guidelines for auditors on information security management system controls

Standard	Summary
ISO 19011	Provides guidance on the management of an audit programme
ISO/IEC 27007	Provides guidance on the management of an information security management system (ISMS) audit programme and in accordance with ISO/IEC 27001:2005 ISMS – Requirements. This Standard should be used in conjunction with the guidance contained in ISO 19011
ISO/IEC TR 27008	Provides guidance on reviewing the implementation and operation of controls, including technical compliance checking of information system controls

Legal Restriction on Cryptography

By | Liyana Chew Binti Nizam Chew, Abdul Alif Bin Zakaria

Introduction

Historically, a number of countries have attempted to restrict the export or import of cryptography tools. This article aims to give a general view on the existing restrictions on cryptography tools. Export restrictions are totally different from imports. Restrictions on exports are referring to restrictions on exporting cryptographic tools out of countries that produce them. Meanwhile restrictions on imports refer to a country that receives cryptography tools for their needs. This article will also discuss the reasons why certain countries do apply these restrictions while other doesn't.

Restriction On Export

The export of cryptography is a transfer of devices and technology related to cryptography from one country to another country. In the early days of the Cold War, the U.S government developed an elaborate series of export control regulations designed to prevent a wide range of Western technology from falling into the hands of others. U.S non-military exports are controlled by Export Administration Regulations (EAR). Encryption items specifically designed, developed, configured, adapted or modified for military applications (including command, control and intelligence applications) are controlled by the Department of State on the United States Munitions List.

U.S government set a restriction on export of cryptography product with strict limit on the key size. In general, products and technologies with exportable cryptography provide much less security than the non-exportable version of the same products and technologies. Non-exportable version of cryptography product use longer key length (128 bits) than exportable (40 bits or 56 bits) version. Communication between these two versions is limited to the longest key length supported by the exportable version. As reported in The New York Times on December 1998, U.S and European Union (EU) officials have reached an agreement on export controls for cryptography software. Both blocs agreed to restrict the export of encryption software that uses keys of 64 bits or more. U.S law currently forbids companies from exporting software that uses that level of encryption. That's why US versions of Web browsers contain 128-bit encryption to encode e-commerce transactions, but European versions use a much lower level of security (40 bits key). The agreement, reached by the 33 members of the Wassenaar Arrangement, will impose those export restrictions on European software suppliers. The more bits in the key, the harder it is to crack. The US government claims 64-bit keys are sufficient for almost all uses. However, research proves that it is possible to break a 56-bit code, albeit using a network of hundreds of PCs operating in parallel. Much tougher keys, including the 128-bit keys commonplace in e-commerce applications, are thought to be virtually impossible to crack using today's technology through the next few generations of processor.

Until January 2000, the export restrictions of Cryptography in the U.S become more relaxed. Export to end-users is approved under a license except to foreign governments or embargoed destinations the likes of Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, Syria, and Taliban-controlled areas of Afghanistan.

Rationale to Export Control

Some countries have restrictions in the export of cryptography because of the government's fear that their intelligence activities are hampered by the use of cryptography by scoundrel states. Governments in these countries tried to block the access of these foreign entities to cryptography systems or cryptography codes. It's clear that these governments wanted to deny their enemies the potentials of cryptography technology. Monitoring diplomatic communications will be difficult if no restrictions are in place. The reasons for controlling cryptography exports are because governments are worried about the misuse of cryptography, where if it is misused it may be detrimental to the interests of a country.

The Controls That Are Contrary to Wassenaar Agreement

The Wassenaar Arrangement was established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

The Wassenaar Arrangement is an international agreement between 33 participating nations with the following being one of its main objectives (copied verbatim from the Initial Elements):

"It is stated that the arrangement will not be directed against any state or group of states and will not impede bona fide civil transactions. Nor will it interfere with the rights of states to acquire legitimate means with which to defend them pursuant to Article 51 of the Charter of the United Nations."

This aim stated that it is not prohibited if the purpose is for self-defence. However, immediate emphasis will happen if any development which threaten regional or international stability and security. This aim clearly stated that the Wassenar Agreement is not to be used legitimately to obstruct genuine civil transactions. This means that products that are designed for civil use should not be restricted by control.

There are several issues that relate to export controls on cryptography under the Wassenaar Agreement. The most important issue is even if cryptography is assessed as important in military terms; it is a purely defensive technology with no offensive uses. Cryptographic products are entirely passive products with a single purpose of defending and protecting information assets from an aggressor who, for their own reasons, seeks to gain access to them. Given its passive and entirely defensive nature, it is thus hard to see any case for the control of cryptographic products under the Wassenaar Arrangement – they simply are not capable of being used offensively in any manner.

Export controls over cryptographic products also affect public civil transactions and applications. The protection of national information assets, the development of secure electronic commerce and the protection of the privacy of citizens all now depend on civil cryptographic products that are subjected to existing export controls. Export controls on cryptographic products have a severe impact on such civil transactions. This is in direct contravention of the aims that clearly stated that the

Wassenaar Agreement "will not impede bona fide civil transactions". In fact, this clause, when combined with the impact that cryptographic export controls are having on the civil market, might allow such controls to be legally challenged where the Wassenaar Arrangement is being used to justify them.

Restriction on Imports

Import of cryptography can be defined as good or services of cryptography brought into one country from another country. Cryptography is subject to import restrictions. Several governments place import restrictions on encryption technology. The availability of these encryption technologies depends on the actual strength of the encryption that you are allowed to use for security. This varies according to import restrictions for a specific geographical area. Not all countries apply the restrictions on importing cryptography tools. It reflects on what is the outcome that a particular government may face if they simply allow import activities of cryptography tools.

Table 1 shows countries with restrictions on importing cryptography tools (refer table below), the colour green represents some countries with no import restrictions at all. The ones in yellow shows that for countries to import cryptography tools, a license is required to import them. Countries that are totally banned from importing cryptography are in red. The "Unknown" column states that these countries are encouraged to seek further advice from their governments before importing any cryptography tools. Meanwhile, those with mixed colours, represent mixed restrictive policies.

Rationale to Import Control

There are reasons why certain governments are really concerned about importing cryptography tools from foreign countries. They are afraid that the public might misuse cryptography for negative purposes, for example, planning a rebellion against the government and the government will not have a chance to monitor the communications as it is encrypted. Governments prefer

GREEN	GREEN	YELLOW	YELLOW	YELLOW	RED	RED	RED	Unknown	Unknown
Ghana	Armenia	Bahrain	Brunei	Belarus	North Korea	Nepal
Saudi Arabia	Czech Republic	China	Tunisia	Iraq	Tatarstan
Malaysia	Hong Kong	Egypt		Mongolia	
Singapore	Hungary	Iran		Myanmar	
	India	Israel		Russia	
	Poland	Kazakhstan		Turkmenistan	
	South Africa	Latvia		Uzbekistan	
		Lithuania			
		Malta			
		Moldova			
		Morocco			
		Pakistan			
		South Korea			
		Ukraine			
		Vietnam			

Table 1: *Import Restriction Table*
(Source: Restriction on Cryptography Imports)

using locally developed cryptography tools because imported cryptography tools might have "trapdoors" or security holes. Trapdoors in this case concerns the use of foreign technology, where the producing country might have their own agenda to break into the national security of another because they know the weakness of the systems that they have developed and they can control the system at any time.

Cryptography Restrictions in Malaysia

In Malaysia, there are no export or import restrictions on cryptography tools. Any transfer of devices and technology related to cryptography from Malaysia to another country or vice versa is allowed without any need for licenses. In terms of the use of crypto, no restrictions are in place and the public can use it freely.

Although Malaysia has no restrictions on cryptography but we are still bound by a few Acts that are related to implications of cryptography misuse. There were three Acts that are worth highlighting here. These three Acts contain powers to require authorities to decrypt during an investigation; such investigation is allowed when there is reasonable cause to believe that an offence under the Act at issue is being or has been committed. There is, therefore no general powers to order decryption.

i. Computer Crimes Act 1997

'Art. 10 (1) (b) of the Computer Crimes Act 1997 requires (likely) users and people otherwise concerned with the operation of computers or material, during a search, to provide reasonable assistance for the purpose of accessing programs or data or material that is reasonably suspected to be used in connection with an offence under the Act, as well as to produce any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible. Refusal to cooperate is punishable with at most RM25,000 and/ or three years' imprisonment (art. 11).'

A police officer conducting a search or an authorized officer conducting a search shall be given access to computerized data whether stored in a computer. The access may include copies of any books, accounts or other documents, including computerized data, which contain or are reasonably suspected to contain information as to any offence so suspected to have been committed. The enactment of appropriate laws, with the aim of protecting victims of computer crimes and to provide legal means of prosecuting those who are found guilty of committing such crimes. In Malaysia, the punishment may take three years imprisonment and/or a monetary fine of RM25,000. Note that stiffer penalties will be meted out if it is found that the guilty party had the intention to cause injury when committing the crime.

ii. Digital Signature Act 1997

'Art. 79 of the Digital Signature Act 1997 requires people, during a search, to give access to computerised data whether stored in a computer or otherwise, which includes providing the necessary password, encryption code, decryption code, software or hardware required to enable comprehension of computerised data. Refusal to cooperate is punishable with at most RM200,000 and/or four years' imprisonment (art. 83).'

The Digital Signature Act was enforced on the 1st October 1998. The Digital Signature Act 1997 aims at promoting the processing of transactions especially commercial

transactions, electronically through the use of digital signatures. This Act is an enabling law that allows for the development of, amongst others, e-commerce by providing an avenue for secure on-line transactions through the use of digital signatures. The Act provides a framework for the licensing and regulation of Certification Authorities, and the recognition of digital signatures. The Controller of the Certification Authority who has the authority to monitor and license recognized Certification Authorities was appointed on 1st of October 1998.

iii. Communications and Multimedia

'Art. 249 of the Communications and Multimedia Act requires people, during a search, to give access to computerised data whether stored in a computer or otherwise, which includes providing the necessary password, encryption code, decryption code, software or hardware required to enable comprehension of computerised data. Refusal to cooperate is punishable with at most RM100,000 and/or two years' imprisonment (art. 242). This Act contains a provision (art. 256(2)) allowing people to refuse answering questions if they thereby would incriminate themselves; by contrast, the privilege against self-incrimination can be deemed not to hold for complying with a decryption order.'

An authorized officer making an investigation under this Act may verbally examine a person who supposed to be acquainted with the facts and circumstances of the case. The person shall be legally bound to answer all questions relating to the case put to him by the authorized officer, but the person may refuse to answer any questions where the answer to which would have a tendency to expose him to a criminal charge or penalty or forfeiture. A person making a statement under this section shall be legally bound to state the truth, whether or not the statement is made wholly or partly in answer to questions.

Conclusion

Cryptography itself is a harmless system. It was built to defend the security systems of individuals or a nation. The nature of cryptography is defensive and not offensive. It depends on the user to use it wisely. Cryptography tools are not easily imported or exported because there may be issues that will arise at the end of the day if people were to use cryptography for negative purposes. Restrictions are not same in all countries and there are no standard restrictions. It depends on what is the government's view on the impact of applying cryptography in their country. From my personal point of view, cryptography restrictions are not necessary because cryptography is not a harmful tool. Cryptography does protect communications and does not serve to take advantage on others. It is the people factor that still plays a role in determining the dangers associated with cryptography. ▪

References

1. Whitfield Diffie and Susan Landau (2005). The Export of Cryptography in the 20th Century and 21st. Palo Alto: Sun Microsystems.

2. Wassenar Arrangement on Export Controls for Conventional and Dual-Use Goods and Technologies. http://www.wassenaar.org/index.html

3. Cryptography Export Laws. http://www.freeswan.org/freeswan_trees/freeswan-1.5/doc/exportlaws.html

4. Export or Import Restrictions. http://www.citrix.com/lang/English/lp/lp_1319021.asp

5. John Markoff. International Group Reaches Agreement on Data-Scrambling Software. The New York Tomes.

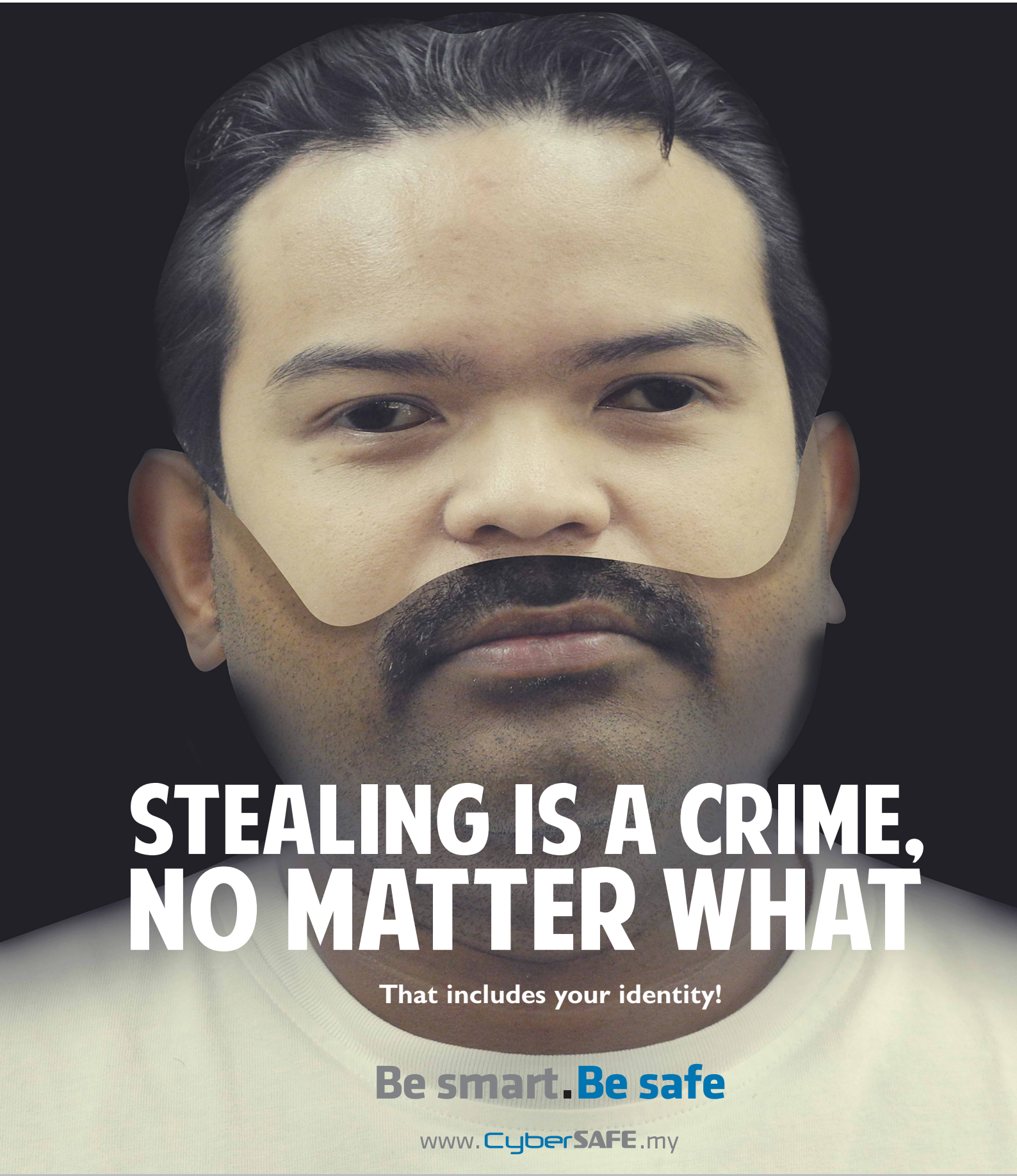
CyberSecurity MALAYSIA

An agency under MOSTI

People First, Performance Now

MOSTI

Ministry of Science, Technology and Innovation



STEALING IS A CRIME, NO MATTER WHAT

That includes your identity!

Be smart. Be safe

www.CyberSAFE.my

Corporate Office:
CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my